Appointment

**From:** (b)(6), (b)(7)(C)

**Sent:** 11/24/2021 12:56:57 AM

**To:** (b)(6), (b)(7)(C)

**CC:** (b)(6), (b)(7)(C)

**Subject:** Review and update CBP Response to NARA Unauthorized Disposition open case

**Attachments:** URGENT - RE: Short Suspense - due noon 11/24/21 - RE: DHS/CBP RIM's response to the NARA Unauthorized Disposition Letter & FW: Draft C1 Memo & Training slides - RE: After Actions & Questions -

**Location:** available by phone after noon

**Start:** 11/24/2021 1:30:00 PM

**End:** 11/24/2021 2:30:00 PM

**Show Time As:** Tentative

**Required Attendees:** (b)(6), (b)(7)(C)

**Optional Attendees:**

**Please forward as you deem appropriate.**

**Meeting Purpose**:

1. Ensure understanding of the risks to CBP in the use of WhatsApp or similar messaging apps
2. Review draft CBP response to NARA Unauthorized Disposition open case
3. Update listed corrective actions with specific CAPA language including lead office, definition of done, and target completion dates:
4. Identify responsible team for:
    a. Completing technical Long term / interim solution

b. Receiving requests and approving / denying requests for access to WhatsApp (or similar messaging apps) on their devices
c. Granting access, providing instruction (training slides) for how to conduct manual record retention
d. Creation, maintenance, and distribution of WhatsApp guidance and documentation
e. Conducting oversight on compliance with manual record retention
f. Communicating applicable laws and regulations on the use of messaging apps to DHS / CBP wide
g. Creating C1 memo, routing through review process, working with OIT Correspondence to route up to C1 for signature and distribution
h. Creating CBP level policy to align with DHS policy on use of messaging apps
i. Creating and maintaining list of apps that have been blocked by CBP
j. Creating and maintaining list of users that have been granted access to use WhatsApp (or similar messaging apps)
k. ...

---

# Microsoft Teams meeting

**Join on your computer or mobile app**
Click here to join the meeting

**Or call in (audio only)**
(b)(6), (b)(7)(C) United States, Arlington
Phone Conference ID: (b)(6), (b)(7)(C)
Find a local number | Reset PIN

This Teams Meeting is hosted on a U.S. Government information system and is provided for U.S. Government-authorized use only. Unauthorized or improper use or access of this system may result in disciplinary action as well as civil and criminal penalties.

Learn More | Meeting options

---

Message

**From:** (b)(6), (b)(7)(C)

**Sent:** 11/23/2021 6:31:57 PM

**To:**

**CC:** (b)(6), (b)(7)(C)

**Subject:** URGENT - RE: Short Suspense - due noon 11/24/21 - RE: DHS/CBP RIM's response to the NARA Unauthorized Disposition Letter & FW: Draft C1 Memo & Training slides - RE: After Actions & Questions -

**Attachments:** 111821.1406 MacNeil edits NARA-Letter-Response.docx; INC0963540 - WhatsApp installation request

**Importance:** High

XD (b)(6), (b)(7)(C)

*Thank you for your input, I have included it here.*

XD (b)(6), (b)(7)(C)

*I have included you here because the **CTO was cited as having responsibilities related to the tracking, approval, and management of WhatsApp access**. The use of WhatsApp and how CBP is managing that use is subject of an OIG Audit and an open case with NARA against CBP alleging CBP has, and is continuing, to conduct Unauthorized Disposition of Federal Records generated by the use of WhatsApp and similar messaging apps.*

XD (b)(6), (b)(7)(C)

*Please also weigh-in.*

In reviewing ENTSD's and the SOC's attached responses to the open NARA Unauthorized Disposition Letter (and OIT's milestones in the CAP against the OIG report) there are definite process gaps and disagreement on which OIT Directorate has responsibility for significant and required actions. It appears that the **CTO (XD (b)(6), (b)(7)(C) included here)** also has a role in the overall process.

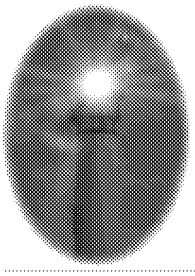
Just a portion of SOC's response highlights the gaps and disconnects: The SOC doesn't approve or take any action regarding WhatApp requests. When a request comes into the SOC, it is forwarded to **CTO who manages the TRM and ENTSD** who manages mobile devices.
**CTO manages the TRM, where WhatApp is listed as Restricted**. Recommend that a list of authorized users be maintained by CTO. CSD is not aware of the existence of this list.

The SOC also does not add approved users to AD. I believe this is done by ENTSD. It is not a SOC responsibility.

**Is it possible to get the SOC, ENTSD, and the CTO stakeholders together on a call to determine how CBP can answer the requirements and identify POCs and expected due dates – ASAP?**

The response will be reviewed with the **aDAC on 11/26/21 Friday**, and the **AC on 11/29/21 Monday**. It will then go to **CIO** (b)(6), (b)(7)(C) for review before being submitted to NARA. The response will be considered publicly available information and several citizen action groups such as (b)(6), (b)(7)(C) will be looking for the DHS/CBP response.

(b)(6), (b)(7)(C), CBP Chief Records Officer
Records and Information Management Program (RIM)
DHS/CBP/OIT/RIM
(C) (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
RIM Website | Request RIM Service! | Email Us



Shine a Light

Suicide Prevention and Awareness

**National Suicide Prevention Lifeline**
800-273-8255
**CBP Employee Assistance Program**
800-755-7002


**From:** (b)(6), (b)(7)(C)
**Sent:** Tuesday, November 23, 2021 12:55 PM
**To:** (b)(6), (b)(7)(C)
**Cc:** (b)(6), (b)(7)(C)

# (b)(6), (b)(7)(C)

**Subject:** RE: Short Suspense - due noon 11/24/21 - RE: DHS/CBP RIM's response to the NARA Unauthorized Disposition Letter & FW: Draft C1 Memo & Training slides - RE: After Actions & Questions -

A determination is needed on exactly who should be approving the WhatsApp requests. Historically these have been sent to the SOC and then an email has come back with the approval. ENTSD created the Active Directory security group allowing for users to be added an removed as needed. This Active Directory security group can be maintained by anyone with granted access. If the SOC is not going to be the group to do this, a determination is needed asap as to who it will be (I see CTO office referenced in this most recent response).

Please also see the attached escalated request where someone in Honduras is requesting WhatsApp. Not sure who is approving it at this point.

(b)(6), (b)(7)(C)
Director, Mobility and Collaboration Branch (MCB)
DHS | CBP | ES | OIT | ENTSD
Work: (b)(6), (b)(7)(C)
Mobile (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)

**From:** (b)(6), (b)(7)(C)
**Sent:** Tuesday, November 23, 2021 12:47 PM
**To:** (b)(6), (b)(7)(C)
**Cc:** (b)(6), (b)(7)(C)
**(b)(6), (b)(7)(C)**
**Subject:** RE: Short Suspense - due noon 11/24/21 - RE: DHS/CBP RIM's response to the NARA Unauthorized Disposition Letter & FW: Draft C1 Memo & Training slides - RE: After Actions & Questions -

(b)(6), (b)(7)(C)

I've attached the document with comments from CSD and SOC perspective. Some comments reflect disagreement with areas of responsibility and recommend formalizing those roles and responsibilities. Thanks

(b)(6), (b)(7)(C)

(b)(6), (b)(7)(C)
Acting Chief Information Security Officer
Acting Executive Director, Cybersecurity Directorate
Office of Information and Technology
U.S. Customs and Border Protection
(b)(6), (b)(7)(C) Mobile
(b)(6), (b)(7)(C)

**From** (b)(6), (b)(7)(C)
**Sent:** Monday, November 22, 2021 5:04 PM
**To:** (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
**Cc:** (b)(6), (b)(7)(C)
**(b)(6), (b)(7)(C)**

**Subject:** Short Suspense - due noon 11/24/21 - RE: DHS/CBP RIM's response to the NARA Unauthorized Disposition Letter & FW: Draft C1 Memo & Training slides - RE: After Actions & Questions -

XD (b)(6), (b)(7)(C) and team,
The attached email tasker that was distributed on 10/28/21 per AC (b)(6), (b)(7)(C) direction – based on discussions and research CBP RIM has learned that **CSD / SOC** is a stakeholder in the tasker.

**BACKGROUND**: In response to a recent Office of Inspector General (OIG) report, "CBP Targeted Americans with the 2018-2019 Migrant Caravan," a CAP was opened by the OIT ALT that includes implied **actions for the SOC**. The National Archives and Records Administration (NARA) became aware, through multiple media reports and the OIG report, that CBP has been using the messaging software WhatsApp and is deploying the encrypted messaging application Wickr across all components of the agency. Subsequently NARA opened a case against DHS/CBP for Unauthorized Destruction of Records due to use of messaging apps such as WhatsApp.

CBP RIM is working with DHS, USBP, OFO, ENTSD, and others to respond to the NARA case. The CBP RIM response to NARA cites **SOC actions** based on the CAP but also based on discussions with ENTSD (XD (b)(6), (b)(7)(C) cc'd here ) and the Messaging Apps WG that meets on alternate Wednesdays.

