Description of document:	US Secret Service (USSS) Documentation regarding Secret Service destruction of records relating to the January 6th attack on the US Capitol 2018-2022 (some records undated)
Requested date:	01-August-2024
Release date:	11-August-2024
Posted date:	25-August-2025
Source of document:	FOIA Request U.S. Secret Service FOIA Office 245 Murray Lane Building T-5 Washington, D.C. 20223 FOIA@usss.dhs.gov FOIA.gov

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: August 11, 2025

File Number: 20241235

Dear Requester:

This is the final response to your Freedom of Information Act/Privacy Act (FOIA/PA) request, originally received by the United States Secret Service (Secret Service) on August 1, 2024, for information pertaining to information pertaining to certain "planning documents, Secret Service policies, notices to employees, and milestone documents" related to the InTune migration referenced in a July 19, 2022 letter from Ronald L. Rowe Jr, to Rep. Bennie G. Thompson, the chairman of the Select Committee to Investigate the January 6th Attack on the United States Capitol (hereafter referred to as "Rowe's letter"), specifically:

1. A copy of the "O365 Capabilities Rollout Schedule" document, which is referenced in Rowe's letter;

2. A copy of all briefing documents for a Dec. 16, 2020 briefing by OCIO's COO briefing on the O365 rollout, which are referenced in Rowe's letter;

3. The Jan. 25, 2021 agency-wide Official Message notifying USSS offices of the InTune migration plan, which is referenced in Rowe's letter;

4. A copy of the guide titled "USSS Preserve Content Guide for iPhone & iPad," which is referenced in Rowe's letter;

5. A copy of GRS-06(01),Management of E-Mail and Other Electronic Message Records, which is referenced in Rowe's letter; and

6. A copy of RPM-01, Secret Service Records Management Program, which is referenced in Rowe's letter.

After a detailed review of all potentially responsive records, 116 pages were released and 0 pages were withheld in their entirety. After considering the "Foreseeable Harm" standard, outlined in Title 5 U.S.C § 552(a)(8)(A)(i) and Department of Justice guidance, exemptions under FOIA Statute Title 5 U.S.C. § 552, and/or the PA Statute Title 5 U.S.C. § 552a, 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)

Section 552a (Privacy Act)

(d) (5)	(j) (2)	(k) (1)	(k) (2)	(k) (3)	(k) (5)	(k) (6)

Please be advised, in the processing of this FOIA/PA request, no fees are being assessed.

If you deem our decision an adverse determination, you may exercise your appeal rights. Should you wish to file an administrative appeal, your appeal should be made in writing and received within ninety (90) days of the date of this letter, by writing to: Freedom of Information Appeal, Deputy Director, U.S. Secret Service, Communications Center, 245 Murray Lane, S.W., Building T-5, Washington, D.C. 20223. If you choose to file an administrative appeal, please explain the basis of your appeal and reference the case number listed above.

Additionally, you have the right to seek dispute resolution services from the Office of Government Information Services (OGIS) which mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. Please note that contacting the Secret Service's FOIA Program and/or OGIS **is not** an alternative to filing an administrative appeal and **does not** stop the 90-day appeal clock. You may contact OGIS at: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001. You may also reach OGIS via email at ogis@nara.gov, telephone at 202-741-5770/toll free at (877) 684-6448, or facsimile at (202) 741-5769.

If you need any further assistance, or would like to discuss any aspect of your request, please contact our FOIA Public Liaison Kevin Tyrrell, at (202) 220-1819. Alternatively, you may send an email to foia@usss.dhs.gov.

FOIA/PA File No. 20241235 is assigned to your request. Please refer to this file number in all future communication with this office.

Sincerely,

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

Enclosure:
FOIA and Privacy Act Exemption List

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

(b)(7)(A)

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: 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

(b)(7)(A)

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: 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

(b)(7)(A)

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: (b)(6); (b)(7)(C) (CIO)
To:
Subject: MDM -- InTune Batch Schedule Notification
Date: Wednesday, January 27, 2021 9:59:00 AM

From: (b)(6); (b)(7)(C)
Sent: Monday, January 25, 2021 3:38 PM
To: (b)(6); (b)(7)(C)
Subject: 145.000 Mobile Device Management Migration

//ROUTINE//

FROM: Office of the Chief Information Officer File: 145.000

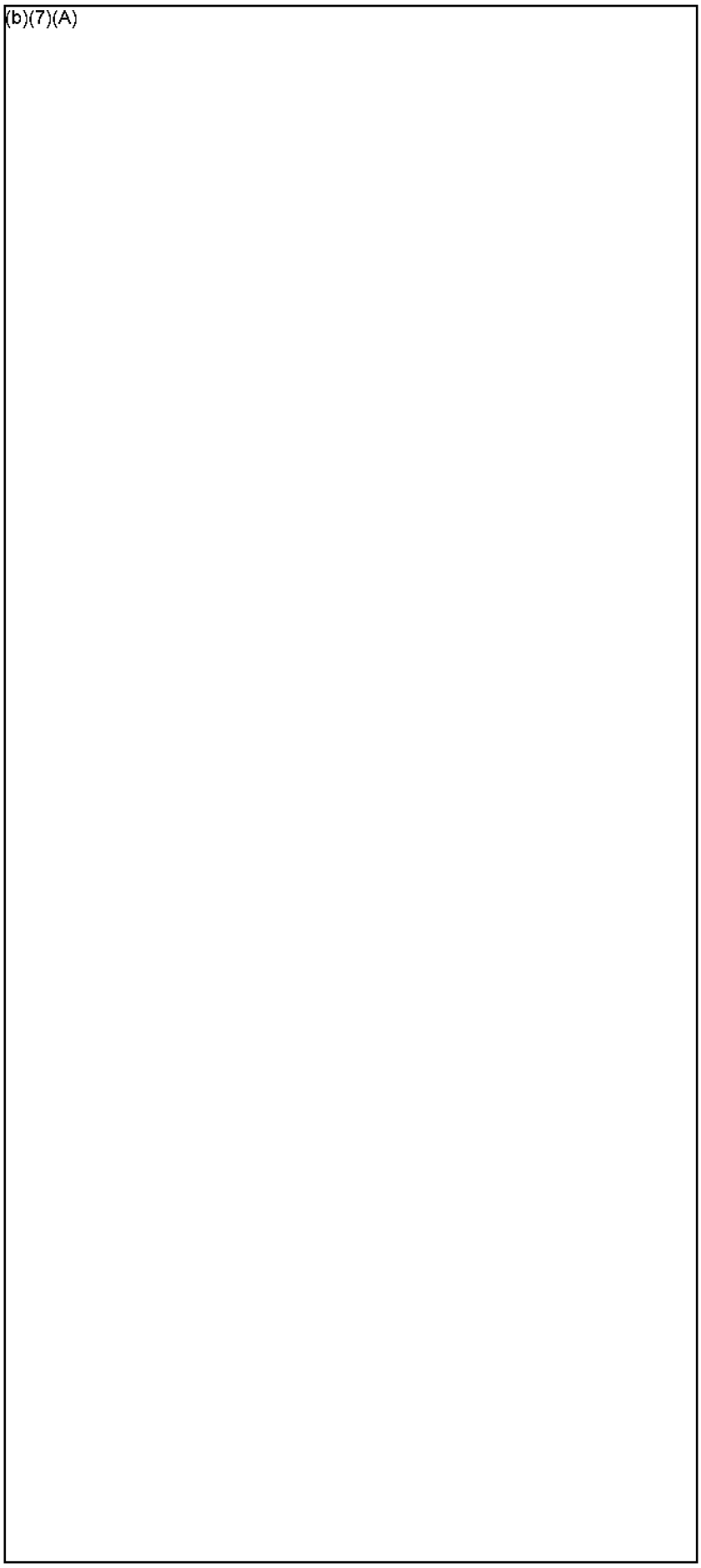
TO: All Offices

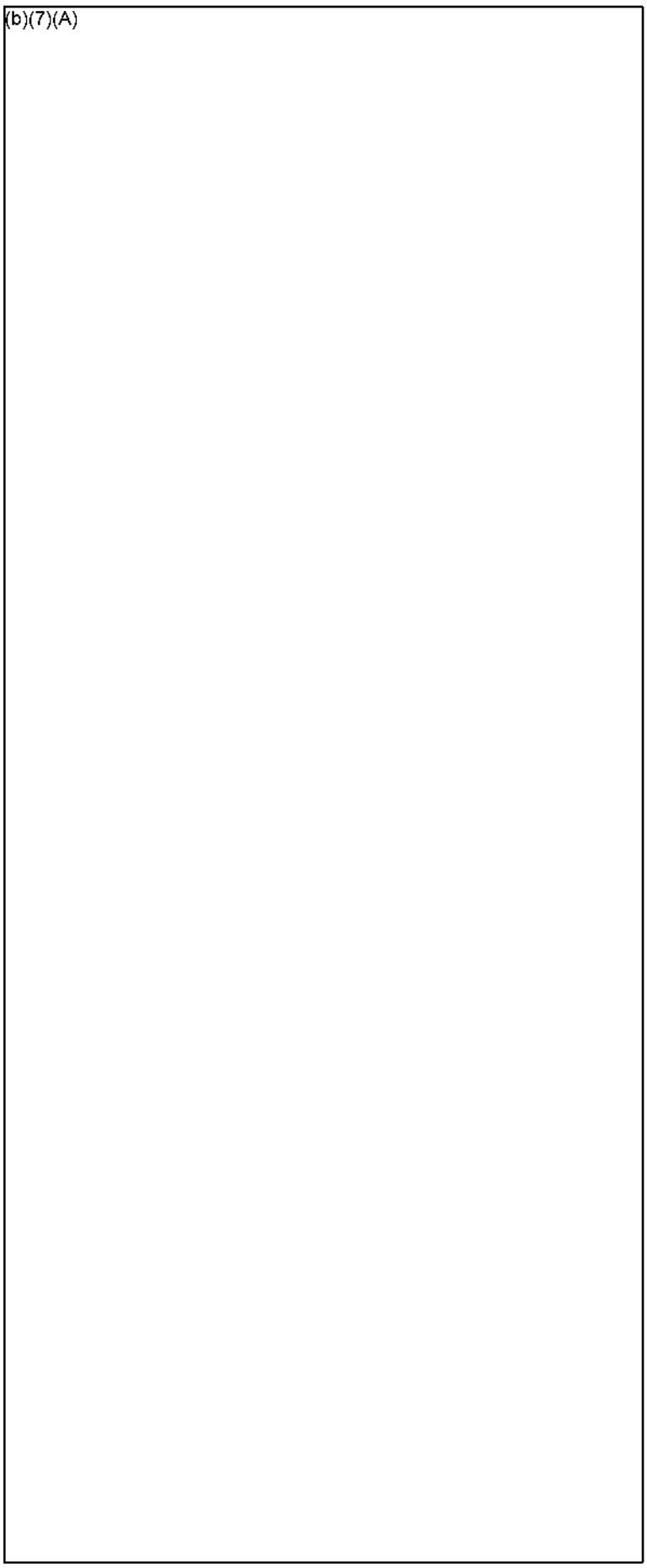
SUBJECT: Mobile Device Management Migration

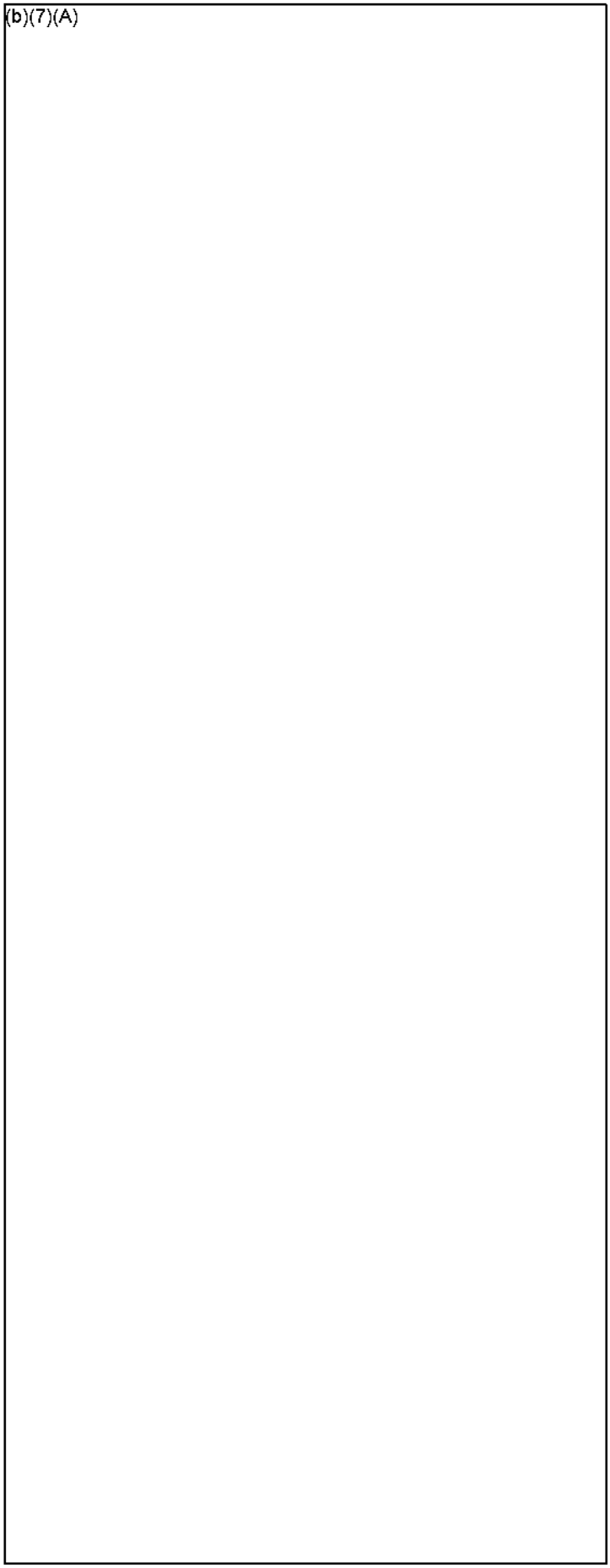
(b)(7)(A)

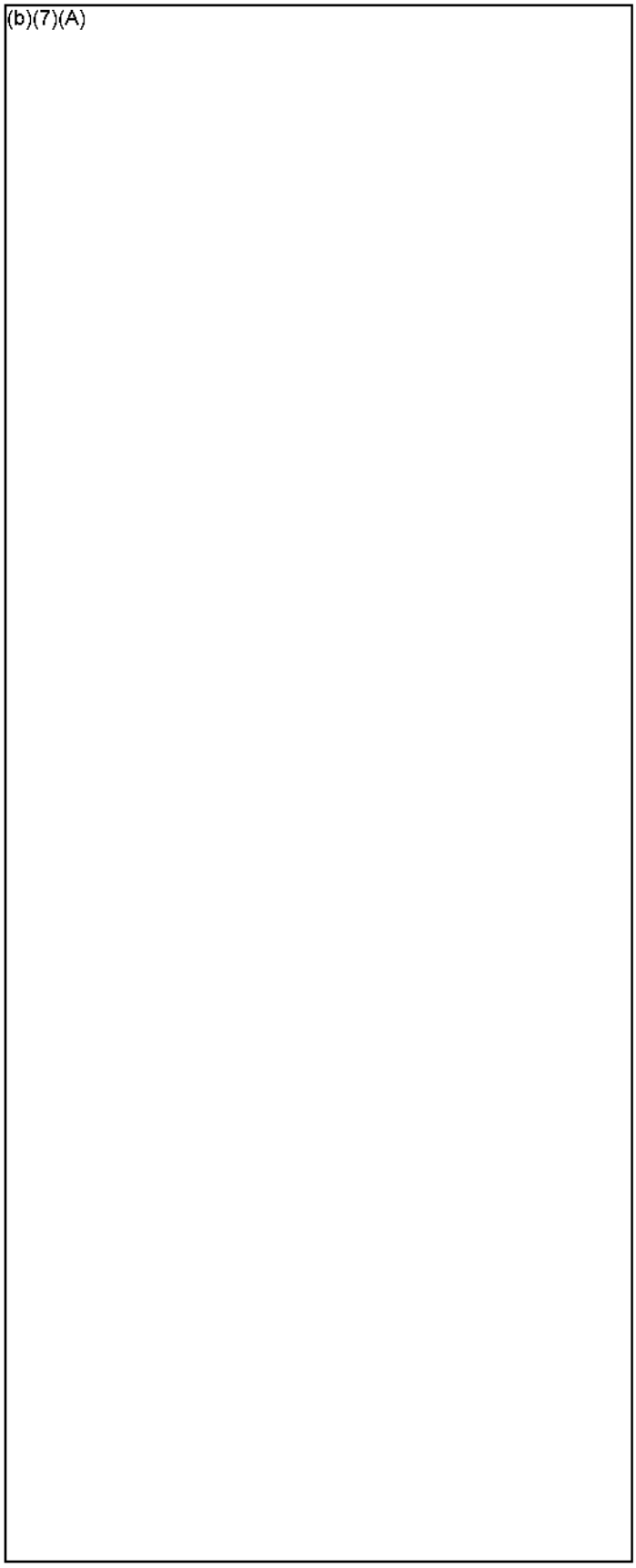
(b)(7)(A)

(b)(7)(A)


(b)(7)(A)


(b)(7)(A)


(b)(7)(A)

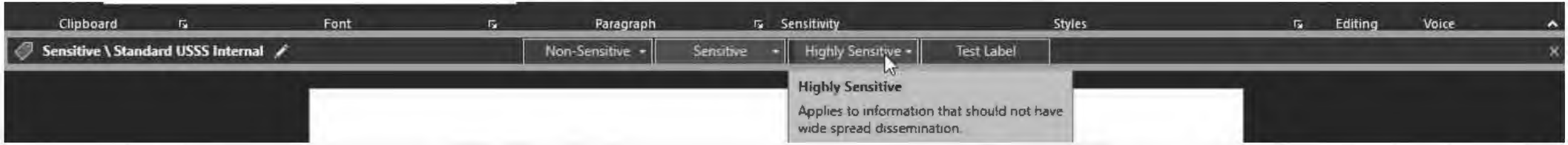

(b)(7)(A)

- Update on DRM Migration Progress (aka AIP)
- Other O365 features
- Other recommendations

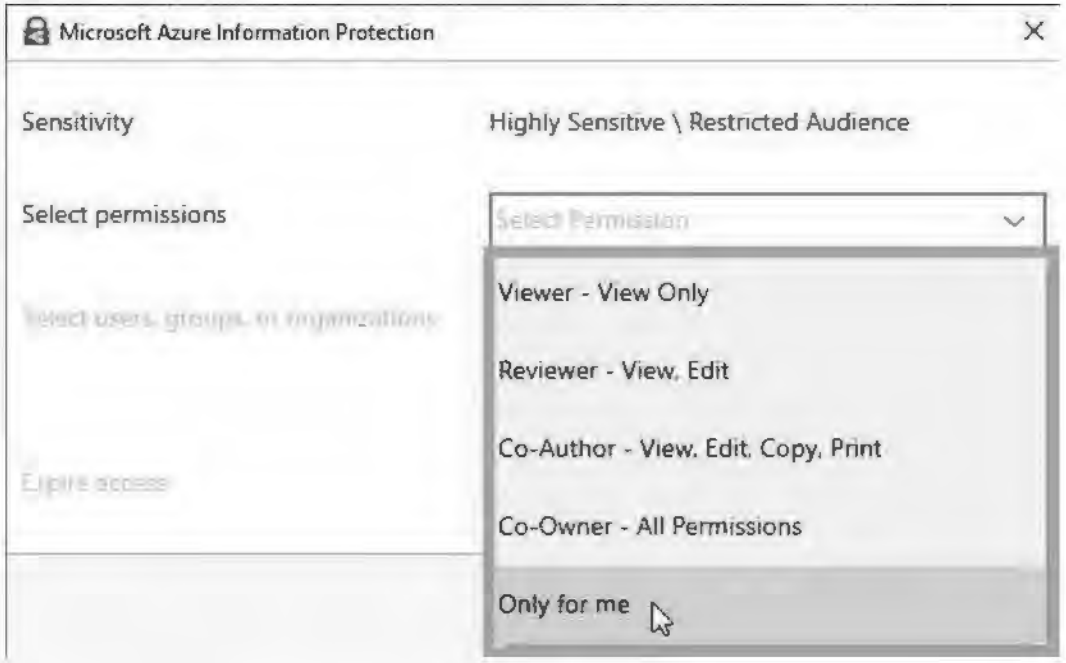
(b)(6); (b)(7)(C)
Cyber Security, Architecture

(b)(6); (b)(7)(C)
Enterprise Server Branch

AIP/DRM - Applying a Label in Word/Excel



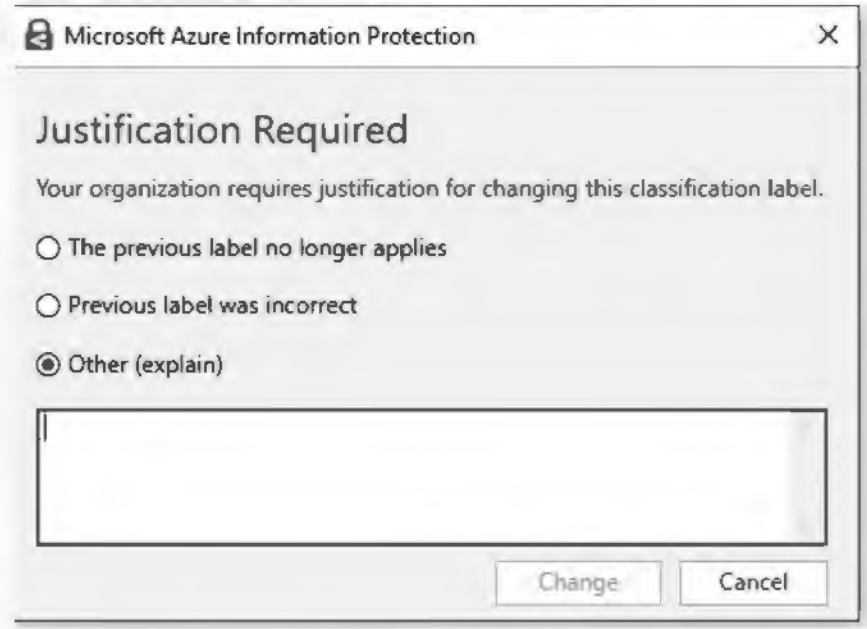
When the Unified Labeling Client is installed, users will have access to a Sensitivity Button and Bar on their main Ribbon in their Microsoft Office client applications. From here, users can select from the labels available to them.



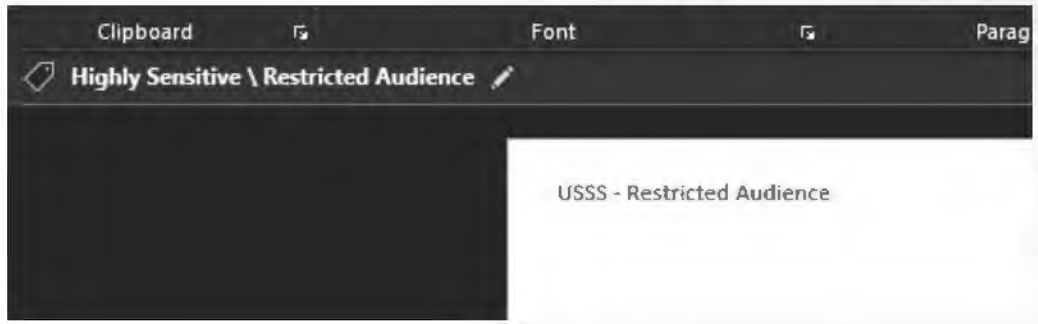
AIP - What Labels Can Do

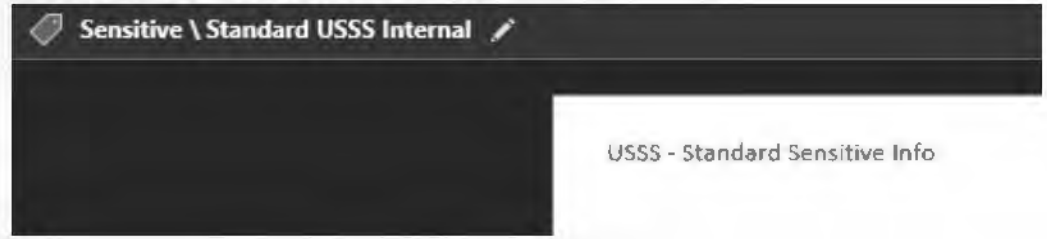
Encrypt and restrict access:

Require justifications for changing a label:



Add watermarks to documents and emails:





Important note about the following slides:

All of the following services related to O365 are already paid for as part of our annual agreement.

Using them would incur $0 in costs.

The data for these services is stored in Microsofts' Government Community Cloud (GCC) (located in VA & Arizona).

Why Cloud?

The short version: because we don't have a lot of choice – Microsoft and indeed the industry at large is investing pretty much all new features in their cloud-only products, and our security posture wont keep pace with modern attacks if we don't adopt at least some of these things. And in certain cases – such as Team's on-prem predecessor Skype, Microsoft has already announced its end-of-life date, making Teams the only viable option. Same for MS Exchange.

There are of course also reasons that aren't so fatalistic. First of all, we have already have paid for these services as part of our annual ELA so from a financial standpoint we may as well use them.

Furthermore the use of cloud apps may have an interesting effect on overall IT servicing @ USSS. Right now when an on-prem application is launched, lets say Air Watch for example, the Application Admins (the MDM team) need to be experts in not only use of the app but also setting it up, patching, and troubleshooting it. By adopting Platform As A Service model applications, like Airwatch's O365 counterpart Intune – those same Administrators have a huge burden lifted and no longer have to have the same mastery of the applications' "back end", and can focus exclusively on "how to use the app". This could, ultimately, provide better service to USSS users.

O365 Offering: Intune

On-prem analogue: AirWatch

BLUF: Increased security, decreased outages, better user experience & huge cost savings.

Security Improvements	Additional Features	Cost Savings
Enrollment only involves the user, so it prevents possibility of impersonation like we have now.	Simplified User Enrollment process, without help from IT	Saving of approximately $1.2M in AirWatch licenses & contractor support staff
Conditional Access (comply to connect for mobile devices & PCs)	Resiliency – automatically load balanced & redundant	Manhours of preventative hardware maintenance (patching)
Defender iOS/iPadOS only supported with Intune	Push notification assurance (launch app requirement is achieved during enrollment). So we can send "emergency" messages via Push	Manhours of reactionary hardware maintenance (outages)
	Less sTokens to monitor for expiration	IT Man hours saved on enrollments, as the user completes their enrollment w/o IT assistance
	Compliance alerts will be sent via push notification which are hopefully less likely to be ignored	Many IT-Man hours saved, plus user frustration during enrollment, as the VPN certificate installs in the correct order.
	Automatically updates the MDM back end – with Air Watch we are always are behind at least a few months, so sometimes we can't use new iOS features until we update.	
	User Self Passcode reset w/o calling Help Desk via web portal	
	Eliminates user error when logging into other Microsoft Apps on the iPhone / iPad	

O365 Offering: OneDrive

On-prem analogue: "P" Drives

BLUF: Unlimited file storage for user documents. More secure & survivable than current P drives. Files are available on iPhone & iPad, a huge improvement over current P drives

Security Improvements	Additional Features	Cost Savings
CASB (aka MCAS) gives us fantastic visibility into who has what files, and whom they are shared with.	Auto Saving of Documents as you type in them	No immediate cost savings as hardware has already been purchased. Will reduce future CapEx by 7 figures.
Huge improvement to eDiscovery & insider threat investigations, as the documents are centrally stored and can be retrieved by admins at any time – regardless if the user is online	Unlimited Storage	Less Storage needed
Continuous Blue/Red Team Testing (per FedRAMP)	Works fantastically on iPhone & iPad	Man hours manually transferring images from iPhone
AIP & DLP Integration	Survivable & resilient: Files remain accessible when Blue Line is "down"	
	Searching files is *much* faster. It's hard to over state how much easier it is to search for a file or it's contents w/ OneDrive over P drives.	
	Files stored in OneDrive can be modified by many people simultaneously, for "co-authoring"	
	Version History for Office Docs	
	iOS photo backup	
	Not producing errors during large file transfers from iOS, which is currently experienced for on-prem	

O365 Offering: Exchange Online

On-prem analogue: Exchange + Enterprise Vault

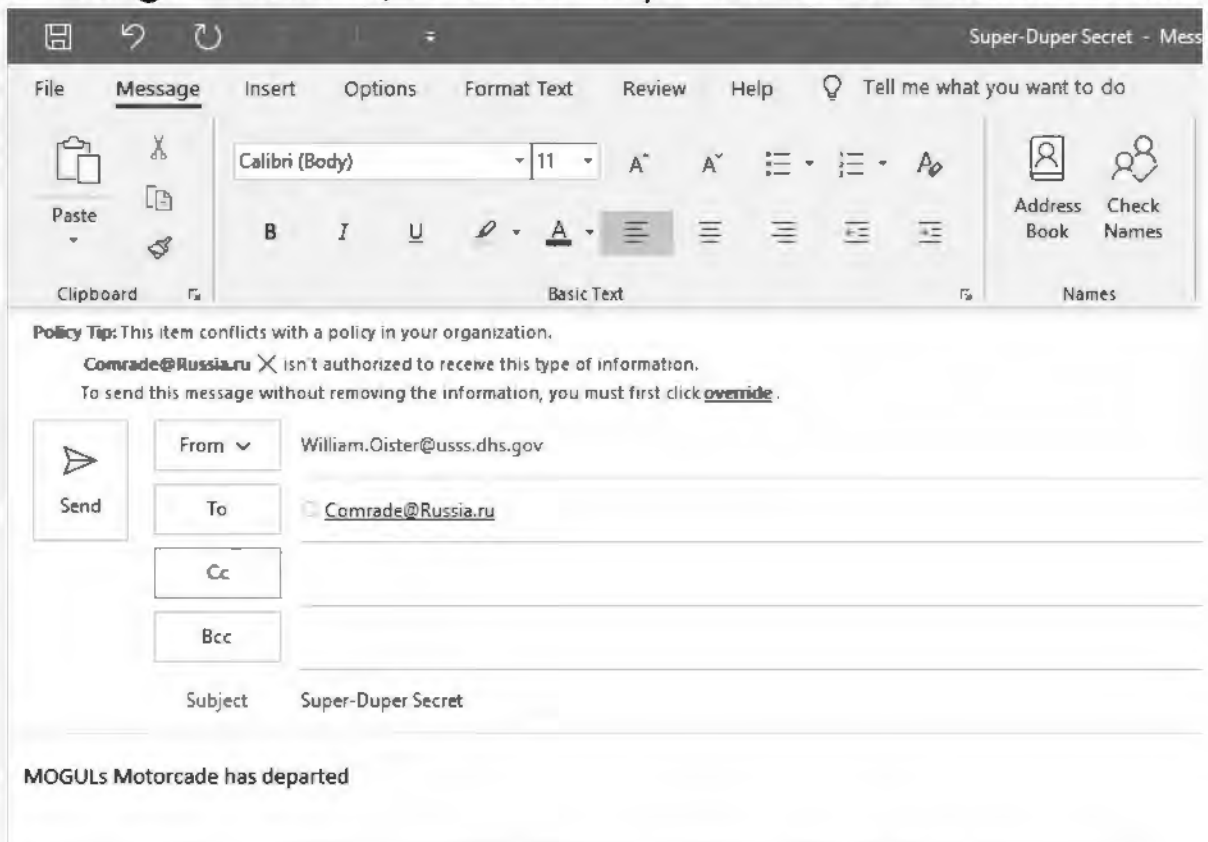
BLUF: Far, far more survivable & huge admin overhead reduction. Integrates w/ Intune for password-less login.

Security Improvements	Additional Features	Cost Savings
AIP & DLP Integration	Index / Searching much improved. Finding old emails is SOOO much better	Cost of EV licenses + contractor ($425,000 / yr) + storage ($ TBD)
eDiscovery built in	Outlook for iOS is phenomenal	Saved manhours of hardware & software maintenance
Massively Resilient / Survivable	Teams “Status” Works	
No more Pulse Secure for email!	150MB send/receive file size	
Litigation hold/in-place	100GB Mailbox Size	
	Unlimited Email Archive Storage	

Show & Tell:
Data Loss Prevention (DLP) in Exchange Online

Exchange

Sending an email w/ sensitive keywords to user outside USSS



This is an exceedingly basic example for illustration purposes only, our actual rules will be much more complex so as to allow for known cases where these keywords are known to be needed to be shared.

O365 Offering: SharePoint Online

On-prem analogue: SharePoint

Security Improvements	Additional Features	Cost Savings
AIP & DLP Integration	Index / Searching	Future CapEx reduction
eDiscovery built in	Massively Redundant & survivable	Saved manhours for patching
Massively Resilient / Survivable		

Where does E5 Fit in?

- Service Encryption with Customer Key
  - The ability for certain data (Exchange Online, OneDrive, Teams & Sharepoint to have an extra layer of USSS-specific encryption.
- Customer Lockbox
- Defender for Office 365
  - Microsofts' in-house version of FireEye, but for Exchange Online, OneDrive, Teams & Sharepoint
- Data-Loss Prevention for Teams
  - Exactly like we already have for Outlook.
- Data-Loss Prevention for Windows 10
  - Monitor/Block files being copied to CD/DVD/Thumbdrives

Now, the non–O365 Stuff…

Mid-term goal: Replace (most) Laptops w/ iPads

We currently have ~6100 "blue line" laptops which constitutes ~80% of the blue line end-user device inventory.

By migrating most of those users to iPads we greatly increase our security posture, as OS and Application patching are far easier on iPads

Some users who regularly use non-standard apps that are not iPad compatible would need to continue to use laptops (for instance, most of IT), however in some cases they could probably use a Virtual Desktop from their iPad.

iPad Air (4th Gen) with Magic Keyboard

Security Improvements	Non-Security Benefits	Cost Savings
Attack Surface Reduction. iOS is a modern OS where applications don't have the ability to interact with most of the system, and none of the other apps. This greatly improves security.	No Image. Zero Touch. We can ship a brand new iPad from the factory to the user without IT every touching it.	Vastly reduced support costs
Due to app Application 'Siloing' vulnerabilities in apps almost never affect the host.	Setup is streamlined	iPad Air w/ Keyboard is about 15% cheaper than PCs
Built-in Patching (e.g. iPhones)	Less equipment to carry, shared charger between USSS issued iPhone	
Automated Application Updates vs manual process w/ SCCM	Better Battery Life than Windows PC	
Remotely Wipe-able when lost (if we get iPads w/ Cellular)	Users, I suspect, would love it	
	Faster deployment of new models (same day as release)	

Mid-term goal: Replace (most) Laptops w/ iPads continued…

With the wireless recompete on the horizon I think we should use that opportunity to reclaim our existing fleet of iPhone XSs and sell them, per GSA & DHS Guidelines to a GSA authorized partner, and use those funds to purchase 500-1000 iPad Air 4th Gen & Magic Keyboards (as shown to the right).

iPad Air (4th Gen) with Magic Keyboard

Costs:
Our standard USSS laptop costs about $1,300
An iPad Air 4th Gen (cellular capable) + Magic Keyboard retails for $1,028
An iPad Air 4th Gen (NON cellular) + Magic Keyboard retails for $898

Setup of new laptops also include a lot of OCIO man hours before delivery to the user, none of which is required for an iPad.
Additionally, every time there is a new model laptop purchased a new/updated image needs to be created – this too costs man hours but also time, meaning by the time the user gets the device in their hands that model may easily be 6-9 months old.

With iPads, we can ship a brand new model direct to the user within days of it being released, for them to setup on their own (via the in-built setup assistant in iOS)

Mid-term goal: Replace (most) Laptops w/ iPads continued…

iPads: Cellular or not

iPad Air (4th Gen) with Magic Keyboard

Long-term Goal: Rearchitect network for iPads (aka greenline-only everywhere)

BLUF: If our users can do all of their work from home – without blue line – then why do we need blue line at all our sites? If "the fleet" becomes mostly iPads, the networking to support it becomes VASTLY less complex, and we can make our network security perimeter exactly 2 sites (HQ & SSE).

USSS iPhones never connect directly to Blue Line, yet function. If we migrate the majority of users to iPads then we can massively simplify & secure USSS network. Effectively all "user networks" (i.e. where current PCs plug into) would become like your home network, with little security – because it's not the network we are trying to secure, it's the data.

With COVID lock downs we've conceptually proven that our users don't need to be "on blue line" to function. So instead of protecting the "network" in 200 sites around the world at our offices – make those networks into completely untrusted networks.

i.e. Zero Trust.

A device "on the network" in a field office would go through the same stack as a device connecting from someone's home.

For the few laptops/desktops that remain, they would VPN back to HQ/SSE, like they do from home today (but, also VPN from their office).

Master Schedule

Teams is deployed.