**Response due noon, 11/24/21 - Attached for SOC review, comment, or concurrence: The initial draft response will be provided to the aDAC for review and approval on 11/26/21.**

1. Initial draft of DHS/CBP response to the NARA open case letter. 111821.1406 (b)(6), (b)(7)(C) edits NARA-Letter-Response

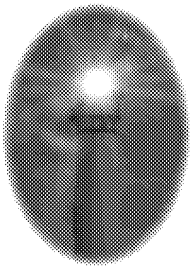
**Due by COB 11/30/21 – Attached for SOC review, comment, or concurrence are**:

1. Proposed edits to the Android/iOS WhatsAppBackup training slides to be included for distribution when SOC approves the use of WhatsApp for users
2. Proposed language for OIT (SOC?) to edit and provide as a C1 memo to communicate with CBP the records management requirements when using messaging apps such as WhatsApp

Please let me know if you have questions on this and/or if someone from the SOC would like to discuss.

Thank you,

(b)(6), (b)(7)(C) CBP Chief Records Officer
Records and Information Management Program (RIM)
DHS/CBP/OIT/RIM
(C) (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
RIM Website | Request RIM Service! | Email Us



Shine a Light

Suicide Prevention and Awareness

**National Suicide Prevention Lifeline**
800-273-8255
**CBP Employee Assistance Program**
800-755-7002

**From:** (b)(6), (b)(7)(C)
**Sent:** Monday, November 22, 2021 3:01 PM
**To:** (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
**Cc:** (b)(6), (b)(7)(C)
# (b)(6), (b)(7)(C)
**Subject:** RE: Draft C1 Memo & Training slides - RE: After Actions & Questions - RE: CBP RIM's response to the NARA Unauthorized Disposition Letter

(b)(6), (b)(7)(C)
The draft of a C1 memo and the edits you made to the draft training materials looks good.

XD:
(b)(6), (b)(7)(C) Is going to schedule a meeting with (b)(6), (b)(7)(C) and the SOC to get any other edits and concurrence of the actions which will be required by the SOC with regard to this audit remediation. These include:

- Edits/concurrence to C1 memo re the need to archive WhatsApp.
- Distribution of the Manual Archiving Training to all existing and future WhatsApp users as the SOC approves/adds people to the AD Security Group (OIG CAP Audit :M-00093 Manual archiving will be required until a solution such as Smarsh or TeleMessage is in place.")
- Edits/concurrence to the NARA response (see previous email).

Thank you

(b)(6), (b)(7)(C)
Director, Mobility and Collaboration Branch (MCB)
DHS | CBP | ES | OIT | ENTSD
Work: (b)(6), (b)(7)(C)
Mobile: (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)

**From:** (b)(6), (b)(7)(C)
**Sent:** Friday, November 19, 2021 6:51 AM
**To:** (b)(6), (b)(7)(C)
**Cc:** (b)(6), (b)(7)(C)
# (b)(6), (b)(7)(C)

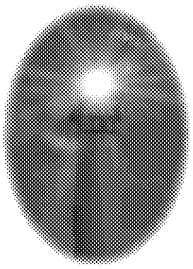
(b)(6), (b)(7)(C)

**Subject:** Draft C1 Memo & Training slides - RE: After Actions & Questions - RE: CBP RIM's response to the NARA Unauthorized Disposition Letter

Good morning,
CBP RIM made edits to the attached WhatsApp training slides – added language in the top box: *Unauthorized disposition of WhatsApp messages can result in criminal prosecution with consequences that include fines and prison. In order to adequately protect these federal records, you must archive them according to the steps outlined below.*
Please let us know if you have questions or concerns with the language that CBPRIM added to the training slides.

Also attached is an initial cut at the C1 memo. The team lifted some of the language from the DHS Directive 141-03 – attached for reference.
**Question**: Will ENTSD call a meeting with RIM, PDO and Policy Directive? Or should we handle edits and input via email exchange?

(b)(6), (b)(7)(C) CBP Chief Records Officer
Records and Information Management Program (RIM)
DHS/CBP/OIT/RIM
(C (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
RIM Website | Request RIM Service! | Email Us



Shine a Light

Suicide Prevention and Awareness

**National Suicide Prevention Lifeline**
800-273-8255
**CBP Employee Assistance Program**
800-755-7002

**From:** (b)(6), (b)(7)(C)
**Sent:** Wednesday, November 17, 2021 8:46 AM
**To:**
**Cc:** (b)(6), (b)(7)(C)
**Subject:** FW: After Actions & Questions - RE: CBP RIM's response to the NARA Unauthorized Disposition Letter
**Importance:** High

Hi (b)(6), (b)(7)(C), see attached and (b)(6), (b)(7)(C) EXCELLENT responses to your questions.

For the NARA ppt, I added slide 8.
I will forward this to (b)(6), (b)(7)(C) to be included in the meeting invite later today unless I hear from you otherwise.

Thanks.

(b)(6), (b)(7)(C)
Executive Director, on detail supporting
Enterprise Networks & Technology Support (ENTSD)
Office of Information and Technology (OIT)
U.S. Customs and Border Protection
Department of Homeland Security
(b)(6), (b)(7)(C) (desk)
(cell)
(b)(6), (b)(7)(C)

To schedule an appointment, please contact (b)(6), (b)(7)(C)

---

**From:** (b)(6), (b)(7)(C)
**Sent:** Tuesday, November 16, 2021 1:11 PM
**To** (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
**Subject:** RE: After Actions & Questions - RE: CBP RIM's response to the NARA Unauthorized Disposition Letter

XD...

Attached are updated draft training guides for existing end users. There is one for Android and one for iOS. These can be further edited by the SOC or RIM as needed.

Other notes are below. Sections from (b)(6), (b)(7)(C) email have been copied below with responses beneath each one in blue:

(b)(6), (b)(7)(C) would **review the NTC WhatsApp Training draft** (attached) to make needed updates and use the deck to 'communicate' 'WhatsApp Record-Keeping' Training
ENTSD::: Attached are updated draft training guides for existing end users. There is one for Android and one for IOS. These can be further edited by the SOC, RIM or Airwatch team as needed.

a. **CBP RIM would like to provide language to Slide 5** with more specific references to NARA regulations and consequences of non-compliance and/or a separate slide altogether to augment Slide 5.

ENTSD::: RIM, please edits the attached draft guides to include the desired language.

b. There is language on **Slides 15 and 27** about the records being 'searchable'. *** That language could be expanded to re-emphasize that records created from messaging apps are subject to FOIA searches, Litigation Holds, Congressional inquiries, etc.

ENTSD::: RIM, please edits the attached draft guides to include the desired language.

c. ??? Can we make this happen or have the plans to utilize the NTC deck changed?

ENTSD::: RIM, please edits the attached draft guides to include the desired language.

It was suggested that **CBP RIM present the CBP RIM slide deck** (attached) during the Wednesday, 11/17/21 Messaging Apps Policy Working Group because CBP's response to the NARA Open Case will reference the Policy and Proposed solution

a. (b)(6), (b)(7)(C) indicated they will **provide CBP RIM with an additional slide** to describe CBP's / ENTSD's proposed response including the pro-active steps being taken to either: replace WhatsApp or bring it into compliance with RIM management requirements; conduct a pilot for the use of Wickr; collaboration within CBP and PDO to address the policy language to support implementation of the 'solution(s)' chosen.

ENTSD::: Suggestion for the SOC, AC, or C1 to send an updated version of the draft manual records retention policies to the WhatsApp users. This good faith effort on how to preserve records manually until we find a more permanent solution will allow the current users to continuing using it and be in compliance with record retention policies. The following corrective actions are being looked at: Additional WhatsApp installations are blocked and only installed after SOC approval, sending instructions to end users on how to manually archive WhatsApp messages, researching 3rd party vendors who offer an automated method of retaining WhatsApp messages, and implementing a small pilot of users that could use the CBP instance of the WICKR messaging application as it includes compliance. Airwatch team has also proactively blocked 41 other messaging applications so there are not similar issues with other messaging platforms.

It was discussed that the **AirWatch** team is responsible for receiving and approving user requests to load WhatsApp onto their devices…

ENTSD::: Correction… the CBP SOC approves WhatsApp messages and will be managing the Active Directory Security Group used to add/remove users (by 11/30/21).

**Question**:

1. **Who is the correct POC** to get insight into how this process is working so it can be included in the CBP response to NARA?

ENTSD::: (b)(6), (b)(7)(C) is the POC for how this is working. The process is:

- As of 11/16/21: request from end user to install WhatsApp is created at TSD and sent to CBP SOC for approval. CBP SOC sends to Airwatch team to have user added to Active Directory Security Group. WhatsApp is automatically added to end user device.
- As of 11/30/21 (and in the OIG Audit response): request from end user to install WhatsApp is created at TSD and sent to CBP SOC for approval. CBP SOC adds user to Active Directory Security Group. WhatsApp is automatically added to end user device. End user would also need to get copy of manual archive training materials.

a. **CBP RIM would like to provide language** into the instructions for executing that process emphasizing NARA regulations and consequences of non-compliance and that records created from messaging apps are subject to FOIA searches, Litigation Holds, Congressional inquiries, etc

ENTSD::: RIM, please edits the attached draft guides to include the desired language.

**From:** (b)(6), (b)(7)(C)
**Sent:** Monday, November 15, 2021 1:45 PM
**To:** (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
**Cc:** (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
**Subject:** After Actions & Questions - RE: CBP RIM's response to the NARA Unauthorized Disposition Letter

(b)(6), (b)(7)(C)

Thank you all for meeting with us last week regarding the NARA Letter / Open Case related to the OIG Audit, Recommendation 6 on messaging apps.