FORMS – Available at https://forms.office.com/

All O365 Apps (Cloud) – Available at https://www.office.com

Intune – Started, rollout began January 27th

OneDrive – Started, migrating users' "P" drives to One Drive through mid February

Master Schedule (continued)

Exchange Online (aka EXO) – OCIO will begin move in March

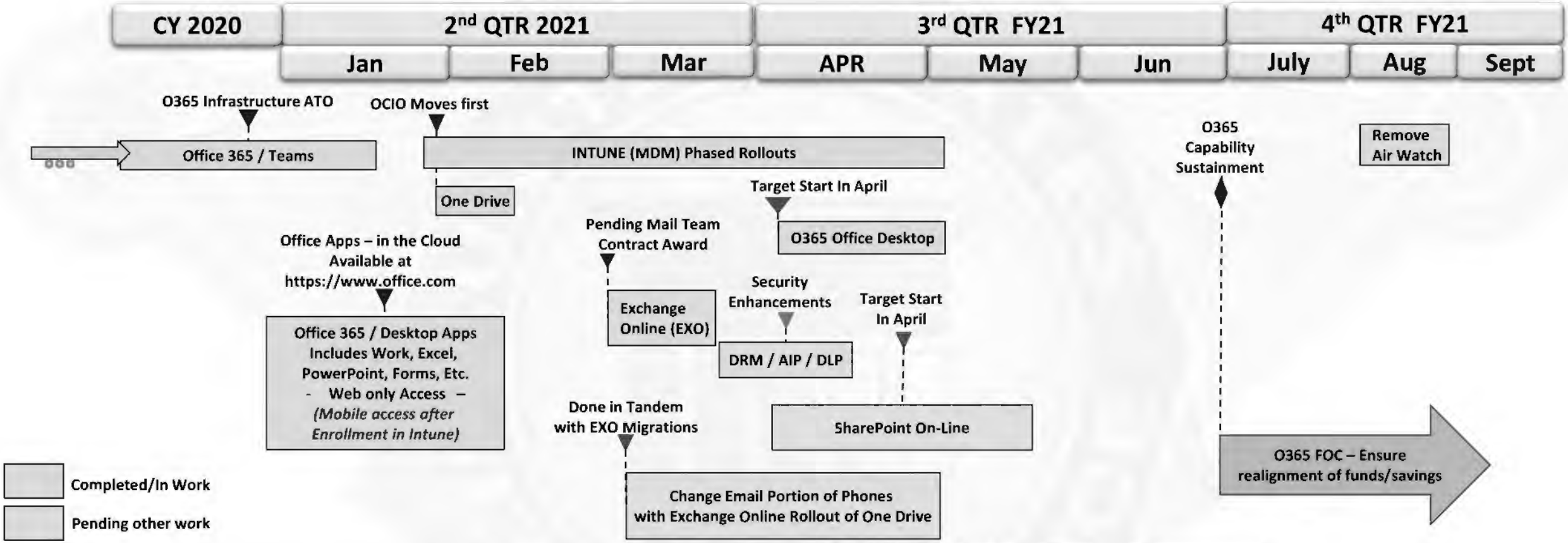
AIP/DRM/DLP* – Once users are moved to EXO, we will begin rollout out the DRM & DLP features.

SharePoint On Line – Rollout Targeted for April

O365 Office desktop – Rollout Targeted for April

O365 Capabilities Rollout Schedule

2 Feb 2021



Program Assumptions

1. Assumes funding will be available for Software and security Product licenses
2. Security Enhancements DRM/AIP/DLP need One Drive and EXO To be completed first

Pending Win 10 OS Desktop deployment

1. Full O365 Office desktop
2. Windows 10 Enterprise Upgrade

USSS Intune Enrollment Quick Start Guide for iPhone & iPad

Rev. Jan 11 2022 RLT

(b)(7)(A)

Enrollment

(b)(7)(A)

Enrollment Continued…

(b)(7)(A)

Enrollment Continued…

(b)(7)(A)

(b)(7)(A)

(b)(7)(A)

USSS Preserve Content Guide for iPhone & iPad

(b)(7)(A)

USSS Preserve Content Guide for iPhone & iPad

(b)(7)(A)

USSS Preserve Content Guide for iPhone & iPad

(b)(7)(A)

USSS Preserve Content Guide for iPhone & iPad

(b)(7)(A)

USSS Preserve Content Guide for iPhone & iPad

(b)(7)(A)

USSS Preserve Content Guide for iPhone & iPad

(b)(7)(A)

USSS Preserve Content Guide for iPhone & iPad

(b)(7)(A)

USSS Preserve Content Guide for iPhone & iPad

(b)(7)(A)

USSS Preserve Content Guide for iPhone & iPad

(b)(7)(A)

USSS Preserve Content Guide for iPhone & iPad

(b)(7)(A)

USSS Preserve Content Guide for iPhone & iPad

(b)(7)(A)

USSS Preserve Content Guide for iPhone & iPad

(b)(7)(A)

USSS Preserve Content Guide for iPhone & iPad

(b)(7)(A)

USSS Preserve Content Guide for iPhone & iPad

(b)(7)(A)

USSS Preserve Content Guide for iPhone & iPad

Table of Contents

Rev. Apr 13 2021 RLT

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

(b)(7)(A)

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

Service Desk at (b)(6); (b)(7)(C)

Headquarters (CIO - Chief Information Officer) (b)(6); (b)(7)(C)

From: CIO
To: (b)(6); (b)(7)(C)
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

(b)(7)(A)

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

Headquarters (CIO - Chief Information Officer) (b)(6); (b)(7)(C)

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

(b)(7)(A)

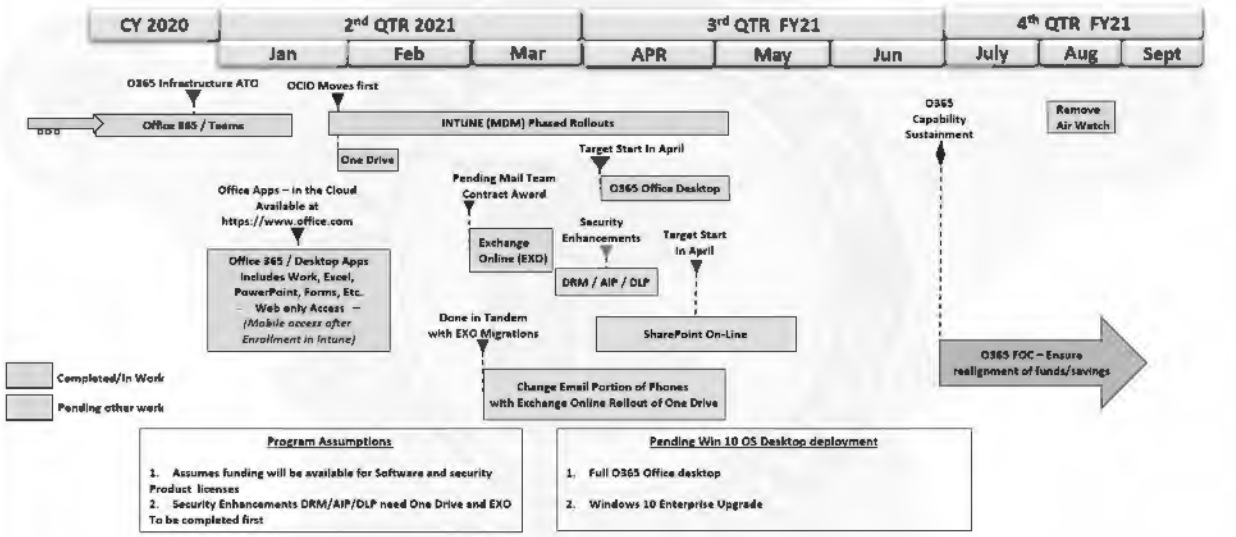
Headquarters (Office of the Chief Information Officer) (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
To:
Cc:
Subject: FW: JAN 6 - OIG
Date: Monday, July 18, 2022 12:42:18 PM
Attachments: O365 Master Schedule and Timeline Slides v2.pptx
MDM – InTune Batch Schedule Notification.msg
image001.png

USSS - Standard Sensitive Info

O365 Capabilities Rollout Schedule

2 Feb 2021



Program Assumptions

1. Assumes funding will be available for Software and security Product licenses
2. Security Enhancements DRM/AIP/DLP need One Drive and EXO To be completed first

Pending Win 10 OS Desktop deployment

1. Full O365 Office desktop
2. Windows 10 Enterprise Upgrade

From: (b)(6); (b)(7)(C)
Sent: Monday, July 18, 2022 11:16 AM
To: (b)(6); (b)(7)(C)
Subject: RE: JAN 6 - OIG

Sir,

Attached are two items that I believe may address item #4.

(b)(6);

Master Schedule

Teams is deployed.

FORMS – Available at https://forms.office.com/

All O365 Apps (Cloud) – Available at https://www.office.com

Intune – Started, rollout began January 27th

OneDrive – Started, migrating users' "P" drives to One Drive through mid February

Master Schedule (continued)

Exchange Online (aka EXO) – OCIO will begin move in March

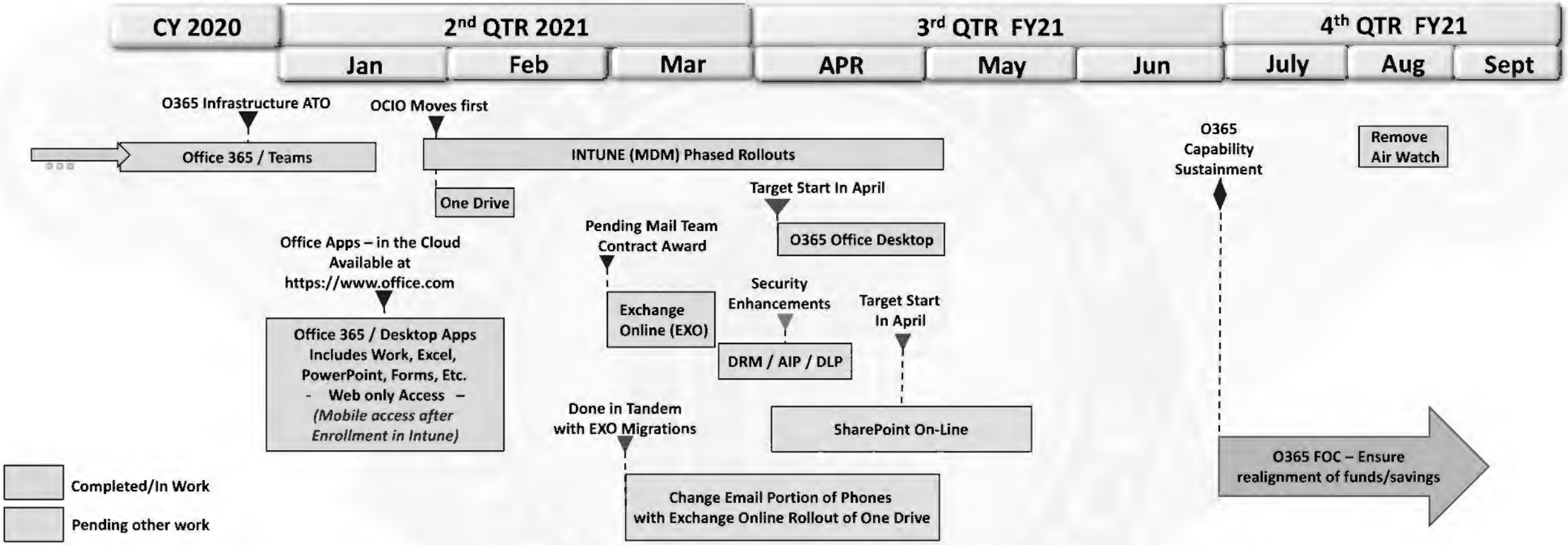
AIP/DRM/DLP* - Once users are moved to EXO, we will begin rollout out the DRM & DLP features.

SharePoint On Line – Rollout Targeted for April

O365 Office desktop – Rollout Targeted for April

O365 Capabilities Rollout Schedule

2 Feb 2021



Program Assumptions

1. Assumes funding will be available for Software and security Product licenses
2. Security Enhancements DRM/AIP/DLP need One Drive and EXO To be completed first

Pending Win 10 OS Desktop deployment

1. Full O365 Office desktop
2. Windows 10 Enterprise Upgrade

From: KEVIN NALLY (CIO)
Sent: Wed, 27 Jan 2021 14:59:25 +0000
To: (b)(6); (b)(7)(C)
Subject: MDM -- InTune Batch Schedule Notification

From: (b)(6); (b)(7)(C)
Sent: Monday, January 25, 2021 3:38 PM
To: (b)(6); (b)(7)(C)
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 Cyber/Thorsheim 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, (b)(6); (b)(7)(C) 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)	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

	(b)(6); (b)(7)(C)			
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		0.4%	Phase 2	

	(b)(6); (b)(7)(C)		
CLT		0.4%	Phase 2
INV		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		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

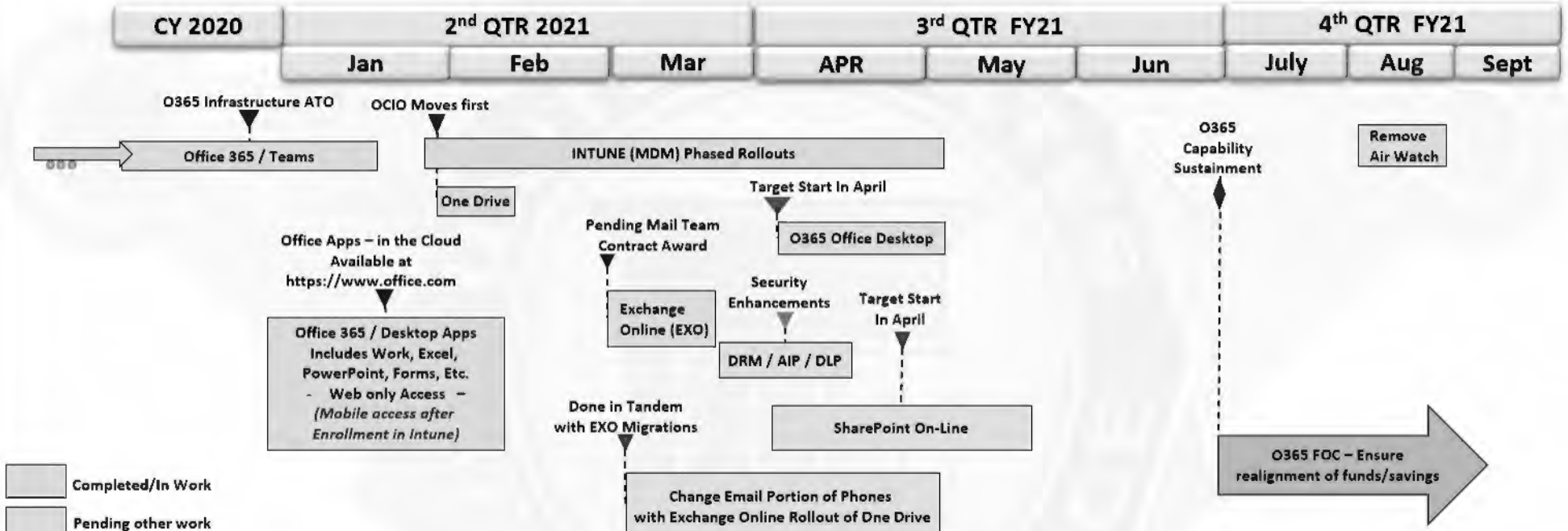
	(b)(6); (b)(7)(C)		
TEC		0.2%	Phase 2
ABQ		0.2%	Phase 2
JAN		0.2%	Phase 2
WPL		0.2%	Phase 2
CLB		0.1%	Phase 2
ERM		0.1%	Phase 2
NHV		0.1%	Phase 2
WPB		0.1%	Phase 2
WPN		0.1%	Phase 2
AUS		0.1%	Phase 2
EAD		0.1%	Phase 2
ABY		0.1%	Phase 2
DAY		0.1%	Phase 2
HRP		0.1%	Phase 2
JFK		0.1%	Phase 2
OMA		0.1%	Phase 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		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	(b)(6); (b)(7)(C)	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		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

	(b)(6); (b)(7)(C)		
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/PAR		0.0%	Phase 2
HKG		0.0%	Phase 2
MAD		0.0%	Phase 2

O365 Capabilities Rollout Schedule

2 Feb 2021



Program Assumptions

1. Assumes funding will be available for Software and security Product licenses
2. Security Enhancements DRM/AIP/DLP need One Drive and EXO To be completed first

Pending Win 10 OS Desktop deployment

1. Full O365 Office desktop
2. Windows 10 Enterprise Upgrade

From: OSP
To: USA
Subject: 101.180 x 200.070 Mandatory DHS Records Management Training
Date: Tuesday, October 22, 2019 9:28:45 AM

//ROUTINE//

FROM: Headquarters (Office of Strategic Planning and Policy)
FILE: 101.080

X200.070
TO: All Secret Service Employees, Contractors, and Personnel Assigned to the Secret Service

SUBJECT: Mandatory DHS Records Management Training

The Office of Strategic Planning and Policy (OSP), via its enterprise Records and Information Management programs, provides the foundation for fulfilling agency mandates found within the Federal Records Act and implementing regulations of the National Archives and Records Administration (NARA).

Consistent with the above authorities, all USSS personnel to include Federal employees, contractors, personnel assigned to joint duty assignments, and interns, have received or will soon receive a notification in the Performance and Learning Management System (PALMS) to complete an annual Records Management course, "OSP1001 DHS Mandatory: Records Management for Everyone."

All current Secret Service employees are required to complete this training no later than January 31, 2020. This training requirement will recur annually and applies to everyone, regardless of whether or not you have already completed a previously assigned records management training course. All new employees (onboarding) after the January 31 date must complete this training within 60 days of reporting for duty with their respective offices.

The course will appear in PALMS under "My Upcoming Learning." If the course does not appear in the "My Upcoming Learning" section, personnel may locate it by entering the name of the course in either of the two search boxes. Employees can locate the OSP1001 DHS Mandatory: Records Management for Everyone training course on the "My Upcoming Learning" section of an employee's PALMS home screen.

- When taking the course, avoid leaving the course open and inactive. You will be prompted to continue in PALMS after 15 minutes of inactivity.
- To verify that your training is complete, scroll down to "My Completed Training," sort by current training completed, then select the completed date column title.
- Training courses completed after the due date in PALMS will be marked as "incomplete" on the employee's transcript and reflected in office statistical reporting.
- This training should take approximately 45 minutes to complete.

If you have any questions regarding this training, please contact Branch Chief (b)(6); (b)(7)(C) in the Office of Strategic Planning and Policy via e-mail or by telephone at (b)(6); (b)(7)(C)

To request technical assistance, please contact the PALMS Help Desk via email at (b)(6); (b)(7)(C) or telephone (b)(6); (b)(7)(C)

Headquarters (Chief Strategy Officer) (b)(6); (b)(7)(C)

From: (b)(6); (OSP)
To: (b)(6); (b)(7)(C) (DIR)
Subject: FW: Draft Official Message on Records Retention
Date: Tuesday, December 8, 2020 10:33:00 AM
Attachments: Record and Document Preservation Requirements OffMsg - 2020-12-02 DRAFT.docx

---

Good morning, (b)(6); (b)(7)(C)

This is the official message draft from the previous email.

Thank you (you're the best),

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

From: (b)(6); (b)(7)(C) (COO)
Sent: Monday, December 7, 2020 4:38 PM
To: (b)(6); (b)(7)(C) (OSP) ; (b)(6); (b)(7)(C) (DEP)
Subject: RE: Draft Official Message on Records Retention

+DEP

(b)(6); (b)(7)(C) and I discussed and raised with Tom Huse as well. While it appears that DUSM is going to send something out along these lines, it is uncertain when that's going to be. There is no risk of getting out in front of the department or anyone else on this . . . by law it's par for the course at the end of every Administration. Attached draft OM has been coordinated btwn OSP, LEG and IGL. All are good with it. Pending your review and any questions, OSP can release . . . as drafted the message is FROM you and me. thanks. -gm

---

From: (b)(6); (b)(7)(C) (OSP) (b)(6); (b)(7)(C)
Sent: Friday, December 4, 2020 5:02 PM
To: (b)(6); (b)(7)(C) (COO) (b)(6); (b)(7)(C)
Subject: Draft Official Message on Records Retention

Good evening, Sir.

Over the last week, we have received letters from both the Hill and NARA reminding us of our responsibilities to retain records, especially in light of the anticipated transition. Based on discussions with both IGL and LEG, we thought it would be a good idea to send out an official message as a reminder to the entire workforce of these responsibilities. In addition to drafting the attached, (b)(6); (b)(7)(C) has been working with a few directorates to talk through the issues.

I had planned to bring this up with you when I had a chance, but I have missed you a couple of times. I am happy to discuss.

Thank you and have a great weekend,

DRAFT

From: Headquarters (Office of the Director) File: 101.081
X 131.010

To: All Offices and Employees

Subject: Record and Document Preservation Requirements

As the 116th Congress and the Presidential administration approach the conclusion of their respective terms, all offices and employees are reminded of their responsibilities to comply with the record preservation obligations set forth in federal law, as well as their ongoing obligations to preserve information relevant to congressional oversight.

All Secret Service employees and officials have a legal responsibility to take appropriate measures to collect, retain, and preserve all documents, communications, and other records in accordance with federal law (including the Federal Records Act and related regulations) until their disposition is authorized. This includes any "information created, manipulated, communicated, or stored" electronically involving official business, correspondence sent using official (and, in limited circumstances, personal) accounts or devices, and records created using text messages, phone-based message applications, or encryption software.

You are likewise obligated to ensure that any information previously requested by Congress – and any other information that is required by law to be preserved – is saved and appropriately archived in a manner that is easily retrievable.

In addition to sanctions contained in the Secret Service Table of Penalties, any employee who conceals, destroys, or attempts to conceal or destroy a federal record requiring preservation may be subject to fine and imprisonment for up to three years.

Comprehensive policy and additional guidance regarding the above obligations may be accessed in the Secret Service Record Programs Management Manual and the Intergovernmental and Legislative Affairs Manual. Also, if and when your office receives a specific document preservation or production order, any employee with questions regarding the above obligations should address them, as applicable, to the following offices/officials:

- Chief Records Officer / Office of Strategic Planning and Policy - (b)(6); (b)(7)(C)
- Congressional Affairs Program / Office of Intergovernmental and Legislative Affairs - (b)(6); (b)(7)(C)
- Office of the Chief Counsel - (b)(6); (b)(7)(C) (See Chief Counsel Homepage for points of contact)

Our agency's records protect the rights and interests of the public, memorialize our successes, hold officials accountable for their actions, and document our nation's history. Sound records management at such critical times ensures today's records will be available for future generations.

Headquarters (Deputy Director)
Headquarters (Chief Operating Officer) (b)(6); (b)(7)(C)

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

MANAGEMENT OF E-MAIL AND OTHER ELECTRONIC MESSAGE RECORDS

Purpose

United States Secret Service (USSS) employees and authorized users routinely create, send, and receive electronic mail (e-mail, e-mails, or e-mail messages) to communicate information related to the mission or administrative matters of the agency.

In accordance with the Federal Records Act, associated regulations of the National Archives and Records Administration (NARA), and Department of Homeland Security (DHS) recordkeeping requirements for retention and disposition, e-mails that are Federal records must be retained in electronic systems that provide the capability to identity, retrieve, and retain the records for as long as they are needed for statutory, regulatory, and business purposes. Secret Service e-mail records are defined as e-mail messages, along with any attachments, and include calendar appointments and tasks managed in the same system as e-mail messages.

In conjunction with Chief Information Officer Manual directives regarding e-mail security, this directive provides an authoritative summary of the records management policies, protocols, and philosophies which govern management of electronic mail ("e-mail") and other types of electronic messages in the Secret Service. It provides guidance to all agency personnel who oversee, administer, or otherwise contribute to the management of agency e-mail. It also establishes a framework for use by all employees (and other authorized users of Secret Service e-mail resources) at all levels of our organization, and reflects expectations and obligations related to managing e-mail as an official Government record.

Scope

This directive applies to e-mail records created or received by authorized Secret Service users on or after December 31, 2016, as well as any prior/earlier messages that have been migrated to the designated USSS e-mail archiving management system, Enterprise Vault ("E-Vault").

Provisions regarding management of records associated with "Capstone" officials are effective upon designation of an individual's account as Capstone/permanent. (The Capstone guidance, developed by NARA to simplify e-mail management, allows agencies to categorize and schedule e-mails based on the role or position of the e-mail account user – with e-mail of top level officials to be preserved for permanent retention.) Once an e-mail user is designated as a Capstone official, the agency must manage all business related e-mails sent or received by that official in a manner that ensures their continued preservation and facilitates their eventual transfer to NARA.

Background and Authorities

Federal agencies and their employees are required to manage e-mail and other types of electronic messaging records in accordance with the Federal Records Act and 36 CFR Chapter XII Sub-chapter B.

In 2013, NARA issued Bulletin 2013-02 "Guidance on a New Approach to Managing Email Records" to supplement these statutory and regulatory authorities. In 2014, NARA and the Office of Management and Budget (OMB) jointly issued a "Managing Government Records Directive" (M-12-18). This directive requires agencies to manage both permanent and temporary e-mail records in an accessible electronic format by December 31, 2016, based upon specific criteria developed by NARA.

The criteria and NARA's corresponding Government-wide guidance was issued as General Records Schedule (GRS) 6.1, *Email Managed under a Capstone Approach.* Commonly known as *Capstone,* this guidance attempts to eliminate the longstanding, paper-based "print-and-file" approach to e-mail recordkeeping by allowing agencies to:

- Base e-mail records retention on the mailbox owner's role in the agency, rather than on the content of each e-mail record.
- Develop mechanisms for organizing and storing e-mails (and their attachments) in their native electronic format, according to established schedules (based on program, mission, or agency need) and for the duration of their retention periods.
- Implement procedures that address retirement, transfer, or other employee separation scenarios to ensure Government records are preserved, and non-records are culled.

36 CFR § 1236.22 also establishes "requirements for managing electronic mail records." Key provisions of this regulation include the following:

- The names of sender and all addressee(s) and date the message was sent must be preserved for each electronic mail record in order for the context of the message to be understood.
- Attachments to electronic mail messages that are an integral part of the record must be preserved as part of the electronic mail record or linked to the electronic mail record with other related records.

Finally, the Presidential and Federal Records Act Amendments of 2014 (Public Law 113-187) modernizes records management by focusing more directly on electronic records. The amendments include provisions which strengthen the Federal Records Act by:

- Expanding the definition of Federal records to clearly include electronic records.
- Confirming that Federal electronic records will be transferred to NARA in electronic form.
- Granting the Archivist of the United States final determination as to what constitutes a Federal record.
- Authorizing (in particular situations) the early transfer of permanent electronic Federal records to the National Archives, while legal custody remains with the agency.

The Department of Homeland Security has addressed the above via DHS Directive 142-03, Email Usage, which serves as a foundation for this Secret Service directive.

Types of Electronic Messages

Electronic messages sent or received by Secret Service employees generally can be categorized as one of the following message types. Additional discussion is contained in the DHS online training course entitled "Electronic Records Management."

Records

Messages having potential direct impact on the Federal government, its employees, and citizens; messages relating to budget, personnel, supply, and similar support functions. This includes messages which:

(a) Have been identified as subject to current or pending litigation.

(b) Document the persons, places, things, or matters dealt with by the agency.

(c) Facilitate action by agency officials and their successors in office.

(d) Make possible a proper scrutiny by the Congress or other duly authorized agencies of the Government.

(e) Protect the financial, legal, and other rights of the Government and of persons directly affected by the Government's actions.

(f) Document the formulation and execution of basic policies and decisions and the taking of necessary actions, including all substantive decisions and commitments reached orally (person-to-person, by telecommunications, or in conference) or electronically.

(g) Document important board, committee, or staff meetings.

Draft documents that are circulated on electronic mail systems also may be records if they meet the criteria specified above.

Messages sent or received as a "carbon copy" (cc) or "For Your Information" (FYI), etc. shall generally be considered records, even if no immediate action is expected/required of the recipient. (The awareness provided generally implies there is a knowledge or understanding required relevant to an assigned business function, even if only for contingency purposes.)

Non-Records

Messages that are kept only for informational or reference purposes; duplicate copies of messages that have been filed as records elsewhere; earlier drafts of messages or partial messages that are used for template or discussion purposes which lead to creation of a final record; email blasts originating from other USSS accounts.

Personal

Messages sent or received by an individual under "limited personal use" provisions (see ITG-03(06)) that are not used to conduct agency business, such as employee copies of personnel actions; materials regarding membership in professional organizations; personal correspondence (such as from a child care provider) that generally must occur during business hours; system correspondence from the Thrift Savings Plan, FSAFeds, and unique other records associated with an individual's service with application beyond the workplace.

If a message includes or encompasses personal or quasi-personal issues but also relates to official business considerations (e.g., leave, training requests, etc.) the message must be treated as a record.

Policy

The Secret Service manages e-mail records under the following Capstone approach, based on the role of the e-mail account user rather than on the content of each e-mail record.

E-Mail Records of Designated Capstone Officials

"Capstone Officials" are top level executives and senior staff of a Government agency, as well as other designated program officials described in General Records Schedule 6.1. **A list of USSS Capstone Officials appears in Appendix 1 of this directive.** Capstone Officials include any officials serving in an acting capacity for these positions for longer than 60 days.

- Business e-mails (including attachments) and related records sent or received by Capstone Officials are permanent records and may not be deleted. (E-mail records include e-mail messages and attachments, as well as calendar appointments and tasks managed via the agency e-mail application platform.) The Component must maintain these e-mails for 15 years after the end of the e-mail user's tenure and then transfer the e-mails to NARA in accordance with the schedule.

- Non-record e-mails are those that do not meet the criteria of a Federal record and are so designated regardless of whether a Capstone Official sends or receives them. Non-record e-mails should be deleted or "culled" as soon as practical. (See "Culling of E-Mail" provisions later in this directive.)

    - Non-record e-mail includes those sent or received as *limited personal use* correspondence (see Office of the Director Manual section ITG-03(06) for more information). Users should delete personal e-mails as soon as possible after receipt or save to a folder marked "Personal" in their electronic mailboxes.

  Non-business e-mails that are not culled will be transferred to NARA at the end of the agency retention life cycle.

- Business e-mails (including attachments) that are sent or received by Capstone Officials may also be duplicated outside the e-mail system (either in electronic format or in hard copy, if appropriate) and retained with the associated administrative or program record in accordance with the approved records retention schedule for that subject (e.g., case files, survey reports, project files, etc.) (Note: duplicate e-mail copies filed in this manner will be disposed of when the associated file reaches the end of its retention period.)

- Legal Holds/Preservation Management: Upon notice of a legal requirement to hold or preserve records, any e-mail associated with the hold will be retained until the legal requirement is lifted. The hold will apply regardless of the record's status and will supersede the records retention schedules.

E-Mail Records of Secret Service Official Messages

Official Message accounts are associated with an office/division-level organizational unit, rather than a person. In contrast with the more informal, unstructured, and often pre-decisional content that generally characterizes person-to-person e-mail, Official Messages serve to formally document historically significant communications and other information of enduring value.

The Official Message system provides a foundation for fulfilling agency mandates established in title 44 United States Code chapter 29 "to achieve adequate and proper documentation of the policies and transactions of the Federal Government," and provides a designated Secret Service mechanism to:

- Transmit documentation of significant agency decisions and commitments reached orally, in person-to-person e-mail, by telecommunications, or in conference and not otherwise documented in agency files;
- Provide background or context for a draft action memorandum, directive, etc., if the Official Message adds to a proper understanding of the formation or execution of an agency action;
- Convey information of value on important agency activities, if the Official Message adds to a proper understanding of agency operations and responsibilities;
- Facilitate action by Secret Service officials and their successors;
- Document important meetings; and
- Protect the financial, legal, and other rights of the Government and of persons directly affected by the Government's actions.

Official Messages are transmitted with file codes that reflect the type of subject matter, and contain signature lines for the cognizant USSS official and his/her office. A person-to-person message containing the type of information described above is generally expected to be retransmitted as an Official Message.

Secret Service Official Messages of Directorate level offices and the Office of the Director, sent/received between January 1, 2001 and December 31, 2017, will be retained as "Capstone" permanent and transferred to NARA in 15 years. All other Secret Service Official Messages are disposable when 7 years old, but longer retention is authorized if required for business use.

E-mail Records from all Other Accounts Not Designated as Capstone Permanent

E-mail records (to include e-mail messages and attachments, as well as calendar appointments and tasks managed via the agency e-mail application platform) of all other Secret Service e-mail accounts will be retained for 7 years, at which time they may be disposed of unless needed for other business purposes or the subject of a litigation hold.

- Non-record E-mails: Non-record e-mails are those e-mails that do not meet the criteria of a Federal record and are so designated regardless of whether a Capstone Official sends or receives them. Non-record e-mails should be deleted or "culled" as soon as practical. (See "Culling of E-Mail" provisions later in this directive.)

  Non-record e-mail includes those sent or received as *limited personal use* correspondence (see Office of the Director Manual section ITG-03(06) for more information). Users should delete personal e-mails as soon as possible after receipt or save to a folder marked "Personal" in their electronic mailbox. (See "Folder Structure" provisions on next page.)

- Business e-mails (including attachments) that are sent or received by Capstone Officials may also be duplicated outside the e-mail system (either in electronic format or in hard copy, if appropriate) and retained with the associated administrative or program record in accordance with the approved records retention schedule for that subject (e.g., case files, survey reports, project files, etc.) (Note: duplicate e-mail copies filed in this manner will be disposed of when the associated file reaches the end of its retention period.)

- Legal Holds/Preservation Management: Upon notice of a legal requirement to hold or preserve records, any e-mail associated with the hold will be retained until the legal requirement is lifted. The hold will apply regardless of the record status and supersede records retention schedules.

Folder Structure

To supplement organization of messages in the top level ("root") e-mail folder, creating subfolders with an appropriate hierarchy (e.g., establishing folders based on fiscal or calendar year; by project/task force name; subject to a litigation holds in a particular case; creating subfolders based on Master File Classification Code (MFCC) number; etc.) is recommended.

In addition, all employees (not only those designated as Capstone Officials) are encouraged to manage their e-mail by creating these additional sub folders within their e-mail application (e.g., Microsoft Outlook) Inbox and Sent Items:

- **Non-Records**
- **Personal**

Once established in the user's e-mail application, these folders will be replicated in the user's long term e-mail archive as well. (See "Enterprise Vault (E-Vault)" provisions below.)

Additional notes:

- Users are reminded that even for e-mail sent or received under limited personal use provisions, there is no expectation of privacy.

- For record-driven compliance activities like FOIA, it may be reasonable to exclude Non-Records and Personal folders from corresponding searches. However, for inquiries involving legal discovery or investigative matters, <u>all</u> folders may be examined for evidentiary purposes, and responsive materials provided to the cognizant requesting authorities. Should responsive materials be located in those folders, they shall be treated as records (at least until the litigation is resolved) and moved to a folder created for that purpose.

- If an e-mail/e-mails have been identified as being subject to a litigation hold, they must be treated as records – even if the message(s) fall within the category of "non-record" or "personal." Optimally, this is accomplished by creating a folder corresponding to the litigation freeze order and copying the e-mail(s) to that folder, and retaining them there until the freeze is lifted.

Culling of E-Mail

Culling refers to the removal – or otherwise excluding from capture – of non-record or personal messages and attachments. Culling typically includes the removal of spam, e-mail blasts originating from other accounts (such as agency-wide communications), and personal materials (such as "limited personal use" e-mails to family members not related to agency business (see Office of the Director Manual section ITG-03(06) for more information)). Culling may be manual, automated, or a hybrid of both. Agencies are expected to ensure that the e-mail of Capstone officials (permanent accounts) is culled to the greatest extent appropriate before transfer to NARA.

Questions regarding the appropriate designation of an e-mail as record, non-record, or personal must be presented to the Office of the Chief Counsel for further coordination with the USSS Chief Records Officer, as appropriate.

Enterprise Vault (E-Vault)

E-Vault is a software application that is currently being utilized by the Secret Service to allow centralized storage, backup, and preservation of e-mail data for more than 180 days. E-Vault stores e-mails and their attachments, and is configured to ingest e-mail messages from local (e.g., Microsoft Outlook Personal Storage Table or .PST) files located outside of the e-mail server.

The Secret Service uses E-Vault as an "electronic file cabinet" that can securely store messages for extended periods of time. **E-Vault helps each authorized Secret Service user fulfill his/her recordkeeping responsibilities, as required by law, by providing a stable medium for longer term retention and by facilitating the aggregation of permanent records for designated Capstone officials.** It also allows authorized program managers and compliance officials to leverage the information contained in Secret Service e-mail to fulfill operational and legal requirements.

Unlike E-Vault, the Secret Service e-mail server that sends and receives messages each day has only limited space to store and retain those messages. Under the Secret Service's concept of operations **any message sent or received by an employee will be available on the Secret Service e-mail server for 30 days, after which it will be automatically migrated to E-Vault**, under a corresponding E-Vault folder designated for the individual user account, unless deleted during the culling process.