I captured a few after actions per our discussion and I have a couple questions – I have captured below:

**After Actions**:

1. (b)(6), (b)(7)(C) would **review the NTC WhatsApp Training draft** (attached) to make needed updates and use the deck to 'communicate' 'WhatsApp Record-Keeping' Training
    a. **CBP RIM would like to provide language to Slide 5** with more specific references to NARA regulations and consequences of non-compliance and/or a separate slide altogether to augment Slide 5.
    b. There is language on **Slides 15 and 27** about the records being 'searchable'. *** That language could be expanded to re-emphasize that records created from messaging apps are subject to FOIA searches, Litigation Holds, Congressional inquiries, etc.
    c. ??? Can we make this happen or have the plans to utilize the NTC deck changed?
2. It was suggested that **CBP RIM present the CBP RIM slide deck** (attached) during the Wednesday, 11/17/21 Messaging Apps Policy Working Group because CBP's response to the NARA Open Case will reference the Policy and Proposed solution
    a. (b)(6), (b)(7)(C) indicated they will **provide CBP RIM with an additional slide** to describe CBP's / ENTSD's proposed response including the pro-active steps being taken to either: replace WhatsApp or bring it into compliance with RIM management requirements; conduct a pilot for the use of Wickr; collaboration within CBP and PDO to address the policy language to support implementation of the 'solution(s)' chosen.

It was discussed that the **AirWatch** team is responsible for receiving and approving user requests to load WhatsApp onto their devices…

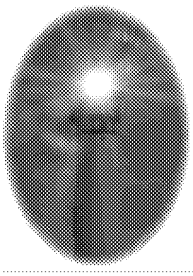
**Question**:

1. **Who is the correct POC** to get insight into how this process is working so it can be included in the CBP response to NARA?
    a. **CBP RIM would like to provide language** into the instructions for executing that process emphasizing NARA regulations and consequences of non-compliance and that records created from messaging apps are subject to FOIA searches, Litigation Holds, Congressional inquiries, etc

Will you please let me know if the actions / suggestions / question above can be accomplished in time for the Wednesday working group meeting and in time for inclusion in CBP's response back to NARA?

Thanks,

(b)(6), (b)(7)(C) CBP Chief Records Officer
Records and Information Management Program (RIM)
DHS/CBP/OIT/RIM
(C (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
RIM Website | Request RIM Service! | Email Us



Shine a Light

Suicide Prevention and Awareness

**National Suicide Prevention Lifeline**
800-273-8255
**CBP Employee Assistance Program**
800-755-7002

-----Original Appointment-----
**From:** (b)(6), (b)(7)(C)
**Sent:** Tuesday, November 9, 2021 3:59 PM
**To:** (b)(6), (b)(7)(C)
**Cc:** (b)(6), (b)(7)(C)
**Subject:** CBP RIM's response to the attached NARA Unauthorized Disposition Letter
**When:** Wednesday, November 10, 2021 11:00 AM-11:30 AM (UTC-05:00) Eastern Time (US & Canada).
**Where:** Microsoft Teams Meeting

Attaching the presentation that (b)(6), (b)(7)(C) just emailed.

(b)(6), (b)(7)(C)
I am requesting 30 mins on XD (b)(6), (b)(7)(C) s calendar to discuss CBP RIM's response to the attached NARA Unauthorized Disposition Letter. The letter was sent from Laurence Brewer Chief Records Officer for the US Government to Eric Hysen Chief Information Officer (CIO), DHS Senior Agency Official for Records Management (SAORM), regarding CBP's planned deployment of WICKR and the information that NARA received in the OIG report, "CBP Targeted Americans with the 2018-2019 Migrant Caravan" regarding the use of WhatsApp. With input from OIT Offices, CBP RIM is the lead for compiling the DHS/CBP response (due 11/12/21) that will go from CIO Hysen to the Laurence Brewer Chief Records Officer for the US Government.

**Purpose of the meeting** with XD (b)(6), (b)(7)(C) is to gain insight into the technical solutions that are being considered; interim solutions and long term solutions. NARA's primary area of concern is the loss of records generated when WhatsApp and similar messaging apps are used. Our deadline is extremely tight due to the multiple levels of reviews the response will have to go through i.e. USBP, OFO, OIT, OCC, DHS SAORM… I want to ensure XD (b)(6), (b)(7)(C) is aware of our conclusions to-date and try to identify POCs within ENTSD that CBP RIM can meet with that have firsthand knowledge of the actions being taken: technical/manual solution, policy creation, training, communication, enforcement, consequences…

The CBP RIM response needs to address current status of the lost records, actions and timelines CBP is taking to 'manage' retention of records generated using messaging apps such as WhatsApp, creation of a NARA approved schedule that is compatible with the technical solutions being pursued.

An important distinction is that response to the OIG Report does NOT replace CBP's need to provide response to NARA's Letter.

*** NARA instructed DHS/CBP RIM to provide a response that addresses the following (as contained in the attached letter):

1. Ensure that Records Management regulations are being adhered to
2. Ensure that the CBP is regulating the use of these messaging applications consistent with NARA's and the Department's records management policies
3. Ensure that CBP is communicating to all employees that they cannot use these applications to circumvent their records management responsibilities and that all employees are aware that they must be retaining all messages that are federal records in accordance with agency policy and all applicable NARA-approved records schedules

4. Include a complete description of the records with volume and dates if known; description of the office maintaining the records; a statement of the exact circumstances surrounding the removal, defacing, alteration, or destruction of records; a statement of the safeguards established to prevent further loss of documentation; and details of the actions taken to salvage, retrieve, or reconstruct the records.

DHS/CBP's response must also include Records Management corrective actions that CBP will be required to implement as a result of the OIG investigation.

(b)(6), (b)(7)(C), CBP Chief Records Officer
Records and Information Management Program (RIM)
DHS/CBP/OIT/RIM
(C) (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
RIM Website | Request RIM Service! | Email Us

---

# Microsoft Teams meeting

**Join on your computer or mobile app**
Click here to join the meeting

**Or call in (audio only)**
(b)(6), (b)(7)(C) United States, Arlington
Phone Conference ID: (b)(6), (b)(7)(C)
Find a local number | Reset PIN

This Teams Meeting is hosted on a U.S. Government information system and is provided for U.S. Government-authorized use only. Unauthorized or improper use or access of this system may result in disciplinary action as well as civil and criminal penalties.

Learn More | Meeting options

---

# *NARA Unauthorized Destruction Letter Response Tasker*

*Dawn Watts, CBP Chief Records Officer* | Date: 11/18/2021

**Summary:**

(b)(6), (b)(7)(C) CBP Chief Records Officer; (b)(6), (b)(7)(C) DHS Department Records Officer; and (b)(6), (b)(7)(C) DHS CIO and DHS Senior Agency Official for Records Management received a letter from (b)(6), (b)(7)(C) Chief Records Officer of the U.S. Government regarding CBP's planned deployment of Wickr and use of WhatsApp and possible unauthorized destruction of records as referenced in OIT Audit "CBP Targeted Americans with the 2018-2019 Migrant Caravan."

The letter requires a CBP response within 30 days to include:

- A report documenting the unauthorized disposition
- Assurance that Records and Information Management (RIM) regulations are being adhered to
- Assurance that CBP is communicating to all employees that messages are federal records and must be retained as such
- Records Management corrective actions CBP will implement in response to OIG audit –
    - To include creation of a NARA approved Records Retention Schedule for all messaging applications
- Any documentation in form of policy, training, approved records schedule, and any other mitigating resources.

**Request:**

Review and provide comments on CBP's draft response to the NARA Letter via track changes or adding comments in the table below. The table provides the draft response including the word-for-word request from NARA in the left column with the proposed language drafted by CBP RIM in response to each section of the NARA Letter in the right column.

**Comments are due by NOON, Monday, November 22nd.** No response indicates concurrence.

| | NARA Letter Paragraphs | Proposed CBP RIM Response |
|---|---|---|
| 1 | The National Archives and Records Administration (NARA) has become aware, through multiple media reports and the recent Office of Inspector General (OIG) report, "CBP Targeted Americans with the 2018-2019 Migrant Caravan," that the Customs and Border Protection (CBP) has been using the messaging software WhatsApp and is deploying the encrypted messaging application Wickr across all components of the agency. Accordingly, I wanted to reach out to ensure that records management regulations are being adhered to and to ensure that the CBP is regulating the use of these messaging applications consistent with NARA's and the Department's records management policies. I also wanted to ensure that CBP is communicating to all employees that they cannot use these applications to circumvent their records management responsibilities and that all employees are aware that they must be retaining all messages that are federal records in accordance with agency policy and all applicable NARA-approved records schedules. | See response to paragraph 6 and 7. |
| 2 | With respect to WhatsApp, the OIG report notes that their ability to determine whether proper processes and procedures were followed was hampered by a failure to retain communication records, including records in WhatsApp (page 4). Further, the OIG report states that there are "instances of CBP officers not documenting information they obtained during caravan-related inspections" (page 12); that CBP officials did not retain communication records (page 17); and that "the CBP officials failure to retain WhatsApp messages likely violated DHS and CBP records retention policies because the messages were information that CBP created or received in carrying out its mission and contained substantive information that was necessary to adequately and properly document the activities and functions of the CBP officials" (page 28). Additionally, the OIG report found | See response to paragraph 6. |