Additional Considerations

- E-Vault does not distinguish between personal and business messages, nor can it automatically infer temporary or permanent retention of stored messages. As noted above, this underscores the importance of each employee or office custodian's deliberate choice on whether (and how) to file the message as a record, non-record, or personal item.

- E-Vault may prompt users to not delete or move a message once it has been placed in the "vault" folder. Even though prompted not to move or delete (cull) the messages, a user still has the ability to complete both actions, **and must perform them in order to fulfill records management responsibilities.**

- Use of E-Vault does not replace existing business practices requiring retention of e-mail with other related records in established recordkeeping systems. When business needs require e-mail records be retained within another recordkeeping system (either paper-based or electronic), users should ensure copies are created and provided for inclusion with those files. (Example: a message stored in E-Vault relating to a particular case file, should be duplicated and filed for inclusion in that case file.)

- For non-Capstone personnel, users are required to practice the same planning and diligence in deleting messages that have reached the end of their retention period as they would with corresponding paper files. Generally, this is done at the commencement of a new calendar year – e.g., review your E-Vault folders for any messages older than 7 years, and delete them if you no longer need them for business/reference purposes. (**NOTE:** Although E-Vault will be configured to allow at least 7 calendar years' worth of e-mail for each employee, it is permissible for active employees to retain messages older than 7 years. Although retention of e-mail messages for longer than 7 years is authorized if needed for business/reference purposes, this practice should be the exception – not the rule.)

- E-Vault storage will not be limited for Capstone officials, to facilitate the eventual production from E-Vault for transfer to NARA as permanent records in its native format, as required by NARA.

E-Vault Capability for Official Messages

Effective January 1, 2018, Official Messages sent to or received by an Official Message account also will be migrated to a corresponding E-Vault account. To access these legacy messages, contact your office personnel with designated Official Message responsibilities.

Local .PST (Personal Storage Table) Files

Only authorized personnel who require the ability to access and create .pst files for vital records, regulatory compliance, litigation, and other compelling purposes will have the capability of creating and using local .pst files.

Journaling

To support various initiatives related to Information Assurance, Insider Threat/Internal Security, Counterintelligence, etc., the Secret Service may undertake or request "journaling" of e-mail (i.e., capture of all e-mail traffic as it is sent/received, and preservation in a separate storage medium). While this practice may support necessary operational activities, it has the potential of undermining appropriate records management practices and disposition – e.g., inappropriately preserving a copy of an e-mail record that was properly disposed of/deleted by its business owner. This scenario could have grave ramifications from a FOIA, privacy, or litigation perspective.

Therefore, any entity engaged in journaling must ensure that retention of journaled data does not exceed the NARA authorized time frame of 180 days for generic use on an e-mail server unless otherwise dictated by a specific legal hold or administrative/investigative inquiry. Contact the Office of the Chief Counsel for additional clarification.

Closed/Dormant E-Mail Accounts

Since record material may exist within individual e-mail accounts on the e-mail or E-Vault servers, when those accounts are closed it is necessary to ensure that: 1) existing record material is preserved/properly migrated; 2) non-record material is purged; and 3) technical measures are applied that will prevent new records from unintentionally being created. Likewise, any e-mail archive that has been established in E-Vault under an individual's name must be migrated to a new custodian. Generally, these issues arise when employees separate from their positions or transfer to new program areas as their primary assignment. As such, the following standards for handling separating employees should be incorporated into corresponding out processing policies and required checklists.

Voluntary/Planned Separations (e.g., Resignations, Transfers, Retirements)

Supervisors:

- Provide/review briefing on records management responsibilities and discuss with separating employee.
- Determine if the separating employee's e-mail is subject to a legal/litigation hold; if so, ensure employee has contacted the Office of the Chief Counsel.
- Determine if separating employee is designated as a Capstone Permanent Official; if so, ensure that the Capstone employee has appropriately culled any non-record material.
- For all e-mail that has not migrated to E-Vault and which remains on the e-mail server, determine which record e-mails should be transferred/forwarded to the supervisor or other employees and which non-records should be deleted. For non-Capstone employees, their corresponding E-Vault account will remain locked and inaccessible unless permissions are granted based on legal, investigative, or other compliance-related bases.
- Ensure the employee notifies internal/external peers, colleagues, and other points-of-contact of his/her separation in advance of the separation. Since the user's e-mail account will be deactivated, there will be no ability to establish an "out of office" message that will autoreply to incoming messages, nor will those intended messages be preserved or forwarded to others. The employee should:
    - Indicate he/she will be leaving the department/agency/component/program
    - Advise that inquiries be directed to the appropriate agency/program contact
- Inactivate, delete, or revise any miscellaneous user IDs, routers, and lists which include the separated employee as a member.

Employees:

- Since your e-mail account will be deactivated, there will be no ability establish an "out of office" message that will autoreply to incoming messages, nor will those intended messages be preserved or forwarded to others You must notify internal/external peers, colleagues, and other points-of-contact of your separation in advance to:
    - Indicate you are leaving the department/agency/component/program
    - Advise that inquiries be directed to the appropriate agency/program contact

- Close out e-mail accounts to ensure all personal e-mail messages and non-record materials have been deleted, and all record materials have been forwarded to a new custodian, as appropriate. **If subject to a litigation hold, employees must contact the Office of the Chief Counsel prior to closing out any e-mail accounts.**

- Capstone Permanent Officials must ensure that their e-mail has been culled to remove any personal or non-record material in preparation for eventual transfer to NARA.

CIO E-Mail Support:

- Deactivate the e-mail account and ensure sustainability in E-Vault for the duration of required retention.
    - For non-Capstone officials, configure autodelete parameters so any message older than seven years is automatically purged, unless the Office of the Chief Counsel has established a litigation freeze or other hold.
    - For Capstone Permanent Officials, ensure account contents are preserved for 15 years after employee separation. At the end of this time period, coordinate review by Office of the Chief Counsel and Chief Records Officer in order facilitate the creation of transportable medium for transfer to NARA.

Involuntary/Unplanned Separations (e.g., Terminations, Death or Incapacitation, etc.)

Supervisors:

- Determine if employee e-mail is subject to a legal/litigation hold; if so, contact the Office of the Chief Counsel to determine the parameters of the hold.
- Engage IT support and other officials (e.g., Office of the Chief Counsel) as appropriate to determine if access to employee's messages should be obtained.
- For employee's e-mail that have not migrated to E-vault and remain on the e-mail server, determine if record e-mails/messages should be transferred/forwarded to the supervisor or other employees and if non-records should be deleted. For non-Capstone employees, their corresponding E-Vault account will remain locked and inaccessible to others unless permissions are granted based on legal, investigative, or other compliance-related bases.
- For E-Vault archives, determine who should be the new custodian of archived records (if applicable)
- To the extent practical/appropriate, notify internal/external peers, colleagues, and other points-of-contact of employee's separation to:
    - Indicate the employee has separated from the department/agency/component/program
    - Advise that inquiries be directed to the appropriate agency/program contact

Since the user's e-mail account will be deactivated, there will be no ability to establish an "out of

office" message that will autoreply to incoming messages, nor will those intended messages be preserved or forwarded to others.

- Inactivate, delete, or revise any miscellaneous user IDs, routers, and lists which include separated employee as a member.

CIO E-Mail Support:

Following consultations described above (typically initiated by the employee's supervisor), and as deemed appropriate by cognizant directorate official, Chief Counsel, and Chief Records Officer:

- Deactivate e-mail account and ensure sustainability in E-Vault for the duration of required retention.
    - For non-Capstone officials, configure autodelete parameters so any message older than seven years is automatically purged, unless the Office of the Chief Counsel has established a litigation freeze or other hold.
    - For Capstone Permanent Officials, ensure account contents are preserved for 15 years after employee separation. At the end of this time period, coordinate review by Office of the Chief Counsel and Chief Records Officer in order facilitate the creation of transportable medium for transfer to NARA.

Other Electronic Messages (e.g., Text, Chat, Instant Messages)

It is the policy of the Department of Homeland Security (DHS) that accountable and comprehensive records management is essential. Unlike e-mail, however, many current messaging technologies do not include an electronic records management capability that can provide storage and access to computerized Federal records and other information for a sustained time period.

For this reason, all employees must give special consideration to when, and how, they use non e-mail based electronic messaging technologies such as text, chat, and instant messaging.

- If the electronic message sent or received is transitory in nature with no administrative, legal, fiscal, or archival value; is a limited personal use message; or is a non-record, then the message can be deleted or allowed to expire at the discretion of the user. Examples include:
    - A message to a co-worker regarding a lunch order
    - A message that a printer is offline (or back online)
    - A severe weather alert or "Amber Alert" sent by external agencies

- **USSS employees are prohibited from conducting official business using chat, text, or instant messaging unless they take any additional steps that may be appropriate to establish and maintain a separate record of the communication.** Much like in-person or telephonic conversations, if substantive business communications between USSS employees are made via chat/text/instant message, they must be formally transacted/documented in a more

permanent medium (such as an e-mail or written memorandum). Examples of affected messages include:

- Messages sent or received in emergency or exigent circumstances
- Messages sent or received in a law enforcement (e.g., undercover) capacity

In most cases, the sender and/or the recipient can meet this obligation by capturing the content of a message, pasting it into an e-mail, and sending the e-mail to a USSS e-mail address within 20 days of the creation or transmission of the record. This will allow the content to be managed consistent with a user's Capstone or non-Capstone status.

- On a computer: Press the [Control] and [Print Screen] to capture an image of the screen that can be pasted into an e-mail; or block the text, copy it, and paste it into an e-mail.
- On agency issued smartphones, press the designated key/button combination to capture a screen shot. (E.g., press the sleep/wake/power button (at the top-right or on top of your device) and press the Home button (below the screen) at the same time. The screen shot will be stored in your Photos folder and can be sent from your smartphone as an attachment to a USSS e-mail.)

Use of Text, Chat, or Instant Messages in Protective Operations

(b)(7)(D); (b)(7)(E)

Use of Text, Chat, or Instant Messages in Investigations

(b)(7)(D); (b)(7)(E)

(b)(7)(D); (b)(7)(E)

Non-USSS / Non-DHS E-Mail Messaging Accounts

The following provisions of DHS Directive 142-03 apply to non-DHS e-mail accounts:

- DHS employees may not use non-DHS e-mail accounts to create or send e-mails that constitute DHS records. In case of an exigency, employees may use a non-DHS e-mail account, but thereafter must ensure the e-mail record is submitted to an official DHS e-mail account within 20 days (by forwarding or cc'ing of the DHS account). In cases of intentional violation of this requirement, disciplinary action as determined by the appropriate supervisor is authorized (Title 5, U.S.C., Chapter 75). Once the employee has ensured the capture of the e-mail information in the DHS account, the DHS e-mail must be removed from the non-official e-mail account.

- DHS employees who are on detail to another agency may use that agency's e-mail system to send e-mails during the course of their detail. This permission also extends to task force, working group, or other project or application-based e-mail accounts established by another Federal agency for use by DHS employees.

- Auto-forwarding or redirecting of DHS e-mail to any e-mail address outside of the .gov or .mil domain is prohibited. DHS employees may manually forward individual messages after determining that the risks or consequences are minimal.

- The use of Internet Webmail (e.g., Gmail, Yahoo, and AOL) or other personal e-mail accounts is not authorized over DHS-furnished equipment or network connections.

Appendix A:
USSS Capstone E-Mail Retention Schedule Provisions

E-mail Managed under a Capstone Approach – U.S. Secret Service
(Citation: GRS 6.1-0087-2018-0001)

This schedule applies to all e-mail, regardless of how the e-mail messages are managed or what e-mail technology is used. E-mail, in the context of this schedule, also includes any associated attachments. This schedule may apply to records affiliated with other commonly available functions of e-mail programs such as calendars/appointments, tasks, and chat.

Records Description	Disposition Instruction	Disposition Authority
E-mail of Capstone officials. Capstone Officials are senior officials designated by account level or by e-mail addresses (whether the addresses are based on an individual's name, title, a group, or a specific program function) and consist of the following personnel: • Director • Deputy Director • Chief Operating Officer • Assistant Director-Protective Operations • Assistant Director-Investigations • Assistant Director-Intergovernmental and Legislative Affairs • Assistant Director-Professional Responsibility • Assistant Director-Strategic Intelligence and Information • Assistant Director-Training • Chief Technology Officer • Chief Financial Officer • Chief Strategy Officer • Chief Human Resources Officer • Chief Information Officer • Chief Counsel • Chief Integrity Officer • Director of Communications and Media Relations This includes those officials in an acting capacity for any of the above positions longer than 60 days. The agency may also include individual emails from otherwise temporary accounts appropriate for permanent disposition in this category.	**Permanent.** Cut off in accordance with agency's business needs. Transfer to NARA 15 years after cutoff, or after declassification review (when applicable), whichever is later.	GRS 6.1, item 010

If a Capstone official has more than one agency-administered e-mail account, this item applies to all accounts. If a Capstone official has an e-mail account managed by other staff (such as personal assistants, confidential assistants, or administrative assistants), this item applies to those accounts. This item applies to all e-mail regardless of the address names used by the Capstone official for agency business, such as nicknames or office title names Not media neutral; applies to records managed in an electronic format only.		
Official Messages. Accounts established for each Secret Service office which provide formal accounts of Executive level decisions and communications, as well those at other managerial levels within the organization.		
• USSS Official Message Accounts - Directorate level and above (2001-2017)	**Permanent.** Cut off in accordance with agency's business needs. Transfer to NARA 15 years after cutoff, or after declassification review (when applicable), whichever is later.	GRS 6.1, Item 010
• Other USSS Official Message Accounts	**Temporary.** Delete when 7 years old, but longer retention is authorized if required for business use.	GRS 6.1, Item 011
E-mail of Non-Capstone Officials. E-mail of all other officials, staff, and contractors not included above.	**Temporary.** Delete when 7 years old, but longer retention is authorized if required for business use.	GRS 6.1, Item 010

SECRET SERVICE RECORDS MANAGEMENT PROGRAM

Introduction

Title 44, Chapter 31 of the United States Code (U.S.C.) requires the head of each Federal agency to make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency. This statute also furnishes information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities.

All records created or received by an official or employee of the United States Secret Service (USSS) in the course of conducting Government business are official records and are property of the United States Government. No person attains a proprietary interest in any official record, or acquires custody or possession of the record, by virtue of his/her position as an official or employee (44 U.S.C., 2905 and 3106). The maximum penalty for the willful and unlawful destruction, damage, removal, or alienation of Federal records is a $2,000 fine, 3 years in prison, or both (U.S. Criminal Code, Title 18, U.S.C., 2071).

In order to control the creation, use, maintenance, and disposition of all Federal records, regardless of format or subject matter, every Federal agency must, by law, have an active and continuing records management program governed by requirements established by the National Archives and Records Administration (NARA), the General Services Administration (GSA), the Government Accountability Office (GAO), and the Office of Management and Budget (OMB). Accordingly, the Office of Strategic Planning and Policy (OSP) houses the Chief Records Officer (CRO) of the U.S. Secret Service.

One important aspect of records management is deciding when to dispose of records. The law recognizes this and states that through authorized records disposition schedules, only the Archivist of the United States has legal authority to: (a) approve the destruction of Federal records, and (b) authorize accession of permanent records into the National Archives for historic preservation. With the oversight of the CRO, and in collaboration with the Department of Homeland Security (DHS) Records Officer, OSP develops retention and disposal instructions that meet Secret Service needs and ensures approval from the Archivist of the United States is secured.

Policy

It is the policy of the Secret Service to comply with the various statutes, regulations, and Department-level guidance governing the management and disposition of Federal records, and to adhere to the legal mandate of reducing the Federal paperwork burden to the minimum practical level.

Objectives

The objectives of the Secret Service Records Management Program are to:

1. Provide life cycle management awareness and procedures for the systematic identification, maintenance, storage, retrieval, and destruction of Secret Service information recorded on any medium (paper, electronic, or any other);

2. Ensure the Director and staff have the information needed to accomplish the Secret Service's mission; that they have it when and where needed, and in a usable format;

3. Ensure records related to matters involved in legal proceedings are retained until the Chief Counsel authorizes resumption of normal dispositions;

4 Preserve records vital to continued operations of the Secret Service; vital to provide for continued protection of the rights and interests of the Federal Government, Secret Service employees, and the public; as well as preserve those records having permanent value;

5. Provide periodic survey, analysis, and evaluation of records holdings, systematic records disposal, procedures, and techniques employed to promote effective utilization of file space and equipment, supplies, and human resources associated with records management; and

6. Control the retention and disposition of records to ensure records of continuing value are preserved, but that valueless or noncurrent information is disposed of or transferred to storage in a timely manner.

Authorities/References

Management of Federal records will comply with statutes and other regulatory guidance prescribed or recommended by the National Archives and Records Administration (NARA). Following are some, but not all, of the statutes, regulations, NARA guidelines, and other policies the Secret Service applies in its recordkeeping and records management practices.

- Federal Register (44 U.S.C. Chapter 15)
- National Archives and Records Administration (NARA) (44 U.S.C. Chapter 21)
- Presidential Records (44 U.S.C. Chapter 22)
- Records Management by NARA (44 U.S.C. Chapter 29)
- Records Management by Federal Agencies (44 U.S.C. Chapter 31)
- Disposal of Records (44 U.S.C. Chapter 33)
- Public Law 113-187, The Presidential and Federal Records Act Amendments of 2014
- Department of Homeland Security Directive 141-01, Records and Information Management (and associated Instructions)

Purpose and Scope

This directive prescribes policy, procedures, standards, and responsibilities for implementing and administering the Secret Service Records Management Program. This directive applies agency wide to both program and administrative records.

Definitions

Accession - A shipment of records sent to a Federal or commercial records center, consisting of a series of records having the same disposal authority. Used as a verb, accession is the formal action acceptance of records for storage in a Federal records center.

Accountable Officers' Accounts - These are specific records supporting disbursements or collections of money, prepared by accountable officers and required by the Government Accountability Office (GAO) to be maintained for audit.

Adequate and Proper Documentation - A record of the conduct of Government business that is complete and accurate to the extent required to document the organization, functions, policies, decisions, procedures, and essential transactions of the agency and that is designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities.

Administrative Records - Records relating to budget, personnel, supply, and similar housekeeping records accumulated or generated within an office that document the internal functions common to most offices, as opposed to those that document the primary mission of the office. These records accumulate because an office exists, not why it exists.

Appraisal - The process of determining the value and the disposition of records, based upon their current administrative, legal, and fiscal use; their evidential and informational or research value; their arrangement; and their relationship to other records.

Archival Value - The determination through appraisal that records are worthy of permanent preservation by an archival function; sometimes referred to as historical or continuing value.