| | NARA Letter Paragraphs | Proposed CBP RIM Response |
|---|---|---|
| | that during this operation, it is not even clear if CBP policies permit the use of WhatsApp. | |
| 3 | With respect to Wickr, NARA is concerned about the use of this messaging application as it has the capability to auto-delete messages after a specified period of time has passed. In light of the information in the OIG report, NARA is concerned about agency-wide deployment of a messaging application that has this functionality without appropriate policies and procedures governing its use. | See response to paragraph 6. |
| 4 | DHS employees using these applications without complying with established recordkeeping requirements expose the Department to the risk of potential unauthorized destruction of records. As a reminder, all actual or impending instances of unauthorized disposition must be reported to NARA per the requirements in 36 CFR Part 1230. | See response to paragraph 5. |
| 5 | In accordance with 36 CFR Part 1230.14, CBP must respond to this letter with a report documenting the unauthorized disposition of the federal records that were identified in the OIG report. At a minimum, this report must include<br>a. a complete description of the records with volume and dates if known;<br>b. description of the office maintaining the records;<br>c. a statement of the exact circumstances surrounding the removal, defacing, alteration, or destruction of records; | a. MORE INFORMATION NEEDED Given the widespread use of WhatsApp during the time period from October 2018 to February 2019 investigated in the OIG Report, an unknown number of WhatsApp messages were deleted or lost from the devices of several CBP Officials supporting the Emergency Operations Center (EOC) for Operation located in San Diego, CA. A complete description of the records with volume and dates is unknown. Records include but are not limited to communications between CBP and local Mexican officials. (OIG Report, pages 2, 29)<br>b. MORE INFORMATION NEEDED<br>c. MORE INFORMATION NEEDED Though the exact circumstances are not known, the OIG Report states that CBP officials communicated with the Mexican government and that the text messages were most likely related to possible requests to deny |

| | NARA Letter Paragraphs | Proposed CBP RIM Response |
|---|---|---|
| | | entry to US Citizens that were being investigated as part of the 2018–2019 Migrant Caravan. In some instances, the messages were deleted by CBP Officials and in another instance the messages were deleted due to issues caused by the upgrade of the mobile device. (OIG Report, pages 21,22,23,28,29) |
| | d. a statement of the safeguards established to prevent further loss of documentation; | d. CBP is currently working on multiple actions to establish safeguards to prevent the future loss of messages, including restricted access to the WhatsApp tool, training on the manual retentions of records, and investigation into tools to automatically capture messages from WhatsApp for records retention needs. *Additional information can be found in the response to paragraph 6.* |
| | e. and details of the actions taken to salvage, retrieve, or reconstruct the records. | e. MORE INFORMATION NEEDED REGARDING TECHNICAL FUNCTIONALITY Due to the nature of WhatsApp functionality, there is no practical way to salvage, retrieve or reconstruct these records. *Additional information can be found in the response to paragraph 6.* |
| 6 | This report must also include any records management corrective actions that CBP will be required to implement as a result of the OIG investigation. | CBP RIM will be contributing to the records management aspect of the response to Recommendation 6 from the OIG Report:<br><br>***Recommendation 6**: Take immediate action to end the use of WhatsApp for operational purposes or to ensure that WhatsApp messages are retained in compliance with legal and policy requirements including records retention schedules.*<br><br>***CBP Response to Recommendation 6:** Concur. CBP's Office of Information and Technology will explore the viability of the continued operational use of WhatsApp, which will include looking for a replacement. Office of Information and Technology is currently piloting a managed messaging platform to replace WhatsApp. CBP is currently working on an operational pilot. CBP expects to complete these actions by December 31, 2021.* |

| | NARA Letter Paragraphs | Proposed CBP RIM Response |
|---|---|---|
| | | ***OIG Analysis:*** *We consider these actions responsive to the intent of Recommendation 6, which is resolved and open. We will close this recommendation when CBP provides documentation showing the results of its pilot to replace WhatsApp and to ensure that messages are retained in compliance with legal and policy requirements including records retention schedules.*<br><br>**Action 1: (Assigned to CBP RIM)**<br><br>**CBP RIM will develop a retention schedule/s covering Messaging Applications and submit to NARA for approval.**<br><br>CBP RIM is currently developing a retention schedule covering records created by messaging applications. CBP RIM will gather feedback from any stakeholders with equity in the schedule (such as CBP OIT) to ensure the retention meets CBP business needs and is implementable within the organization. It is CBP RIM's intent to submit this schedule for NARA approval during Fiscal Year 2022.<br><br>**Action 2: (Assigned to CBP Office of Information and Technology (OIT))**<br><br>**CBP will provide updated guidance to WhatsApp users about archiving messages.**<br><br>Until WhatsApp messaging capture technology is deployed (see Action 3), CBP WhatsApp users will be reminded of the requirement to manually capture messages and store them in an official CBP account. CBP RIM will work with CBP OIT to develop updated guidance and documentation on how to manually capture WhatsApp messages. CBP OIT will distribute this updated documentation to all WhatsApp users. This will ensure that users are aware of the records management policies regulating use of this application, and that they must retain all messages that are federal records in accordance with agency policy and all applicable NARA-approved records schedules.<br><br>**Action 3: (Assigned to CBP OIT)**<br><br>**Update the approval process for user access to messaging applications.** |

| | NARA Letter Paragraphs | Proposed CBP RIM Response |
|---|---|---|
| | | Currently, CBP users must submit an IT Service Desk request to obtain WhatsApp installation permission on their CBP devices. As of 11/30/2021, all requests will go through the CBP Security Operations Center (SOC) for approval. Once approved, users will receive the updated guidance on their message archiving responsibilities. In addition to this approval process, CBP OIT has proactively blocked 41 other messaging applications from installation to minimize future issues.<br><br>**Action 4: (Assigned jointly to CBP RIM and CBP OIT)**<br><br>**CBP RIM will work with CBP OIT to implement the approved retention schedule/s for Wickr, WhatsApp, and similar messaging applications in the appropriate technology.**<br><br>CBP is responding to the OIG Audit Recommendation 6 on two fronts. The first involves continuing the deployment of the Enterprise version of the Wickr communication application for potential replacement of some WhatsApp instances. The Enterprise version of Wickr captures all messages to and from CBP personnel and stores them in a central repository. This version captures messages from Wickr instances even if they have been configured for immediate deletion. The repository contains compliance functionality, allowing retention periods to be configured for messages. CBP RIM will work with CBP OIT to implement the appropriate retention schedule after NARA approval. This is currently the Wickr version in use at CBP and all messages are currently retained indefinitely until CBP RIM has an approved retention schedule to implement.<br><br>The second front involves the acquisition and implementation of technology to capture WhatsApp messages and store them in a central repository. Once the messages are stored in the repository, retention rules can be applied to messages based on the approved schedule. This solution will allow continued use of WhatsApp in instances where it is necessary for the mission while applying all appropriate retention rules and functionality that will prevent unauthorized disposition. Once the technology is acquired and implemented by CBP OIT, CBP RIM will work with CBP OIT to implement the appropriate NARA-approved retention schedule.<br><br>CBP RIM will work with CBP OIT to identify and appropriately retain messages from similar messaging applications. |

| | NARA Letter Paragraphs | Proposed CBP RIM Response |
|---|---|---|
| | | **Action 5: (Assigned to CBP RIM and CBP OIT)**<br><br>**CBP will send reminders to all users about employee obligations for managing records in official and non-official accounts and the consequences of unauthorized disposition.**<br><br>CBP RIM will work with CBP OIT to develop a reminder message for all CBP users about their obligations for retaining messaging records according to CBP and DHS policy as well as all applicable NARA-approved records schedules. The reminder message will include references to the consequences of unauthorized disposition and notification obligations if it occurs. The message will be sent by the appropriate CBP authority. |
| 7 | Additionally, please include in your report any documentation in the form of policies, training, approved records schedules or other resources CBP has established to mitigate the records management risk associated with the improper use of Wickr, WhatsApp, or similar messaging applications. | **Polices and Training**<br><br>**DHS Policy Directive 141-03** directs DHS employees that:<br><br>*All DHS business transactions by electronic means are required to comply with the Department's records management policies. DHS employees should take steps to establish and maintain federal records when conducting business using chat, text, or instant messaging.*<br><br>**CBP's Records and Information Management Directive and updated Records and Information Management Handbook** were published in June 2019. CBP RIM is currently reviewing and updating both documents with publication expected in 2022.<br><br>In the CBP RIM Handbook, CBP users are directed to do the following for Electronic Messages in non-official CBP accounts (Part 3, Section M):<br><br>*All CBP email and messaging accounts contain federal records. This includes email accounts with multiple users (such as public correspondence email addresses) or email accounts for an individual on multiple systems (such as classified and unclassified email accounts), text, and instant messaging, including third party applications (such as Twitter, Instagram, and Snapchat). All email and messaging created in the course of conducting CBP business is a record, and is treated like any other record. (To determine its retention period, refer to the file plans under the record category to which it pertains.) …* |

| | NARA Letter Paragraphs | Proposed CBP RIM Response |
|---|---|---|
| | | • *In 2014, the Federal Records Act was amended to require that officers and employees may not create or send a record using a non-official electronic messaging account unless they:*<br>  ○ *Copy an official electronic messaging account of the officer or employee in the original creation or transmission of the record; or*<br>  ○ *Forward a complete copy of the record to an official electronic messaging account of the officer or employee no later than 20 calendar days after the original creation or transmission of the record.*<br>• *NARA guidance further requires that if an officer or employee of an executive agency receives electronic messages on a personal account, they must forward a complete copy of the record to an official electronic messaging account of the officer or employee no later than 20 calendar days after the original creation or transmission of the record.*<br><br>**CBP RIM's "RIM 101" training deck** is available to CBP employees and contractors on the CBP RIM internal website. Included in this deck are references to the topics mentioned above from the CBP RIM Directive and CBP RIM Handbook. CBP Employees are required to take annual records management training developed by DHS. That training does not mention specific responsibilities about records management for messaging applications, but it does remind employees about the requirement to send email records from non-DHS accounts to a DHS account within 20 days of creation ("What is a Federal Record?" slides in the Records Management for Everyone training). DHS RIM is actively updating this training.<br><br>CBP has established a **Messaging Applications Policy Working Group** to define a comprehensive Secure Messaging Platform policy. CBP RIM is participating in this working group to provide the proper records management requirements for inclusion in the policy. |

[Mock-up of response format]

## Unauthorized Disposal Report

**MORE INFORMATION NEEDED** Given the widespread use of WhatsApp during the time period from October 2018 to February 2019 investigated in the OIG Report, an unknown number of WhatsApp messages were deleted or lost from the devices of several CBP Officials supporting the Emergency Operations Center (EOC) for Operation located in San Diego, CA. A complete description of the records with volume and dates is unknown. Records include but are not limited to communications between CBP and local Mexican officials.

**MORE INFORMATION NEEDED** describing the office that maintains these records.

**MORE INFORMATION NEEDED** Though the exact circumstances are not known, the OIG Report states that CBP officials communicated with the Mexican government and that the text messages were most likely related to possible requests to deny entry to US Citizens that were being investigated as part of the 2018–2019 Migrant Caravan. In some instances, the messages were deleted by CBP Officials and in another instance the messages were deleted due to issues caused by the upgrade of the mobile device.

CBP is currently working on multiple actions to establish safeguards to prevent the future loss of messages, including restricted access to the WhatsApp Messaging Application, training on the manual retentions of records, and investigation into tools to automatically capture messages from WhatsApp for records retention needs.

**MORE INFORMATION NEEDED REGARDING TECHNICAL FUNCTIONALITY** Due to the nature of WhatsApp functionality, there is no practical way to salvage, retrieve or reconstruct these records.

## CBP Plan of Action

CBP RIM will be contributing to the records management aspect of the response to Recommendation 6 from the OIG Report:

***Recommendation 6****: Take immediate action to end the use of WhatsApp for operational purposes or to ensure that WhatsApp messages are retained in compliance with legal and policy requirements including records retention schedules.*

***CBP Response to Recommendation 6:*** *Concur. CBP's Office of Information and Technology will explore the viability of the continued operational use of WhatsApp, which will include looking for a replacement. Office of Information and Technology is currently piloting a managed messaging platform to replace WhatsApp. CBP is currently working on an operational pilot. CBP expects to complete these actions by December 31, 2021.*

***OIG Analysis:*** *We consider these actions responsive to the intent of Recommendation 6, which is resolved and open. We will close this recommendation when CBP provides documentation showing the results of its pilot to replace WhatsApp and to ensure that messages are retained in compliance with legal and policy requirements including records retention schedules.*

**Action 1: (Assigned to CBP RIM)**

**CBP RIM will develop a retention schedule/s covering Messaging Applications and submit to NARA for approval.**

CBP RIM is currently developing a retention schedule covering records created by messaging applications. CBP RIM will gather feedback from any stakeholders with equity in the schedule (such as

CBP OIT) to ensure the retention meets CBP business needs and is implementable within the organization. It is CBP RIM's intent to submit this schedule for NARA approval during Fiscal Year 2022.

**Action 2: (Assigned to CBP Office of Information and Technology (OIT))**

**CBP will provide updated guidance to WhatsApp users about archiving messages.**

Until WhatsApp messaging capture technology is deployed (see Action 3), CBP WhatsApp users will be reminded of the requirement to manually capture messages and store them in an official CBP account. CBP RIM will work with CBP OIT to develop updated guidance and documentation on how to manually capture WhatsApp messages. CBP OIT will distribute this updated documentation to all WhatsApp users. This will ensure that users are aware of the records management policies regulating use of this application, and that they must retain all messages that are federal records in accordance with agency policy and all applicable NARA-approved records schedules.

**Action 3: (Assigned to CBP OIT)**

**Update the approval process for user access to messaging applications.**

Currently, CBP users must submit an IT Service Desk request to obtain WhatsApp installation permission on their CBP devices. As of 11/30/2021, all requests will go through the CBP Security Operations Center (SOC) for approval. Once approved, users will receive the updated guidance on their message archiving responsibilities. In addition to this approval process, CBP OIT has proactively blocked 41 other messaging applications from installation to minimize future issues.

**Action 4: (Assigned jointly to CBP RIM and CBP OIT)**

**CBP RIM will work with CBP OIT to implement the approved retention schedule/s for Wickr, WhatsApp, and similar messaging applications in the appropriate technology.**

CBP is responding to the OIG Audit Recommendation 6 on two fronts. The first involves continuing the deployment of the Enterprise version of the Wickr communication application for potential replacement of some WhatsApp instances. The Enterprise version of Wickr captures all messages to and from CBP personnel and stores them in a central repository. This version captures messages from Wickr instances even if they have been configured for immediate deletion. The repository contains compliance functionality, allowing retention periods to be configured for messages. CBP RIM will work with CBP OIT to implement the appropriate retention schedule after NARA approval. This is currently the Wickr version in use at CBP and all messages are currently retained indefinitely until CBP RIM has an approved retention schedule to implement.

The second front involves the acquisition and implementation of technology to capture WhatsApp messages and store them in a central repository. Once the messages are stored in the repository, retention rules can be applied to messages based on the approved schedule. This solution will allow continued use of WhatsApp in instances where it is necessary for the mission while applying all appropriate retention rules and functionality that will prevent unauthorized disposition. Once the technology is acquired and implemented by CBP OIT, CBP RIM will work with CBP OIT to implement the appropriate NARA-approved retention schedule.

CBP RIM will work with CBP OIT to identify and appropriately retain messages from similar messaging applications.

**Action 5: (Assigned to CBP RIM and CBP OIT)**

**CBP will send reminders to all users about employee obligations for managing records in official and non-official accounts and the consequences of unauthorized disposition.**

CBP RIM will work with CBP OIT to develop a reminder message for all CBP Users about their obligations for retaining messaging records according to CBP and DHS policy as well as all applicable NARA-approved records schedules. The reminder message will include references to the consequences of unauthorized disposition and notification obligations if it occurs. The message will be sent by the appropriate CBP authority.

## Supplemental Polices and Training Documentation Summary

**DHS Policy Directive 141-03** directs DHS employees that:

> *All DHS business transactions by electronic means are required to comply with the Department's records management policies. DHS employees should take steps to establish and maintain federal records when conducting business using chat, text, or instant messaging.*

**CBP's Records and Information Management Directive and updated Records and Information Management Handbook** were published in June 2019. CBP RIM is currently reviewing and updating both documents with publication expected in 2022.

In the CBP RIM Handbook, CBP users are directed to do the following for Electronic Messages in non-official CBP accounts (Part 3, Section M):

> *All CBP email and messaging accounts contain federal records. This includes email accounts with multiple users (such as public correspondence email addresses) or email accounts for an individual on multiple systems (such as classified and unclassified email accounts), text, and instant messaging, including third party applications (such as Twitter, Instagram, and Snapchat). All email and messaging created in the course of conducting CBP business is a record, and is treated like any other record. (To determine its retention period, refer to the file plans under the record category to which it pertains.) …*
>
> - *In 2014, the Federal Records Act was amended to require that officers and employees may not create or send a record using a non-official electronic messaging account unless they:*
>   - *Copy an official electronic messaging account of the officer or employee in the original creation or transmission of the record; or*
>   - *Forward a complete copy of the record to an official electronic messaging account of the officer or employee no later than 20 calendar days after the original creation or transmission of the record.*
> - *NARA guidance further requires that if an officer or employee of an executive agency receives electronic messages on a personal account, they must forward a complete copy of the record to an official electronic messaging account of the officer or employee no later than 20 calendar days after the original creation or transmission of the record.*

**CBP RIM's "RIM 101" training deck** is available to CBP employees and contractors on the CBP RIM internal website. Included in this deck are references to the topics mentioned above from the CBP RIM Directive and CBP RIM Handbook. CBP Employees are required to take annual records management training developed by DHS. That training does not mention specific responsibilities about records

management for messaging applications, but it does remind employees about the requirement to send email records from non-DHS accounts to a DHS account within 20 days of creation ("What is a Federal Record?" slides in the Records Management for Everyone training). DHS RIM is actively updating this training.

CBP has established a **Messaging Applications Policy Working Group** to define a comprehensive Secure Messaging Platform policy. CBP RIM is participating in this working group to provide the proper records management requirements for inclusion in the policy.