Archivist - A person responsible for, or engaged in, one or more of the following activities in an archival repository: appraisal and disposition, accessioning, preservation, arrangement, description, reference service, exhibition, and publication. Also, the Archivist of the United States, the head of NARA.

Authenticity - A condition that proves a record is authentic and/or genuine based on its mode, form, state or transmission, and manner of preservation and custody.

Case Files - Records, regardless of media, documenting a specific action, event, person, place, project, or other matter. They are usually filed by a unique name or number. A particular event or action causes the case to be closed and become inactive.

Classified Records - Records designated as "Top Secret," "Secret," or "Confidential" which are restricted to processing, use, or handling by cleared individuals. They require stringent accountability, control, and safeguard measures.

Collections of Records - Selected records identified by the Secret Service or National Archives requiring special safeguard to ensure preservation for historical and/or legal purposes. Some examples are the 911 files; Hurricane Katrina records; and records related to substantial high-level investigations or decisions affecting the Secret Service.

Comprehensive Records Schedule - A schedule or collection of schedules based on disposition authorities, approved by NARA, and issued as a directive or manual to cover all the records of an independent agency or department, or those of a bureau, service, or office within a department.

Convenience Files - Nonrecord copies of correspondence, completed forms, and other documents kept solely for ease of access and reference.

Current Files Area (CFA) - Area and official space where current, day-to-day work is done and current records are created and maintained.

Current Records - Records or files presently in the physical custody of organizational units, the maintenance of which is required to conduct current work.

Custody - The guardianship or control of records including both physical possession and legal title responsibility.

Cutoff (COFF) - Breaking or ending files at regular intervals, usually at the close of a fiscal or calendar year, to permit their disposal or transfer in complete blocks and, for subject correspondence files, to permit the setting up of new files. Case files are generally cut off at the end of the calendar year in which the case is closed.

Description - In records management, the process of giving a written account of the contents and characteristics of a record series or system.

Digitization - The process of converting materials from an analog medium (such as paper) to an electronic or machine readable format.

Disposition - The action taken regarding Federal records after they are no longer required to conduct current Agency business. It means the retirement, transfer, donation, or destruction of records.

Disposition Authority (AUTH) - The legal approval authorizing an agency to carry out the disposal of temporary records, or to transfer permanent records to the National Archives. A sample disposition authority: (NC1-87-78-2, Item No. 17).

Disposition/Records Schedules - The legal authority to dispose of records. Schedules contain the records description and disposition instructions approved by the National Archives and Records Administration (NARA).

Electronic Record - Any information recorded in a format that only a computer or other electronic device can process and that satisfies the definition of a Federal Record (Refer to Professional Responsibility, section MNO-06(07) for detailed information).

Enterprise Records Schedule (ERS) - A schedule, developed by the Department of Homeland Security for DHS-wide application, governing the disposition of specified recurring record series common to most DHS Components.

Emergency Operating Records - Records vital to the essential functions of the Federal Government for the duration of an emergency/disaster. These records include those necessary for mobilization and protection of material and manpower resources, of services, and other systems; the maintenance of public health, safety, and order; and the conduct of essential civil defense activities. These records must be available as needed at or in the vicinity of the emergency operating centers.

Essential Records - Records essential to the continued functioning or reconstruction of an agency or office and its operating units during and after an emergency or disaster (Emergency Operating records.), including those records essential to protect the rights and interests of an agency or organization and of individuals directly affected by its activities (Rights and Interests records).

Federal Enterprise Architecture (FEA) File Number – The FEA is an Office of Management and Budget (OMB) supported file plan numbering system the Department of Homeland Security (DHS) has adopted for implementation, by all DHS Components, to support future Enterprise recordkeeping initiatives.

Field Records - Records accumulated by field operating offices and staff support offices, as opposed to those accumulated by Headquarters.

File - An accumulation of records, which includes papers, photographs, maps, machine-readable information or other recorded information regardless of physical form or characteristics, accumulated or maintained in filing equipment, or machine-readable media, or on shelves, and occupying office or storage space.

File Break - Termination of a file at regular periodic intervals to facilitate continuous disposal or transfer of the file series. Also called cutoff; abbreviated as COFF.

Frozen Records (Suspended Records Disposition) - Records that have been identified as subject to current or pending litigation. These records must be retained until the Chief Counsel's office announces otherwise. Offices retain frozen records in their own file stations. However, frozen records may be transferred to Federal Records Centers if space limitations dictate the need.

General Records Schedule (GRS) - A schedule, issued by NARA, governing the disposition of specified recurring record series common to most agencies.

Inactive Records (PIF) - Records no longer required to conduct current business which can be relocated to a separate storage area, microfilmed, or destroyed according to the appropriate records disposition schedule.

Inventory – A survey of office or agency records and non-record materials that is conducted primarily to develop an office file plan or to develop records disposition schedules. It is also used to assist in identifying various records management problems, such as improper applications of recordkeeping technology.

Life Cycle of Records - The management concept that records pass through three stages: creation or receipt, maintenance and use, and disposition.

Master File Classification Code - Commonly referred to as MFCC, is a number which identifies a specific file category within the Secret Service filing system. MFCCs are often related to electronic systems for tracking and statistical and accountability purposes, as well as paper records.

Nonrecord Material - A designation used for papers that are not included within the definition of the word "records." Nonrecords include:

1. Library and museum material made or acquired and preserved solely for reference or exhibition purposes.
2. Extra copies of letters, memoranda, reports, and other papers distributed or kept only for informational or reference purposes.
3. Reader file copies of correspondence.

4. Tickler, follow-up, or suspense copies of correspondence.
5. Identical duplicate copies of all documents maintained in the same file.
6. Stocks of blank forms, publications, and other documents retained for supply purposes.

Office File Plan - A list describing the records accumulated or generated within an office, including the MFCC, file title/description, Privacy Act systems notice number (if applicable), media (paper or electronic.), and location within the office. This list is located in front of the first file folder of the current year's files.

Office of Record - The office designated to maintain the official record copy. Normally, it would be the "business owner" of the information, i.e., the office that created or received the records relating to its assigned functions.

Official File Copy (OSP) – For selected classes or collections of records (see Special Collections of Records below), an exact duplicate of the original outbound document or record copy, including signature, date, and enclosures or attachments, kept on file by OSP for use as a finding aid and/or for other archival or reference purposes. **(Note: For FOIA, legal, or other document search and production purposes, this copy typically does not serve as the Record Copy.)**

Permanent Records - Records of continuing value which are considered to be so valuable or unique in documenting the history of an agency or for informational content that they should be preserved "forever" as part of the National Archives of the United States.

Personal/Private Papers - Documentary materials belonging to an individual that are not used to conduct Agency business. Related solely to an individual's own affairs or used exclusively for that individual's convenience. These documents must be designated as personal or private papers and must be kept separate from Agency records. These are examples of personal/private papers:

1. Employee's copy of personnel actions;
2. Materials regarding membership in professional organizations;
3. Journal of daily events, kept separate from an official schedule of daily activities;
4. Notes taken during training sessions not intended for circulation to others; and
5. Notes taken at meetings which are not circulated to others, and are not used as a basis for official action.

These are **not** private/personal papers:

1. Calendars, appointment books, schedules of activities, etc., that record your daily activities as a federal employee;
2. Drafts, background material, notes, etc., prepared in the course of your assigned duties;
3. Speeches or articles written in your capacity as a federal employee; and
4. Notes used to give a briefing to agency staff.

Privacy Act Records (PA) - Records maintained on individuals. These records are created, maintained, and retrieved using the person's name, social security number, race, sex, or some other personal identifier.

Program Records - Records created, received, and maintained by an agency in the conduct of the mission and functions for which it is responsible. The term is used in contrast to administrative, housekeeping, or facilitative records.

Record - All recorded information, regardless of form or characteristics, made, made or received by a Federal agency 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 United States Government or because of the informational value of data in them.

Generally, an item should be treated as a record if an office created it; an office acted on it; an office received it for action; and/or an office serves as a custodian of it because of oversight duties.

Record Copy – The original document or an exact duplicate of the original document, complete with signature, date, and enclosures or related supporting documents, resulting from specific transactions and operations. Official Agency records include information recorded on any medium, including paper, microform, cards, film, audio and video tape, optical disk, or magnetic media. These records may be generated from and/or stored on electronic systems and devices such as e-mail, network storage, databases, etc. **The record copy generally is maintained by the originating office of record (i.e., the sender), unless other arrangements are made with OSP.**

Records Custodian – Individuals responsible for ensuring the safety, timely availability, and proper retention and/or transfer of information in their custody.

Record Group Number (RG) - A number assigned by the National Archives and Records Administration to each Agency for convenience in identifying records. Record Group Number 87 is assigned to the Secret Service.

Records Liaison - An individual who has been assigned responsibility for the operation and/or management of office files.

Records Management - The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with records creation, maintenance and use, and disposition, in order to achieve adequate documentation of the policies and transactions of the Federal Government.

Retention Period - The time period established for particular record series to be retained.

Rights and Interests Records - Records having potential direct impact on the Federal Government, its employees, and citizens. These records are vital to an agency shortly after a disaster or emergency occurs in order to restore, in part, agency operations to normal. Examples of these records encompass payroll, retirement, Social Security, significant research and other types of data collected on individuals.

Screening - The examination of records to determine the presence of documents eligible for destruction and the removal of such documents from the files.

Series - Documents arranged in accordance with a filing system or maintained as a unit because they relate to a particular subject or function, result from the same activity, have a particular form, or because of some other relationship arising out of their creation, receipt, or use.

Special Collections of Records - Selected records identified by the Secret Service or National Archives requiring special segregation or safeguarding to ensure preservation for historical and/or legal purposes. Some examples are files related to the 9/11 terrorist attacks; Hurricane Katrina records; records related to particular high-level investigations or decisions affecting the Secret Service; and/or other special collections established via Executive, Congressional, or judicial order.

Subject Files - Records arranged and filed according to their general information content. Also known as correspondence files. Consist mainly of general correspondence but may include forms, reports, and other material that relate to office functions. The purpose of a subject file is to bring together all papers on the same topic to facilitate information retrieval.

System of Records (Privacy Act) - A group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or the identifying particular assigned to the individual.

Transfer of Records (TRF) – The approved relocation of Secret Service records from the Responsible Office to either a records storage facility (Federal or commercial) or to the National Archives and Records Administration.

Transitory Records - A general term for those types of records that lose their value within a short period of time and should be separated during filing from records requiring longer retention.

Unscheduled Records - Records that do not have a final disposition approved by NARA.

Working Files - Preliminary drafts, rough notes, and similar material used to prepare final copies. Working files may meet the definition of records and should be maintained if:

1. They were/are circulated and made available to employees other than the creator for official purpose such as approval, comment, action, recommendation, follow-up, or to communicate with agency staff about business; and

2. They contain unique information, such as substantive annotations or comments, which add to the understanding of the agency's formulation and execution of basic policies, decisions, actions, or responsibilities.

Responsibilities

Chief Strategy Officer, Office of Strategic Planning and Policy (OSP), provides oversight of and support to the Secret Service Records Management Program and the development and issuance of policies and standards to carry out the program objectives through the Chief Records Officer and the CRO's subordinate staff

Chief Records Officer, OSP, has overall responsibility for development/dissemination of records management policy and procedures for Headquarters and Field Offices; participates in Secret Service decisions which result in the creation of Government records; periodically reviews Secret Service records and documents management practices for compliance with relevant authorities, and, if necessary, recommends corrective actions; and provides overall program direction, vision, and guidance.

The Office of the Chief Information Officer (CIO) and its subordinate elements facilitate and implement records management as it relates to information systems and their acquisition, implementation, operation, maintenance, backup, safeguard, and life cycle.

Assistant Directors, Executive Chiefs, Special Agents In Charge (SAICs), and Division Chiefs will:

1. Ensure the Secret Service records management program is implemented within their respective operations.

2. Ensure records having permanent value are identified and earmarked for offering to the National Archives for permanent preservation by using records appraisal guidelines provided in Record Programs Management Manual policy on Disposition of Permanent Records.

3. Designate a Records Liaison within their respective chains of command to execute records

management activities.

a. Ensure designated Records Liaisons receive NARA-mandated records management training as facilitated by OSP.

b. Include records management responsibilities in the position description of the individual designated as Records Liaison.

4. Report discoveries of lost or damaged records immediately to the Chief Records Officer.

Headquarters and Field Office Records Liaisons. The individual(s) designated as division/office Records Liaisons will:

1. Conduct annual inventories of all office file stations to assist in preparation or update of the Office File Plan. The inventory assists in identifying unscheduled records and vital records.

2. Prepare the Office File Plan ensuring records maintained by the office are included and are described accurately in the agency's applicable records disposition schedules.

3. Ensure proper disposition and maintenance of office records to include:

a. Systematic file cutoffs/breaks;

b. Retirement of eligible records to the designated Federal or commercial records centers;

c. Disposal of temporary records when their retention periods expire; and

d. Safeguarding and proper retention of frozen records.

4. Cooperate and assist OSP records staff in periodic evaluations and/or surveys of office records.

5. Maintain the record copy and associated documentation to ensure a complete account of essential transactions of the Secret Service.

6. Notify OSP of organization or program changes resulting in the establishment of new types of records, the transfer or termination of records no longer required, or an increase or decrease in the retention period for records.

Field Offices and Protective Divisions are designated as the offices of record for the files in their respective operations.

All Secret Service Employees and Contractors. Every employee or contractor who works for the Secret Service is responsible for records created in the course of his/her daily business transactions. If an employee or contractor creates a document using a personal computer; enters information into a database; files a document in a folder; answers an inquiry from the public; responds to a FOIA request; or does anything else that documents activities of the Secret Service, that employee or contractor is a records custodian. Records custodians are responsible for ensuring the safety, timely availability, and proper retention and/or transfer of information in their custody.

All Secret Service employees and contractors will:

1. Conduct work according to Federal records management regulations and Secret Service records management policy and procedures.

2. Create and manage records necessary to document their official activities, including creation of appropriate records documenting meetings, conversations, electronic mail messages, telephone calls and other forms of communication that affect the conduct of Secret Service business.

3. Destroy records only in accordance with approved records dispositions.

4. Obtain prior authorization to remove records or copies of records from Secret Service custody.

5. File personal papers and nonrecord materials separately from official Secret Service records.

Recordkeeping Requirements

Responsible Offices will ensure their directives identify recordkeeping requirements by referencing applicable sections within the Record Programs Management Manual; and/or Agency Records Schedules (ARS), Enterprise Records Schedules (ERS), or General Records Schedules (GRS). Directives requiring users to create and maintain records must identify applicable Master File Classification Codes (MFCC) and DHS FEA Codes (when applicable) to be used. Offices requiring new or revised MFCCs must provide a justification memorandum to and receive approval from OSP prior to use of the new file.

1. **Electronic Records.** The creation, maintenance, use, storage, and final disposition of electronic records, which include numeric, graphic, and textual information, must comply with Secret Service requirements outlined in its records control schedules and records management policies. Electronic mail (e-mail) messages and other electronic messages are addressed in the agency's (b)(7)(E) for such records; see GRS-06(01). (b)(7)(E)
(b)(7)(E)

2. **Contractor Records.** Records management oversight of contractors' records is necessary to ensure that Secret Service long-term recordkeeping needs are met. Many types of contracts involve the creation of background data of value to the Government. Contractors performing program functions must create and maintain records to document these programs. The contract must include requirements for the delivery of all pertinent documentation of contractor execution.

Contractors will comply with these specific Secret Service recordkeeping requirements:

a. Delivery of background data of value and use to the Secret Service.

b. Provision of electronic data with accompanying technical documentation to permit the Secret Service to use the data.

c. Provision of any data and records that may have value to the Secret Service that were not identified in advance, but fall under the "deferred ordering and delivery clause" of the contract.

3. **Privacy Act Records.** The Privacy Act of 1974, as amended (5 U.S.C. 552a), applies to records under the control of an agency that contain information about an individual, such as a person's education, financial transactions, medical history and criminal or employment history that contain the individual's name, or some other item that identifies that person and from which information is retrieved by the name or other particular assigned to the individual. Extra care must be taken when handling Privacy Act records to provide certain safeguards for an individual against an invasion of personal privacy.

For hard copy records, established Privacy Act Systems Notice numbers are identified for use on file folder labels of records covered by the Privacy Act. These numbers alert the record handler/holder that "personal" information is contained within the document and/or folder and is subject to requirements and restrictions of the Privacy Act. Access to these records is restricted to employees responsible for records management and operational employees who have a need-to-know such information. Records liaisons may devise a simple economical color-coding system for additional emphasis of these files.

Agencies publish "Systems of Records" (Privacy Act records) for which they have Government-wide responsibility. The Office of Personnel Management (OPM) has Government-wide responsibility for a number of human resource management functions common to most offices within the Federal government. These are:

a. OPM/GOVT-1 = General Personnel Records

b. OPM/GOVT-2 = Employee Performance File System Records

c. OPM/GOVT-3 = Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers

d. OPM/GOVT-5 = Recruiting, Examining, and Placement Records

e. OPM/GOVT-6 = Personnel Research and Test Validation Records

f. OPM/GOVT-7 = Applicant Race, Sex, National Origin, and Disability Status Records

g. OPM/GOVT-9 = File on Position Classification Appeals, Job Grading Appeals, Retained Grade or Pay Appeals, and Fair Labor Standard Act (FLSA) Claims and Complaints

h. OPM/GOVT-10 = Employee Medical File Systems Records

NOTE: These records are OPM's records, although they are in the physical custody of other agencies.

More detailed information regarding the Privacy Act can be obtained by contacting the Privacy Services Program of the Office of Intergovernmental and Legislative Affairs.

4. **Litigation (Frozen or Suspended Records)**. Records identified by the Office of the Chief

Counsel as being subject to current or pending litigation must be retained indefinitely by all offices. (Previously approved disposition instructions for these specific records are suspended; thus, the term "frozen records.") When called for by Chief Counsel's office, copies of the frozen records must be forwarded to the Chief Counsel. Original copies of frozen records must be separated from other office records to prevent premature, unauthorized disposition of those frozen records. A listing of records currently "frozen" is maintained on the OSP Records Management home page. Cancellations of suspended records dispositions are announced by Chief Counsel's office, at which time offices can execute disposition instructions for the subject records.

5. **Unscheduled Records.** Offices having records not covered by an approved disposition schedule must establish a temporary file number based on the applicable policy directive. Contact OSP to inventory the records and compose a disposition schedule for NARA approval. Temporary disposition instructions will read "Retain in current files area (CFA) until disposition instructions are published." No record may be destroyed until an approved disposition has been determined.

Files Maintenance

Files maintenance includes planning for the location of files, assigning responsibility for their maintenance, and ensuring efficient and economical use of files equipment and space. One critical test of any file system is how quickly information can be retrieved. It may be helpful to set up a "network" of records liaisons within each directorate, with a lead person for each division/office, to accomplish effective files management. Proper files maintenance promotes efficient and effective use of the information in the files, and ensures that the information is available in usable form when needed.

File Locations

41 CFR 101-11.305-4 requires official file locations (file stations) be established for filing of official records. A files station is every separate location at which records of any kind are accumulated. Identify your office file station locations on your Office File Plan.

Inventory

Conduct an inventory of office records documenting activities and functions of your office. An inventory helps identify which materials are records, reference materials (nonrecords), personal papers (nonrecords), and extra copies of documents, publications, and forms (nonrecords). The inventory also aids in identifying which records are needed immediately in the event of an emergency (Essential Records).

Records Disposition Schedules

Match the records identified in your inventory with the records disposition schedules described in this manual, to include Agency Records Schedules (ARS), DHS Enterprise Records Schedules (ERS), and/or General Records Schedules (GRS). The schedules prescribe retention periods of records and what happens when records are no longer needed in the office for current operations (inactive records). The **approved retention periods stated in these approved NARA schedules are mandatory.** Exceptions to retention periods are those records identified as "frozen" due to current or pending litigation actions.

Office File Plan

Prepare an Office File Plan to identify and document the records of the office. If multiple file stations are used, consolidate the listing of records of all file stations onto one file plan. The file plan contains the Master File Classification Code (MFCC) number, file title/description, disposition dates, Privacy Act Systems Notice number (if applicable), media type (paper, electronic, microform, etc.) and file station location. Place the Office File Plan ahead of the first file folder at each file station. The Records Liaison keeps the file plan current by making changes as files are added, deleted, or relocated throughout the year. **A copy of the Office File Plan is submitted to OSP annually, by January 31.** Revisions are also forwarded to OSP.

The file plan aids office personnel in retrieval of records; accounts for the maintenance of specific records used in the office; provides assurance of adequate and proper documentation of Secret Service functions and transactions; and, indicates the level of attention afforded to records management within the office.

Inspect Records

Prior to filing, inspect records to ensure all actions have been completed. Eliminate unnecessary attached material (routing slips which bear no essential information, and extra copies). Identify incomplete actions to ensure they are followed up on to ensure the file is not prematurely cut off or destroyed. If an action is complete, but essential documentation is missing, try to obtain the missing information. If unsuccessful, note the action taken to obtain the missing information, and file it with the incomplete action.

Cross Reference

If a document being filed involves more than one subject or case and there is a good chance it might be utilized in multiple file systems, a cross reference should be prepared as a finding aid.

1. Select and indicate the file designation for the additional subject or case directly below the file designation for the main subject or case. Mark an "X" in front of this file designation to show that a cross reference is required. Generally it is more efficient to use a photocopy or duplicate electronic document rather than a cross reference form.

2. A cross reference may be used to indicate that a record has been relocated from one place in the file to another.

Assembly of Records

1. Make sure the file is complete and all enclosures/attachments are accounted for; if enclosures/attachments are too bulky to attach to correspondence records, annotate on the original incoming communication where the enclosures/attachments are filed.

2. Ensure part(s) of another file are not accidentally attached to your file copy; destroy duplicate copies.

3. Remove all classified cover sheets, unless records are in suspense files or when cases are placed in security containers pending completion of an action.

4. Avoid use of paper clips, binder clips, rubber bands, and metal fasteners embedded in file folders. These objects, if found in records stored by a Federal Records Center or other authorized storage provider, will result in additional charges to the Secret Service at time of destruction.

Classified Records

Custodians of classified information or material are responsible for providing protection, security, and accountability of such information or material at all times. Custodians ensure unauthorized persons do not gain access to classified information or material by sight or sound. Classified information or material must not be discussed with, or in the presence of, unauthorized persons. Classification and downgrade or declassification of records is accomplished by designated Secret Service officials; the Security Management Division (SMD) maintains information on current designees.

(b)(7)(E)

Detailed procedures for handling classified materials are contained in the Human Resources Manual, Security Management Division (SMD) chapter.

(b)(7)(E)

(b)(7)(E)

Damage to and Unauthorized Destruction of Records

The Archivist of the United States and the Director of the Secret Service are responsible for preventing unauthorized disposition of Secret Service records, including all forms of mutilation and alienation. Removal or destruction of records in the legal custody of the Secret Service without regard to approved records disposition schedules is illegal and penalties include fines and imprisonment.

In cases of accidental destruction of records by fire or other means:

1. Immediately contact the Chief Records Officer (OSP).

2. Reconstruct as much of the lost or destroyed record(s) as possible. Information from Secret Service offices can often be gathered to reconstruct a record series.

3. Identify damaged or destroyed records that cannot be reconstructed for inclusion of a records transfer to a Federal Records Center on Standard Form 135, Request for Records Transmittal and Receipt at the time the records are transferred.

In other cases, Assistant Directors, Executive Chiefs, SAICs, or Division Chiefs must immediately report the discovery of lost or damaged records to the Chief Records Officer. Offices will document information pertaining to items 1 through 5 below, as well as any additional information requested by OSP, for use in reporting to NARA. Offices will cooperate fully with OSP and NARA and initiate necessary action to ensure recovery of records.

When requested, the Secret Service will report any unlawful or accidental destruction, defacement, alienation, or removal of records in the custody of the Secret Service. The report must include:

1. A complete description of the records with volume and dates if known;

2. The office of origin;

3. A statement of the exact circumstances surrounding the defacement, alienation, or destruction of the records;

4. A statement of established safeguards and specific procedures implemented to prevent further loss of documentation;

5. When appropriate, details of actions taken to salvage, retrieve, or reconstruct the records; and

6. Use Interagency (b)(6); (b)(7)(C) on this report as prescribed by Title 36 CFR, Chapter 12.

The Archivist of the United States will assist the Director of the Secret Service when contact with the Attorney General for the recovery of any unlawfully removed records is required.

Transfer of Records to Federal Records Centers or Commercial Records Centers

Inactive records that have not reached the end of their retention period generally should be transferred for storage at an approved records center facility.

While most agencies have relied on NARA's Federal Records Centers for offsite storage and safeguarding, recent changes in NARA regulations permit (and eventually will mandate) offsite storage of paper records at a an approved commercial facility.

(b)(7)(E)

Transfer of Records from the Custody of One Executive Agency to Another

No records are to be transferred from the custody of the Secret Service to another executive agency without the prior written approval of NARA, except as provided in 36 CFR, Subpart H. Clarification on this can be obtained by contacting the Chief Records Officer (Division Chief – OSP).

Restrictions on the Use of Secret Service Records

Once Secret Service records have been transferred to the National Archives, legal custody of the records is assumed by NARA. However, specific restrictions on their use by other agencies or individuals, as applied by the Secret Service, is imposed by the Archivist of the United States. These restrictions can only be removed by agreement between the Director of the Secret Service and the Archivist of the United States.

MANAGEMENT OF E-MAIL AND OTHER ELECTRONIC MESSAGE RECORDS

Purpose

United States Secret Service (USSS) employees and authorized users routinely create, send, and receive electronic mail (e-mail, e-mails, or e-mail messages) to communicate information related to the mission or administrative matters of the agency.

In accordance with the Federal Records Act, associated regulations of the National Archives and Records Administration (NARA), and Department of Homeland Security (DHS) recordkeeping requirements for retention and disposition, e-mails that are Federal records must be retained in electronic systems that provide the capability to identity, retrieve, and retain the records for as long as they are needed for statutory, regulatory, and business purposes. Secret Service e-mail records are defined as e-mail messages, along with any attachments, and include calendar appointments and tasks managed in the same system as e-mail messages.

In conjunction with Chief Information Officer Manual directives regarding e-mail security, this directive provides an authoritative summary of the records management policies, protocols, and philosophies which govern management of electronic mail ("e-mail") and other types of electronic messages in the Secret Service. It provides guidance to all agency personnel who oversee, administer, or otherwise contribute to the management of agency e-mail. It also establishes a framework for use by all employees (and other authorized users of Secret Service e-mail resources) at all levels of our organization, and reflects expectations and obligations related to managing e-mail as an official Government record.

Scope

This directive applies to e-mail records created or received by authorized Secret Service users on or after December 31, 2016, as well as any prior/earlier messages that have been migrated to the designated USSS e-mail archiving management system, Enterprise Vault ("E-Vault").

Provisions regarding management of records associated with (b)(7)(E) officials are effective upon designation of an individual's account as (b)(7)(E) permanent. (b)(7)(E) guidance, developed by NARA to simplify e-mail management, allows agencies to categorize and schedule e-mails based on the role or position of the e-mail account user – with e-mail of top level officials to be preserved for permanent retention.) Once an e-mail user is designated as a (b)(7)(E) official, the agency must manage all business related e-mails sent or received by that official in a manner that ensures their continued preservation and facilitates their eventual transfer to NARA.

Background and Authorities

Federal agencies and their employees are required to manage e-mail and other types of electronic messaging records in accordance with the Federal Records Act and 36 CFR Chapter XII Sub-chapter B.

In 2013, NARA issued Bulletin 2013-02 "Guidance on a New Approach to Managing Email Records" to supplement these statutory and regulatory authorities. In 2014, NARA and the Office of Management and Budget (OMB) jointly issued a "Managing Government Records Directive" (M-12-18). This directive requires agencies to manage both permanent and temporary e-mail records in an accessible electronic format by December 31, 2016, based upon specific criteria developed by NARA.

The criteria and NARA's corresponding Government-wide guidance was issued as General Records Schedule (GRS) 6.1, *Email Managed under a* (b)(7)(E) *Approach.* Commonly known as (b)(7)(E) this guidance attempts to eliminate the longstanding, paper-based "print-and-file" approach to e-mail recordkeeping by allowing agencies to:

- Base e-mail records retention on the mailbox owner's role in the agency, rather than on the content of each e-mail record.
- Develop mechanisms for organizing and storing e-mails (and their attachments) in their native electronic format, according to established schedules (based on program, mission, or agency need) and for the duration of their retention periods.
- Implement procedures that address retirement, transfer, or other employee separation scenarios to ensure Government records are preserved, and non-records are culled.

36 CFR § 1236.22 also establishes "requirements for managing electronic mail records." Key provisions of this regulation include the following:

- The names of sender and all addressee(s) and date the message was sent must be preserved for each electronic mail record in order for the context of the message to be understood.
- Attachments to electronic mail messages that are an integral part of the record must be preserved as part of the electronic mail record or linked to the electronic mail record with other related records.

Finally, the Presidential and Federal Records Act Amendments of 2014 (Public Law 113-187) modernizes records management by focusing more directly on electronic records. The amendments include provisions which strengthen the Federal Records Act by:

- Expanding the definition of Federal records to clearly include electronic records.
- Confirming that Federal electronic records will be transferred to NARA in electronic form.
- Granting the Archivist of the United States final determination as to what constitutes a Federal record.
- Authorizing (in particular situations) the early transfer of permanent electronic Federal records to the National Archives, while legal custody remains with the agency.

The Department of Homeland Security has addressed the above via DHS Directive 142-03, Email Usage, which serves as a foundation for this Secret Service directive.

Types of Electronic Messages

Electronic messages sent or received by Secret Service employees generally can be categorized as one of the following message types. Additional discussion is contained in the DHS online training course entitled "Electronic Records Management."

Records

Messages having potential direct impact on the Federal government, its employees, and citizens; messages relating to budget, personnel, supply, and similar support functions. This includes messages which:

(a) Have been identified as subject to current or pending litigation.

(b) Document the persons, places, things, or matters dealt with by the agency.

(c) Facilitate action by agency officials and their successors in office.

(d) Make possible a proper scrutiny by the Congress or other duly authorized agencies of the Government.

(e) Protect the financial, legal, and other rights of the Government and of persons directly affected by the Government's actions.

(f) Document the formulation and execution of basic policies and decisions and the taking of necessary actions, including all substantive decisions and commitments reached orally (person-to-person, by telecommunications, or in conference) or electronically.

(g) Document important board, committee, or staff meetings.

Draft documents that are circulated on electronic mail systems also may be records if they meet the criteria specified above.

Messages sent or received as a "carbon copy" (cc) or "For Your Information" (FYI), etc. shall generally be considered records, even if no immediate action is expected/required of the recipient. (The awareness provided generally implies there is a knowledge or understanding required relevant to an assigned business function, even if only for contingency purposes.)

Non-Records

Messages that are kept only for informational or reference purposes; duplicate copies of messages that have been filed as records elsewhere; earlier drafts of messages or partial messages that are used for template or discussion purposes which lead to creation of a final record; email blasts originating from other USSS accounts.

Personal

Messages sent or received by an individual under "limited personal use" provisions (see ITG-03(06)) that are not used to conduct agency business, such as employee copies of personnel actions; materials regarding membership in professional organizations; personal correspondence (such as from a child care provider) that generally must occur during business hours; system correspondence from the Thrift Savings Plan, FSAFeds, and unique other records associated with an individual's service with application beyond the workplace.

If a message includes or encompasses personal or quasi-personal issues but also relates to official business considerations (e.g., leave, training requests, etc.) the message must be treated as a record.

Policy

The Secret Service manages e-mail records under the following (b)(7)(E) approach, based on the role of the e-mail account user rather than on the content of each e-mail record.

E-Mail Records of Designated (b)(7)(E) Officials

(b)(7)(E) Officials" are top level executives and senior staff of a Government agency, as well as other designated program officials described in General Records Schedule 6.1. **A list of USSS (b)(7)(E) Officials appears in Appendix 1 of this directive.** (b)(7)(E) Officials include any officials serving in an acting capacity for these positions for longer than 60 days.

- Business e-mails (including attachments) and related records sent or received by (b)(7)(E) Officials are permanent records and may not be deleted. (E-mail records include e-mail messages and attachments, as well as calendar appointments and tasks managed via the agency e-mail application platform.) The Component must maintain these e-mails for 15 years after the end of the e-mail user's tenure and then transfer the e-mails to NARA in accordance with the schedule.

- Non-record e-mails are those that do not meet the criteria of a Federal record and are so designated regardless of whether a (b)(7)(E) Official sends or receives them. Non-record e-mails should be deleted or "culled" as soon as practical. (See "Culling of E-Mail" provisions later in this directive.)

    - Non-record e-mail includes those sent or received as *limited personal use* correspondence (see Office of the Director Manual section ITG-03(06) for more information). Users should delete personal e-mails as soon as possible after receipt or save to a folder marked "Personal" in their electronic mailboxes.

  Non-business e-mails that are not culled will be transferred to NARA at the end of the agency retention life cycle.

- Business e-mails (including attachments) that are sent or received by (b)(7)(E) Officials may also be duplicated outside the e-mail system (either in electronic format or in hard copy, if appropriate) and retained with the associated administrative or program record in accordance with the approved records retention schedule for that subject (e.g., case files, survey reports, project files, etc.) (Note: duplicate e-mail copies filed in this manner will be disposed of when the associated file reaches the end of its retention period.)

- Legal Holds/Preservation Management: Upon notice of a legal requirement to hold or preserve records, any e-mail associated with the hold will be retained until the legal requirement is lifted. The hold will apply regardless of the record's status and will supersede the records retention schedules.

E-Mail Records of Secret Service Official Messages

Official Message accounts are associated with an office/division-level organizational unit, rather than a person. In contrast with the more informal, unstructured, and often pre-decisional content that generally characterizes person-to-person e-mail, Official Messages serve to formally document historically significant communications and other information of enduring value.

The Official Message system provides a foundation for fulfilling agency mandates established in title 44 United States Code chapter 29 "to achieve adequate and proper documentation of the policies and transactions of the Federal Government," and provides a designated Secret Service mechanism to:

- Transmit documentation of significant agency decisions and commitments reached orally, in person-to-person e-mail, by telecommunications, or in conference and not otherwise documented in agency files;
- Provide background or context for a draft action memorandum, directive, etc., if the Official Message adds to a proper understanding of the formation or execution of an agency action;
- Convey information of value on important agency activities, if the Official Message adds to a proper understanding of agency operations and responsibilities;
- Facilitate action by Secret Service officials and their successors;
- Document important meetings; and
- Protect the financial, legal, and other rights of the Government and of persons directly affected by the Government's actions.

Official Messages are transmitted with file codes that reflect the type of subject matter, and contain signature lines for the cognizant USSS official and his/her office. A person-to-person message containing the type of information described above is generally expected to be retransmitted as an Official Message.

Secret Service Official Messages of Directorate level offices and the Office of the Director, sent/received between January 1, 2001 and December 31, 2017, will be retained as (b)(7)(E) permanent and transferred to NARA in 15 years. All other Secret Service Official Messages are disposable when 7 years old, but longer retention is authorized if required for business use.

E-mail Records from all Other Accounts Not Designated as (b)(7)(E) Permanent

E-mail records (to include e-mail messages and attachments, as well as calendar appointments and tasks managed via the agency e-mail application platform) of all other Secret Service e-mail accounts will be retained for 7 years, at which time they may be disposed of unless needed for other business purposes or the subject of a litigation hold.

- Non-record E-mails: Non-record e-mails are those e-mails that do not meet the criteria of a Federal record and are so designated regardless of whether a (b)(7)(E) Official sends or receives them. Non-record e-mails should be deleted or "culled" as soon as practical. (See "Culling of E-Mail" provisions later in this directive.)

  Non-record e-mail includes those sent or received as *limited personal use* correspondence (see Office of the Director Manual section ITG-03(06) for more information). Users should delete personal e-mails as soon as possible after receipt or save to a folder marked "Personal" in their electronic mailbox. (See "Folder Structure" provisions on next page.)

- Business e-mails (including attachments) that are sent or received by (b)(7)(E) Officials may also be duplicated outside the e-mail system (either in electronic format or in hard copy, if appropriate) and retained with the associated administrative or program record in accordance with the approved records retention schedule for that subject (e.g., case files, survey reports, project files, etc.) (Note: duplicate e-mail copies filed in this manner will be disposed of when the associated file reaches the end of its retention period.)

- Legal Holds/Preservation Management: Upon notice of a legal requirement to hold or preserve records, any e-mail associated with the hold will be retained until the legal requirement is lifted. The hold will apply regardless of the record status and supersede records retention schedules.

Folder Structure

To supplement organization of messages in the top level ("root") e-mail folder, creating subfolders with an appropriate hierarchy (e.g., establishing folders based on fiscal or calendar year; by project/task force name; subject to a litigation holds in a particular case; creating subfolders based on Master File Classification Code (MFCC) number; etc.) is recommended.