Message

**From:** (b)(6), (b)(7)(C)

**Sent:** 11/23/2021 5:49:31 PM

**To:**

**CC:** (b)(6), (b)(7)(C)

**Subject:** INC0963540 - WhatsApp installation request

Sir,

(b)(6), (b)(7)(C) located overseas in Honduras and is requesting the mobile application WhatsApp to be install on his device to use communication between fellow CBP officer Overseas. He stated he submitted the request to TRM but they closed those ticket. He requests to be escalated. Please advise

CBPO (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
Device: Iphone
Cell: (b)(6), (b)(7)(C)
Office (b)(6), (b)(7)(C)

Thank you in advance for your assistance

(b)(6), (b)(7)(C)
Team Patriot (Contractor)
TSD Advanced Support -Team Lead
Technology Service Desk
CBP/OIT/FSD/TSD
Desk
Cell: (b)(6), (b)(7)(C)

Appointment

**From:** (b)(6), (b)(7)(C)

**Sent:** 11/28/2021 12:47:54 PM

**To:** (b)(6), (b)(7)(C)

**Subject:** Review & prep for NARA Letter briefing to AC & aDAC

**Attachments:** NARA Letter AC_DAC_211128-dw.pptx; NARA Unauth Disp Report Mockup 211128draft.docx; CBP Response to NARA Letter - from Dawn to AC & aDAC

**Location:** Microsoft Teams Meeting

**Start:** 11/29/2021 2:00:00 PM

**End:** 11/29/2021 3:00:00 PM

**Show Time As:** Tentative

**Required Attendees:** (b)(6), (b)(7)(C)

Review and final updates to:

1. Word version of response to XDs, (b)(6), (b)(7)(C) etc
2. Word version of response – (b)(5)
3. Email status from (b)(6), (b)(7)(C) that AC can forward to CIO Hysen if he so chooses
4. Briefing deck for mtg with AC, etc
5. ?? memo from AC to CBP users of WhatsApp – not sure is XD (b)(6), (b)(7)(C) made updates

---

# Microsoft Teams meeting

**Join on your computer or mobile app**

Click here to join the meeting

**Or call in (audio only)**

(b)(6), (b)(7)(C) United States, Arlington

Phone Conference ID: (b)(6), (b)(7)(C)

Find a local number | Reset PIN

This Teams Meeting is hosted on a U.S. Government information system and is provided for U.S. Government-authorized use only. Unauthorized or improper use or access of this system may result in disciplinary action as well as civil and criminal penalties.

Learn More | Meeting options

---


# NARA Unauthorized Destruction Letter

CBP Records and Information Management Program

November 2021

# NARA Letter Review & Submission

Logistics of DHS / CBP Review and Submission to NARA:

1. CBP Response and status of corrective actions to NARA open case letter will be **public** and **discoverable**
2. CBP response and corrective actions to OIG-21-62 report will be **public** and **discoverable**
3. Review and submission of CBP response – managing expectations:
   a. CBP response due to DHS RIM 12/2/21 – due to NARA 12/10/21 – extension needed?
   b. CBP's response will go through **4 layers of DHS leadership before it reaches CIO Hysen**
      i. CBP CRO (b)(6), (b)(7)(C) >> DHS ARO (b)(6), (b)(7)(C) >> DHS Deputy CDO Carlene Ileto >> DHS CDO (b)(6), (b)(7)(C) >> DHS Deputy CIO (b)(6), (b)(7)(C) >> *THEN* to DHS CIO (b)(6), (b)(7)(C)
      ii. Unclear how CBP visibility into DHS comments / concerns will be shared with CBP RIM before it is sent to NARA
   c. Recommend that AC (b)(6), (b)(7)(C) send **FYI email to CIO** (b)(6), (b)(7)(C) informing him CBP RIM and OIT has compiled the response and will be working on corrective actions with regular status updates to NARA
4. Input solicited and received from:
   a. OIT XDs (significant input) from ENTSD, CTO, CSD / SOC, CBP RIM
   b. USBP-Audit and OFO-Audit (no content contribution / no comment on draft)
5. Draft is with Office of Chief Counsel for approval and Messaging App Policy working group for awareness
6. Unauthorized disposition - **Unauthorized disposal of Federal records is against the law** (44 U.S.C. 3106) and can carry penalties of a fine of $2,000 and up to three years of imprisonment

# NARA Letter Requirements

CBP's response must include:

1. A **report documenting the unauthorized disposition** of the federal records identified in OIG report:
   a. complete description of the records with volume and dates if known
   b. description of the office maintaining the records
   c. statement of the exact circumstances surrounding the removal, defacing, alteration, or destruction of records
   d. statement of the safeguards established to prevent further loss of documentation
   e. details of the actions taken to salvage, retrieve, or reconstruct the records

2. **Records Management corrective actions** that CBP must implement as a result of OIG investigation

3. Any **documentation in the form of policies, training, approved records schedules** or other resources CBP has established to mitigate the records management risk associated with the **improper use of Wickr, WhatsApp, or similar messaging applications**

# CBP Action Required

- **Take immediate action to end the use of WhatsApp** for operational purposes or to ensure that WhatsApp messages are retained
- Ensure **records created outside of a system of record are accessible, preserved, and retained** per a NARA-approved records retention schedule, to be destroyed or transferred at the appropriate time
- Ensure CBP has **communicated to all employees** through policy, training, interim solutions that messaging applications cannot be used to circumvent records management responsibilities and that all messages that are federal records must be retained
- CBP RIM must provide **NARA periodic status** until all corrective actions have been closed

CBP MUST REVIEW OTHER SIMILAR MESSAGING APPS TO ENSURE RECORDS RETENTION REGULATION COMPLIANCE

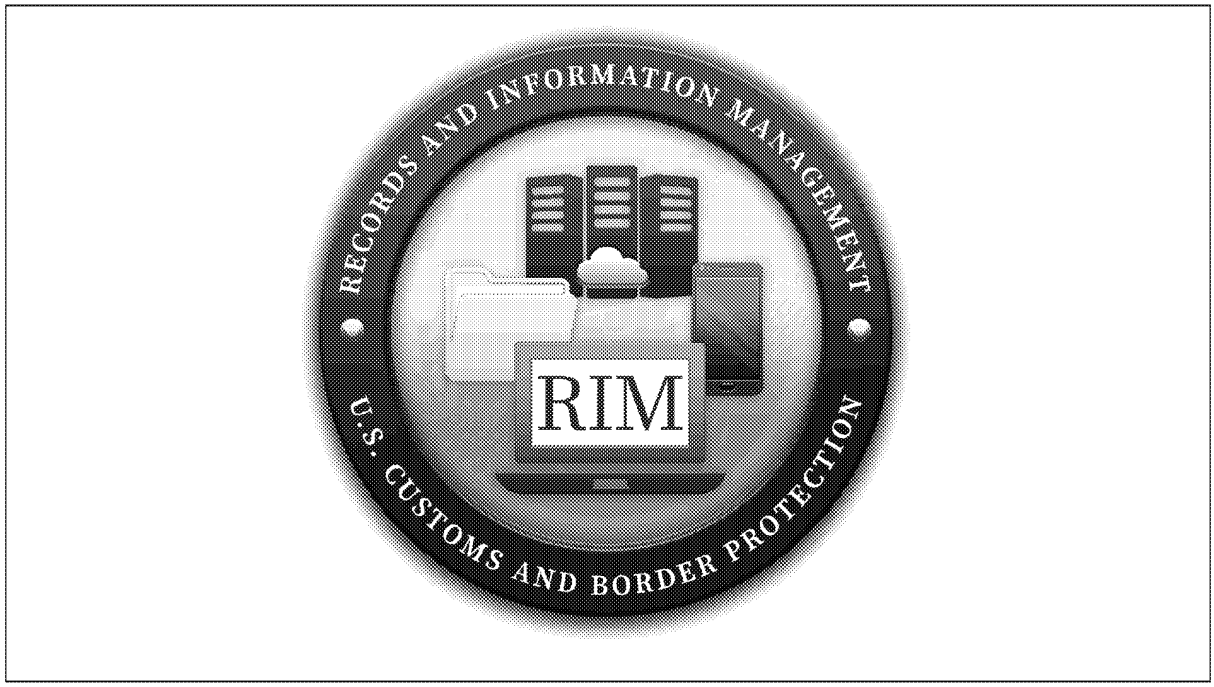
# Actions Completed / In-Progress

**Completed**:

1. Restricted user ability to download WhatsApp
2. Updated approval process to allow for "approved" users to be added in the interim
3. Blocked an additional 41 other known messaging apps from being downloaded
4. Developed manual archiving steps for WhatsApp messages
5. Formed a Messaging Application Policy working group to address

**In-Progress**:

1. Developing communication message to all users advising of records management obligations and the consequences of unauthorized disposition
2. Developing NARA approved retention schedule(s) for messaging apps
3. Researching to determine if other instances of messaging-related unauthorized disposition have occurred, investigate, and if credible, report such instances consistent with regulations.
4. Working with Telemessage to pilot the capture of WhatsApp messages
5. Working with INVNT and user community to pilot Wickr


RECORDS AND INFORMATION MANAGEMENT
RIM
U.S. CUSTOMS AND BORDER PROTECTION

# Unauthorized Destruction

- **Unauthorized disposal** is the **unlawful or accidental** removal, defacing, alteration, or destruction of records **without regard to a NARA approved records schedule**

- **Unauthorized disposal of Federal records is against the law** (44 U.S.C. 3106) and can carry penalties of a fine of $2,000 and up to three years of imprisonment

- CBP RIM must report to NARA any unlawful or accidental removal, defacing, alteration, or destruction of records in the custody of CBP (36 CFR 1230.14)

# NARA Letter Introduction

- (b)(6), (b)(7)(C) Chief Records Officer for the US Government at the National Archives and Records Administration (NARA), **sent a letter** to:
  - (b)(6), (b)(7)(C) Chief Information Officer (CIO), DHS Senior Agency Official for Records Management (SAORM), and
  - (b)(6), (b)(7)(C) CBP Chief Records Officer (CRO)
- Letter regards CBP's **planned deployment of Wickr** and information that NARA received in the Office of Inspector General (OIG) report , "CBP Targeted Americans with the 2018-2019 Migrant Caravan" regarding the **use of WhatsApp** and **possible unauthorized destruction of records.**
- This Letter constitutes formal notice of an opened NARA unauthorized destruction or removal case. CBP must provide the report requested and periodic corrective action status updates to NARA or **be subject to possible referral to Congress.**

# NARA Letter Overview

- The National Archives and Records Administration (NARA) became aware, through multiple media reports and the recent OIG report (21-62) that CBP has been **using the messaging software *WhatsApp* and is deploying the encrypted messaging application *Wickr***.
- Use of these applications ***without complying with established recordkeeping requirements expose the Department to the risk of potential unauthorized destruction of records.***
- All actual or impending instances of unauthorized disposition must be reported to NARA per the requirements in 36 CFR Part 1230.

# OIG Audit Overview

## CBP Targeted Americans with the 2018-2019 Migrant Caravan

- OIG also determined that the CBP officials' failure to retain WhatsApp messages likely violated DHS and CBP records retention policies, because the messages were records.
- **OIG Recommendation 6:** *"Take immediate action to end the use of WhatsApp for operational purposes or to ensure that WhatsApp messages are retained in compliance with legal and policy requirements including records retention schedules."*
- **OIG Analysis of CBP Response to Recommendation 6:** *"…We will close this recommendation when CBP provides documentation showing the results of its pilot to replace WhatsApp and to ensure that messages are retained in compliance with legal and policy requirements including records retention schedules."*

Message

**From:** (b)(6), (b)(7)(C)

**Sent:** 11/28/2021 8:36:56 PM

**To:** (b)(6), (b)(7)(C)

**Subject:** CBP Response to NARA Letter - from Dawn to AC & aDAC

AC (b)(6), (b)(7)(C) and aDAC (b)(6), (b)(7)(C)

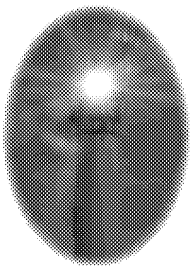
I wanted to give you a quick status update on CBP's response to the NARA Letter regarding the use of WhatsApp and possible unauthorized destruction of records.

1. CBP's response is due to DHS RIM on 12/2/21 and due to NARA 12/10/21
2. CBP RIM has compiled the response report with input and/or concurrence from OIT ENTSD, CTO, CSD / SOC, (b)(5) (b)(5)
3. Actions Completed / In-Progress to address the NARA Letter:
    a. **Completed**:
        i. Restricted user ability to download WhatsApp
        ii. Updated approval process to allow for "approved" users to be added in the interim
        iii. Blocked an additional 41 other known messaging apps from being downloaded
        iv. Developed manual archiving steps for WhatsApp messages
        v. Formed a Messaging Application Policy working group to address
    b. **In-Progress**:
        i. Developing communication message to all users advising of records management obligations and the consequences of unauthorized disposition
        ii. Developing NARA approved retention schedule(s) for messaging apps
        iii. Researching to determine if other instances of messaging-related unauthorized disposition have occurred, investigate, and if credible, report such instances consistent with regulations
        iv. Working with Telemessage to pilot the capture of WhatsApp messages
        v. Working with INVNT and user community to pilot Wickr
4. CBP RIM will be providing **NARA quarterly status updates** until all corrective actions have been closed

Please let me know if you have any questions or would like additional detail.

Thank you,

(b)(6), (b)(7)(C) CBP Chief Records Officer
Records and Information Management Program (RIM)
DHS/CBP/OIT/RIM
(C) (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
RIM Website | Request RIM Service! | Email Us



Shine a Light

Suicide Prevention and Awareness

**National Suicide Prevention Lifeline**
800-273-8255
**CBP Employee Assistance Program**
800-755-7002


RIM

Appointment

**From:** (b)(6), (b)(7)(C)

**Sent:** 11/2/2021 11:26:25 AM

**To:** (b)(6), (b)(7)(C)

**CC:**

**Subject:** NARA Unauthorized Destruction Letter: WhatsApp / Wickr

**Attachments:** RE: CBP Response due Re: NARA Unauthorized Destruction Letter tied to OIG Audit - short suspense; 2021-10-26_UD-2022-0001_DHS-CBP_Open Letter-1301-1b.pdf

**Location:** Microsoft Teams Meeting

**Start:** 11/2/2021 1:15:00 PM

**End:** 11/2/2021 2:00:00 PM

**Show Time As:** Tentative

**Required Attendees:** (b)(6), (b)(7)(C)

**Optional Attendees:**

**Please see attachments**

**Meeting Purpose:**

*** Review NARA Letter and obtain responses and/or identify additional OFO POCs based on instruction from NARA: NARA instructed DHS/CBP to provide a response that addresses the following (as contained in the attached letter):

1. Ensure that Records Management regulations are being adhered to
2. Ensure that the CBP is regulating the use of these messaging applications consistent with NARA's and the Department's records management policies
3. Ensure that CBP is communicating to all employees that they cannot use these applications to circumvent their records management responsibilities and that all employees are aware that they must be retaining all messages that are federal records in accordance with agency policy and all applicable NARA-approved records schedules
4. The final response from CBP must include:
    a. a complete description of the records with volume and dates if known
    b. a description of the office maintaining the records
    c. a statement of the exact circumstances surrounding the removal, defacing, alteration, or destruction of records
    d. a statement of the safeguards established to prevent further loss of documentation
    e. details of the actions taken to salvage, retrieve, or reconstruct the records
5. DHS/CBP's response must also include Records Management corrective actions that CBP will be required to implement as a result of the OIG investigation
6. Additionally, the response must include any documentation in the form of policies, training, approved records schedules or other resources CBP has established to mitigate the records management risk associated with the improper use of Wickr, WhatsApp, or similar messaging applications.

*** Identify which OIG Audit recommendations OFO is responding to and information from CAP that is relevant for inclusion in DHS/CBP response to NARA Letter

**Recommendation 1:** Update Customs Directive No. 4320-003, July 1990 (TECS Directive) to clarify the appropriate bases for placing lookouts and provide training to all CBP officials who have the authority to place lookouts.

**CBP Response to Recommendation 1:** Concur. CBP will update lookout placement procedures in the TECS Directive. Additionally, CBP will modify existing training to inform users that lookouts should only be created for law enforcement purposes. CBP expects to complete these actions by December 31, 2021.

**Recommendation 2:** Develop and implement procedures to ensure CBP officials update and remove lookouts in accordance with the TECS Directive.

**CBP Response to Recommendation 2:** Concur. CBP will update lookout placement procedures in the TECS Directive. In addition, CBP will issue a memorandum and muster to remind CBP officers of their responsibilities to remove and update lookouts in accordance with policy. CBP expects to complete these actions by December 31, 2021.

**Recommendation 3:** Develop and issue a policy regarding asking, advising, or otherwise communicating with foreign governments about denying entry to U.S. citizens. At a minimum, the policy should specify the appropriate circumstances for such communications, who is authorized to approve such communications, and the procedures to follow when making such communications.

**CBP Response to Recommendation 3:** Concur. CBP will revise Directive No. 4320-025A, "Disclosure of Official Information to Foreign Authorities," dated April 2014, by adding a provision on sharing U.S. persons' information with foreign governments. CBP component offices will collaborate to revise and issue the policy. CBP expects to complete these actions by July 29, 2022.

**Recommendation 4:** Conduct a review of all instances in which CBP, as part of its response to the migrant caravan, disclosed U.S. citizens' Sensitive Personally Identifiable Information to Mexican officials, between October 2018 and March 2019, to identify any instances that did not comply with foreign disclosure requirements and take remedial actions. Remedial actions may include rescinding requests to deny entry to U.S. citizens, retroactively instructing foreign authorities to hold CBP information in confidence and use CBP information only for the purpose for which CBP provided it, ensuring disclosures are properly documented in CBP's systems of records, and any other steps necessary to ensure that all foreign disclosures comply with *CBP Directive No. 4320-025A, Disclosure of Official Information to Foreign Authorities*, *DHS Sensitive Systems Policy Directive 4300A, DHS Handbook for Safeguarding Sensitive Personally Identifiable Information*, and all other applicable policies
and procedures.

**CBP Response to Recommendation 4:** Concur. CBP will identify and review disclosures of U.S. citizens' Personally Identifiable Information to Mexican officials that occurred as part of its response to the migrant caravans between October 2018 and March 2019, to ensure compliance with foreign disclosure requirements (specifically established policies and delegations of authority). To the extent remedial actions are required, CBP will remediate each noncompliant disclosure. CBP expects to complete these actions by March 31, 2022.

**Recommendation 5:** Provide training to all CBP personnel on the process for sharing information with foreign nations, covering all applicable policies and procedures, including which CBP personnel are authorized to make foreign disclosures.

**CBP Response to Recommendation 5:** Concur. CBP's Privacy and Diversity Office, in coordination with various CBP components, will identify individuals and work units that regularly disclose PII to foreign partners, and will provide virtual training regarding all applicable policies and procedures by March 31, 2022. The Privacy and Diversity Office, in coordination with the Office of Training and Development, will also develop a new course focused on domestic and foreign information sharing in the DHS Performance and Learning Management System. CBP expects to complete these actions by December 30, 2022.