In addition, all employees (not only those designated as (b)(7)(E) Officials) are encouraged to manage their e-mail by creating these additional sub folders within their e-mail application (e.g., Microsoft Outlook) Inbox and Sent Items:

- **Non-Records**
- **Personal**

Once established in the user's e-mail application, these folders will be replicated in the user's long term e-mail archive as well. (See "Enterprise Vault (E-Vault)" provisions below.)

Additional notes:

- Users are reminded that even for e-mail sent or received under limited personal use provisions, there is no expectation of privacy.

- For record-driven compliance activities like FOIA, it may be reasonable to exclude Non-Records and Personal folders from corresponding searches. However, for inquiries involving legal discovery or investigative matters, all folders may be examined for evidentiary purposes, and responsive materials provided to the cognizant requesting authorities. Should responsive materials be located in those folders, they shall be treated as records (at least until the litigation is resolved) and moved to a folder created for that purpose.

- If an e-mail/e-mails have been identified as being subject to a litigation hold, they must be treated as records – even if the message(s) fall within the category of "non-record" or "personal." Optimally, this is accomplished by creating a folder corresponding to the litigation freeze order and copying the e-mail(s) to that folder, and retaining them there until the freeze is lifted.

Culling of E-Mail

Culling refers to the removal – or otherwise excluding from capture – of non-record or personal messages and attachments. Culling typically includes the removal of spam, e-mail blasts originating from other accounts (such as agency-wide communications), and personal materials (such as "limited personal use" e-mails to family members not related to agency business (see Office of the Director Manual section ITG-03(06) for more information)). Culling may be manual, automated, or a hybrid of both. Agencies are expected to ensure that the e-mail of (b)(7)(E) officials (permanent accounts) is culled to the greatest extent appropriate before transfer to NARA.

Questions regarding the appropriate designation of an e-mail as record, non-record, or personal must be presented to the Office of the Chief Counsel for further coordination with the USSS Chief Records Officer, as appropriate.

Enterprise Vault (E-Vault)

E-Vault is a software application that is currently being utilized by the Secret Service to allow centralized storage, backup, and preservation of e-mail data for more than 180 days. E-Vault stores e-mails and their attachments, and is configured to ingest e-mail messages from local (e.g., Microsoft Outlook Personal Storage Table or .PST) files located outside of the e-mail server.

The Secret Service uses E-Vault as an "electronic file cabinet" that can securely store messages for extended periods of time. **E-Vault helps each authorized Secret Service user fulfill his/her recordkeeping responsibilities, as required by law, by providing a stable medium for longer term retention and by facilitating the aggregation of permanent records for designated (b)(7)(E) officials.** It also allows authorized program managers and compliance officials to leverage the information contained in Secret Service e-mail to fulfill operational and legal requirements.

Unlike E-Vault, the Secret Service e-mail server that sends and receives messages each day has only limited space to store and retain those messages. Under the Secret Service's concept of operations **any message sent or received by an employee will be available on the Secret Service e-mail server for 30 days, after which it will be automatically migrated to E-Vault**, under a corresponding E-Vault folder designated for the individual user account, unless deleted during the culling process.

Additional Considerations

- E-Vault does not distinguish between personal and business messages, nor can it automatically infer temporary or permanent retention of stored messages. As noted above, this underscores the importance of each employee or office custodian's deliberate choice on whether (and how) to file the message as a record, non-record, or personal item.

- E-Vault may prompt users to not delete or move a message once it has been placed in the "vault" folder. Even though prompted not to move or delete (cull) the messages, a user still has the ability to complete both actions, **and must perform them in order to fulfill records management responsibilities.**

- Use of E-Vault does not replace existing business practices requiring retention of e-mail with other related records in established recordkeeping systems. When business needs require e-mail records be retained within another recordkeeping system (either paper-based or electronic), users should ensure copies are created and provided for inclusion with those files. (Example: a message stored in E-Vault relating to a particular case file, should be duplicated and filed for inclusion in that case file.)

- For (b)(7)(E) personnel, users are required to practice the same planning and diligence in deleting messages that have reached the end of their retention period as they would with corresponding paper files. Generally, this is done at the commencement of a new calendar year – e.g., review your E-Vault folders for any messages older than 7 years, and delete them if you no longer need them for business/reference purposes. (**NOTE:** Although E-Vault will be configured to allow at least 7 calendar years' worth of e-mail for each employee, it is permissible for active employees to retain messages older than 7 years. Although retention of e-mail messages for longer than 7 years is authorized if needed for business/reference purposes, this practice should be the exception – not the rule.)

- E-Vault storage will not be limited for (b)(7)(E) officials, to facilitate the eventual production from E-Vault for transfer to NARA as permanent records in its native format, as required by NARA.

E-Vault Capability for Official Messages

Effective January 1, 2018, Official Messages sent to or received by an Official Message account also will be migrated to a corresponding E-Vault account. To access these legacy messages, contact your office personnel with designated Official Message responsibilities.

Local .PST (Personal Storage Table) Files

Only authorized personnel who require the ability to access and create .pst files for vital records, regulatory compliance, litigation, and other compelling purposes will have the capability of creating and using local .pst files.

Journaling

To support various initiatives related to Information Assurance, Insider Threat/Internal Security, Counterintelligence, etc., the Secret Service may undertake or request "journaling" of e-mail (i.e., capture of all e-mail traffic as it is sent/received, and preservation in a separate storage medium). While this practice may support necessary operational activities, it has the potential of undermining appropriate records management practices and disposition – e.g., inappropriately preserving a copy of an e-mail record that was properly disposed of/deleted by its business owner. This scenario could have grave ramifications from a FOIA, privacy, or litigation perspective.

Therefore, any entity engaged in journaling must ensure that retention of journaled data does not exceed the NARA authorized time frame of 180 days for generic use on an e-mail server unless otherwise dictated by a specific legal hold or administrative/investigative inquiry. Contact the Office of the Chief Counsel for additional clarification.

Closed/Dormant E-Mail Accounts

Since record material may exist within individual e-mail accounts on the e-mail or E-Vault servers, when those accounts are closed it is necessary to ensure that: 1) existing record material is preserved/properly migrated; 2) non-record material is purged; and 3) technical measures are applied that will prevent new records from unintentionally being created. Likewise, any e-mail archive that has been established in E-Vault under an individual's name must be migrated to a new custodian. Generally, these issues arise when employees separate from their positions or transfer to new program areas as their primary assignment. As such, the following standards for handling separating employees should be incorporated into corresponding out processing policies and required checklists.

Voluntary/Planned Separations (e.g., Resignations, Transfers, Retirements)

Supervisors:

- Provide/review briefing on records management responsibilities and discuss with separating employee.
- Determine if the separating employee's e-mail is subject to a legal/litigation hold; if so, ensure employee has contacted the Office of the Chief Counsel.
- Determine if separating employee is designated as a (b)(7)(E) Permanent Official; if so, ensure that the (b)(7)(E) employee has appropriately culled any non-record material.
- For all e-mail that has not migrated to E-Vault and which remains on the e-mail server, determine which record e-mails should be transferred/forwarded to the supervisor or other employees and which non-records should be deleted. For (b)(7)(E) employees, their corresponding E-Vault account will remain locked and inaccessible unless permissions are granted based on legal, investigative, or other compliance-related bases.
- Ensure the employee notifies internal/external peers, colleagues, and other points-of-contact of his/her separation in advance of the separation. Since the user's e-mail account will be deactivated, there will be no ability to establish an "out of office" message that will autoreply to incoming messages, nor will those intended messages be preserved or forwarded to others. The employee should:
    - Indicate he/she will be leaving the department/agency/component/program
    - Advise that inquiries be directed to the appropriate agency/program contact
- Inactivate, delete, or revise any miscellaneous user IDs, routers, and lists which include the separated employee as a member.

Employees:

- Since your e-mail account will be deactivated, there will be no ability establish an "out of office" message that will autoreply to incoming messages, nor will those intended messages be preserved or forwarded to others You must notify internal/external peers, colleagues, and other points-of-contact of your separation in advance to:
    - Indicate you are leaving the department/agency/component/program
    - Advise that inquiries be directed to the appropriate agency/program contact

- Close out e-mail accounts to ensure all personal e-mail messages and non-record materials have been deleted, and all record materials have been forwarded to a new custodian, as appropriate. **If subject to a litigation hold, employees must contact the Office of the Chief Counsel prior to closing out any e-mail accounts.**

- (b)(7)(E) Permanent Officials must ensure that their e-mail has been culled to remove any personal or non-record material in preparation for eventual transfer to NARA.

CIO E-Mail Support:

- Deactivate the e-mail account and ensure sustainability in E-Vault for the duration of required retention.
  - For (b)(7)(E) officials, configure autodelete parameters so any message older than seven years is automatically purged, unless the Office of the Chief Counsel has established a litigation freeze or other hold.
  - For (b)(7)(E) Permanent Officials, ensure account contents are preserved for 15 years after employee separation. At the end of this time period, coordinate review by Office of the Chief Counsel and Chief Records Officer in order facilitate the creation of transportable medium for transfer to NARA.

Involuntary/Unplanned Separations (e.g., Terminations, Death or Incapacitation, etc.)

Supervisors:

- Determine if employee e-mail is subject to a legal/litigation hold; if so, contact the Office of the Chief Counsel to determine the parameters of the hold.
- Engage IT support and other officials (e.g., Office of the Chief Counsel) as appropriate to determine if access to employee's messages should be obtained.
- For employee's e-mail that have not migrated to E-vault and remain on the e-mail server, determine if record e-mails/messages should be transferred/forwarded to the supervisor or other employees and if non-records should be deleted. For (b)(7)(E) employees, their corresponding E-Vault account will remain locked and inaccessible to others unless permissions are granted based on legal, investigative, or other compliance-related bases.
- For E-Vault archives, determine who should be the new custodian of archived records (if applicable)
- To the extent practical/appropriate, notify internal/external peers, colleagues, and other points-of-contact of employee's separation to:
  - Indicate the employee has separated from the department/agency/component/program
  - Advise that inquiries be directed to the appropriate agency/program contact

Since the user's e-mail account will be deactivated, there will be no ability to establish an "out of

office" message that will autoreply to incoming messages, nor will those intended messages be preserved or forwarded to others.

- Inactivate, delete, or revise any miscellaneous user IDs, routers, and lists which include separated employee as a member.

CIO E-Mail Support:

Following consultations described above (typically initiated by the employee's supervisor), and as deemed appropriate by cognizant directorate official, Chief Counsel, and Chief Records Officer:

- Deactivate e-mail account and ensure sustainability in E-Vault for the duration of required retention.
    - For (b)(7)(E) officials, configure autodelete parameters so any message older than seven years is automatically purged, unless the Office of the Chief Counsel has established a litigation freeze or other hold.
    - For (b)(7)(E) Permanent Officials, ensure account contents are preserved for 15 years after employee separation. At the end of this time period, coordinate review by Office of the Chief Counsel and Chief Records Officer in order facilitate the creation of transportable medium for transfer to NARA.

Other Electronic Messages (e.g., Text, Chat, Instant Messages)

It is the policy of the Department of Homeland Security (DHS) that accountable and comprehensive records management is essential. Unlike e-mail, however, many current messaging technologies do not include an electronic records management capability that can provide storage and access to computerized Federal records and other information for a sustained time period.

For this reason, all employees must give special consideration to when, and how, they use non e-mail based electronic messaging technologies such as text, chat, and instant messaging.

- If the electronic message sent or received is transitory in nature with no administrative, legal, fiscal, or archival value; is a limited personal use message; or is a non-record, then the message can be deleted or allowed to expire at the discretion of the user. Examples include:
    - A message to a co-worker regarding a lunch order
    - A message that a printer is offline (or back online)
    - A severe weather alert or "Amber Alert" sent by external agencies

- **USSS employees are prohibited from conducting official business using chat, text, or instant messaging unless they take any additional steps that may be appropriate to establish and maintain a separate record of the communication.** Much like in-person or telephonic conversations, if substantive business communications between USSS employees are made via chat/text/instant message, they must be formally transacted/documented in a more

permanent medium (such as an e-mail or written memorandum). Examples of affected messages include:

- Messages sent or received in emergency or exigent circumstances
- Messages sent or received in a law enforcement (e.g., undercover) capacity

In most cases, the sender and/or the recipient can meet this obligation by capturing the content of a message, pasting it into an e-mail, and sending the e-mail to a USSS e-mail address within 20 days of the creation or transmission of the record. This will allow the content to be managed consistent with a user's (b)(7)(E) or (b)(7)(E) status.

- On a computer: Press the [Control] and [Print Screen] to capture an image of the screen that can be pasted into an e-mail; or block the text, copy it, and paste it into an e-mail.
- On agency issued smartphones, press the designated key/button combination to capture a screen shot. (E.g., press the sleep/wake/power button (at the top-right or on top of your device) and press the Home button (below the screen) at the same time. The screen shot will be stored in your Photos folder and can be sent from your smartphone as an attachment to a USSS e-mail.)

Use of Text, Chat, or Instant Messages in Protective Operations

Particularly in scenarios involving text messages sent by a protectee to protective detail personnel, the use of non-e-mail based electronic messaging technologies in protective operations can raise potential issues related to recordkeeping law, technical security, and rules of evidence.

Generally, the electronic correspondence of many protectees is governed by the Presidential Records Act, and as such is not stored or maintained as a Federal record by USSS personnel. However, even informal non-record correspondence between a protectee and USSS personnel may be examined as evidence by investigative and/or oversight officials, should an unusual protective event occur. Likewise, the security and integrity of non-USSS approved devices should not be taken for granted.

USSS employees are strongly encouraged to preempt these issues to the greatest extent possible, via consultation with the USSS Office of the Chief Counsel, as well as discussion with technical/IT staff counterparts.

Any correspondence content must remain formal and professional at all times, even for informal non-record correspondence between a protectee and USSS personnel.

Use of Text, Chat, or Instant Messages in Investigations

The use of non-e-mail based electronic messaging technologies in investigative operations can raise additional issues related to criminal discovery and the admissibility of evidence. USSS employees are strongly encouraged to preempt these issues to the greatest extent possible. Accordingly, when communicating in such a manner with witnesses, victims, or undercover sources USSS investigators should consult with the relevant U.S. Attorney's Office to determine if any additional steps – such as maintaining non-e-mail based electronic messaging files in their native format – will be required to satisfy criminal discovery requirements or to assist in the authentication of evidence.

For more information, USSS employees must either contact the Office of Chief Counsel, or consult with the relevant U.S. Attorney's Office. An additional resource is the written guidance produced by the Department of Justice and Administrative Office of the U.S. Court Joint Working Group on Electronic Technology in the Criminal Justice System: "Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases" created in February 2012. Be sure to check the Working Groups webpage to ensure you are using the most up-to-date guidance. However, USSS employees should be aware that individual judicial districts may vary in their ESI discovery practices, hence the need to engage with the relevant U.S. Attorney's Office.

Non-USSS / Non-DHS E-Mail Messaging Accounts

The following provisions of DHS Directive 142-03 apply to non-DHS e-mail accounts:

- DHS employees may not use non-DHS e-mail accounts to create or send e-mails that constitute DHS records. In case of an exigency, employees may use a non-DHS e-mail account, but thereafter must ensure the e-mail record is submitted to an official DHS e-mail account within 20 days (by forwarding or cc'ing of the DHS account). In cases of intentional violation of this requirement, disciplinary action as determined by the appropriate supervisor is authorized (Title 5, U.S.C., Chapter 75). Once the employee has ensured the capture of the e-mail information in the DHS account, the DHS e-mail must be removed from the non-official e-mail account.

- DHS employees who are on detail to another agency may use that agency's e-mail system to send e-mails during the course of their detail. This permission also extends to task force, working group, or other project or application-based e-mail accounts established by another Federal agency for use by DHS employees.

- Auto-forwarding or redirecting of DHS e-mail to any e-mail address outside of the .gov or .mil domain is prohibited. DHS employees may manually forward individual messages after determining that the risks or consequences are minimal.

- The use of Internet Webmail (e.g., Gmail, Yahoo, and AOL) or other personal e-mail accounts is not authorized over DHS-furnished equipment or network connections.

Appendix A:
USSS (b)(7)(E) E-Mail Retention Schedule Provisions

E-mail Managed under a (b)(7)(E) Approach – U.S. Secret Service
(Citation: GRS 6.1-0087-2018-0001)

This schedule applies to all e-mail, regardless of how the e-mail messages are managed or what e-mail technology is used. E-mail, in the context of this schedule, also includes any associated attachments. This schedule may apply to records affiliated with other commonly available functions of e-mail programs such as calendars/appointments, tasks, and chat.

Records Description	Disposition Instruction	Disposition Authority
E-mail of (b)(7)(E) officials. (b)(7)(E) Officials are senior officials designated by account level or by e-mail addresses (whether the addresses are based on an individual's name, title, a group, or a specific program function) and consist of the following personnel: • Director • Deputy Director • Chief Operating Officer • Assistant Director-Protective Operations • Assistant Director-Investigations • Assistant Director-Intergovernmental and Legislative Affairs • Assistant Director-Professional Responsibility • Assistant Director-Strategic Intelligence and Information • Assistant Director-Training • Chief Technology Officer • Chief Financial Officer • Chief Strategy Officer • Chief Human Resources Officer • Chief Information Officer • Chief Counsel • Chief Integrity Officer • Director of Communications and Media Relations This includes those officials in an acting capacity for any of the above positions longer than 60 days. The agency may also include individual emails from otherwise temporary accounts appropriate for permanent disposition in this category.	**Permanent.** Cut off in accordance with agency's business needs. Transfer to NARA 15 years after cutoff, or after declassification review (when applicable), whichever is later.	GRS 6.1, item 010

If a (b)(7)(E) official has more than one agency-administered e-mail account, this item applies to all accounts. If a (b)(7)(E) official has an e-mail account managed by other staff (such as personal assistants, confidential assistants, or administrative assistants), this item applies to those accounts. This item applies to all e-mail regardless of the address names used by the (b)(7)(E) official for agency business, such as nicknames or office title names Not media neutral; applies to records managed in an electronic format only.		
Official Messages. Accounts established for each Secret Service office which provide formal accounts of Executive level decisions and communications, as well those at other managerial levels within the organization.		
• USSS Official Message Accounts - Directorate level and above (2001-2017)	**Permanent.** Cut off in accordance with agency's business needs. Transfer to NARA 15 years after cutoff, or after declassification review (when applicable), whichever is later.	GRS 6.1, Item 010
• Other USSS Official Message Accounts	**Temporary.** Delete when 7 years old, but longer retention is authorized if required for business use.	GRS 6.1, Item 011
E-mail of (b)(7)(E) Officials. E-mail of all other officials, staff, and contractors not included above.	**Temporary.** Delete when 7 years old, but longer retention is authorized if required for business use.	GRS 6.1, Item 010