**Recommendation 6:** Take immediate action to end the use of WhatsApp for operational purposes or to ensure that WhatsApp messages are retained in compliance with legal and policy requirements including records retention schedules.

**CBP Response to Recommendation 6:** Concur. CBP's Office of Information and Technology will explore the viability of the continued operational use of WhatsApp, which will include looking for a replacement. Office of Information and Technology is currently piloting a managed messaging platform to replace WhatsApp. CBP is currently working on an operational pilot. CBP expects to complete these actions by December 31, 2021.

---

# Microsoft Teams meeting

**Join on your computer or mobile app**
Click here to join the meeting

**Or call in (audio only)**
(b)(6), (b)(7)(C) United States, Arlington
Phone Conference ID: (b)(6), (b)(7)(C)
Find a local number | Reset PIN

This Teams Meeting is hosted on a U.S. Government information system and is provided for U.S. Government-authorized use only. Unauthorized or improper use or access of this system may result in disciplinary action as well as civil and criminal penalties.

Learn More | Meeting options

---

Message

**From:** (b)(6), (b)(7)(C)

**Sent:** 11/2/2021 12:52:42 AM

**To:**

**CC:**

(b)(6), (b)(7)(C)

**Subject:** RE: CBP Response due Re: NARA Unauthorized Destruction Letter tied to OIG Audit - short suspense

Good evening (b)(6), (b)(7)(C)

I hope you and the family are healthy and safe!

The Office of Field Operations, Admissibility and Passenger Programs Directorate, Traveler Entry Programs' subject matter expert, Director (b)(6), (b)(7)(C) is available tomorrow at 0915 hours. Will that time be doable?


**(b)(6), (b)(7)(C)**
Director, Quality Assurance Enterprise Division
Planning, Program Analysis & Evaluation
Office of Field Operations
U.S. Customs & Border Protection
1300 Pennsylvania Avenue
Room 5.5A-4
Washington, DC 20229
Cell: (b)(6), (b)(7)(C)
*UnClass:* (b)(6), (b)(7)(C)
*HSDN:* (b)(6), (b)(7)(C)


**QAED Motto – "Trust but Verify"**

U.S. Customs and Border Protection



**From:** (b)(6), (b)(7)(C)
**Sent:** Monday, November 1, 2021 2:35 PM
**To:** OFO AUDITS (b)(6), (b)(7)(C)

(b)(6), (b)(7)(C)

**Cc** (b)(6), (b)(7)(C)

# (b)(6), (b)(7)(C)

**Subject:** CBP Response due Re: NARA Unauthorized Destruction Letter tied to OIG Audit - short suspense

Good afternoon
CBP RIM is seeking assistance from OFO in responding to a NARA Letter regarding the use of WhatsApp and Wickr and possible unauthorized destruction of records.

Laurence Brewer Chief Records Officer for the US Government sent a letter (*see attached*) to (b)(6), (b)(7)(C) Chief Information Officer (CIO), DHS Senior Agency Official for Records Management (SAORM), and (b)(6), (b)(7)(C) CBP Chief Records Officer (CRO), regarding CBP's planned deployment of Wickr and information that NARA received in the Office of Inspector General (OIG) report, "CBP Targeted Americans with the 2018-2019 Migrant Caravan" (link to the report: OIG-21-62 - CBP Targeted Americans Associated with the 2018-2019 Migrant Caravan (dhs.gov)) regarding the use of WhatsApp and possible unauthorized destruction of records.

**Request:**
With input from OFO and other CBP Offices, CBP RIM is compiling the DHS/CBP response to the NARA letter. We were given your names as **POCs for OFO** by the *OIT Audit & Assessment Management Branch (OIT-AAMB)*, (b)(6), (b)(7)(C) *Branch Chief*. Per the information below, CBP RIM is seeking your assistance to (1) provide input to address the NARA Letter to include unauthorized destruction and (2) provide specific information related to the use of and retention practices for records created by WhatsApp and Wickr. We are also seeking to talk with the OFO POCs that participated in the OIG audit interviews and/or are working on remediation responses to the six recommendations that OIG cited in their report.

CBP has been given a short suspense for responding to the NARA Letter. Are you (or the appropriate POCs / SMEs) available to meet for approximately 1 hour during any of the following times:
Tuesday – 11/2/21 9am – 10am ~or~ 12:00 – 2:30pm
Wednesday – 11/3/21 10am – 11:30 ~or~ 2pm – 4pm

**Background**:
The National Archives and Records Administration (NARA) indicated in their letter that they became aware, through multiple media reports and the recent Office of Inspector General (OIG) report, "CBP Targeted Americans with the 2018-2019 Migrant Caravan," that CBP has been using the messaging software WhatsApp and is deploying the encrypted messaging application Wickr across all components of the agency.

*** NARA instructed DHS/CBP to provide a response that addresses the following (as contained in the attached letter):

1. Ensure that Records Management regulations are being adhered to
2. Ensure that the CBP is regulating the use of these messaging applications consistent with NARA's and the Department's records management policies
3. Ensure that CBP is communicating to all employees that they cannot use these applications to circumvent their records management responsibilities and that all employees are aware that they must be retaining all messages that are federal records in accordance with agency policy and all applicable NARA-approved records schedules
4. The final response from CBP must include:
    a. a complete description of the records with volume and dates if known
    b. a description of the office maintaining the records

c. a statement of the exact circumstances surrounding the removal, defacing, alteration, or destruction of records
d. a statement of the safeguards established to prevent further loss of documentation
e. details of the actions taken to salvage, retrieve, or reconstruct the records

5. DHS/CBP's response must also include Records Management corrective actions that CBP will be required to implement as a result of the OIG investigation
6. Additionally, the response must include any documentation in the form of policies, training, approved records schedules or other resources CBP has established to mitigate the records management risk associated with the improper use of Wickr, WhatsApp, or similar messaging applications.

**Key NARA Letter citations from OIG report**:
Further, the OIG report states that there are "instances of CBP officers not documenting information they obtained during caravan-related inspections" (page 12); that CBP officials did not retain communication records (page 17); and that "the CBP officials failure to retain *WhatsApp* messages likely violated DHS and CBP records retention policies because the messages were information that CBP created or received in carrying out its mission and contained substantive information that was necessary to adequately and properly document the activities and functions of the CBP officials" (page 28). This violation of policy resulted in what NARA identified as *unauthorized destruction* of records caused by use of WhatApp and Wickr.

The OIG identified the following 6 **Recommendations** within their audit report:

**Recommendation 1:** Update Customs Directive No. 4320-003, July 1990 (TECS Directive) to clarify the appropriate bases for placing lookouts and provide training to all CBP officials who have the authority to place lookouts.
**CBP Response to Recommendation 1:** Concur. CBP will update lookout placement procedures in the TECS Directive. Additionally, CBP will modify existing training to inform users that lookouts should only be created for law enforcement purposes. CBP expects to complete these actions by December 31, 2021.

**Recommendation 2:** Develop and implement procedures to ensure CBP officials update and remove lookouts in accordance with the TECS Directive.
**CBP Response to Recommendation 2:** Concur. CBP will update lookout placement procedures in the TECS Directive. In addition, CBP will issue a memorandum and muster to remind CBP officers of their responsibilities to remove and update lookouts in accordance with policy. CBP expects to complete these actions by December 31, 2021.

**Recommendation 3:** Develop and issue a policy regarding asking, advising, or otherwise communicating with foreign governments about denying entry to U.S. citizens. At a minimum, the policy should specify the appropriate circumstances for such communications, who is authorized to approve such communications, and the procedures to follow when making such communications.
**CBP Response to Recommendation 3:** Concur. CBP will revise Directive No. 4320-025A, "Disclosure of Official Information to Foreign Authorities," dated April 2014, by adding a provision on sharing U.S. persons' information with foreign governments. CBP component offices will collaborate to revise and issue the policy. CBP expects to complete these actions by July 29, 2022.

**Recommendation 4:** Conduct a review of all instances in which CBP, as part of its response to the migrant caravan, disclosed U.S. citizens' Sensitive Personally Identifiable Information to Mexican officials, between October 2018 and March 2019, to identify any instances that did not comply with foreign disclosure requirements and take remedial actions. Remedial actions may include rescinding requests to deny entry to U.S. citizens, retroactively instructing foreign authorities to hold CBP information in confidence and use CBP information only for the purpose for which CBP provided it, ensuring disclosures are properly documented in CBP's systems of records, and any other steps necessary to ensure that all foreign disclosures comply with *CBP*

*Directive No. 4320-025A, Disclosure of Official Information to Foreign Authorities*, *DHS Sensitive Systems Policy Directive 4300A, DHS Handbook for Safeguarding Sensitive Personally Identifiable Information*, and all other applicable policies
and procedures.

**CBP Response to Recommendation 4:** Concur. CBP will identify and review disclosures of U.S. citizens' Personally Identifiable Information to Mexican officials that occurred as part of its response to the migrant caravans between October 2018 and March 2019, to ensure compliance with foreign disclosure requirements (specifically established policies and delegations of authority). To the extent remedial actions are required, CBP will remediate each noncompliant disclosure. CBP expects to complete these actions by March 31, 2022.

**Recommendation 5:** Provide training to all CBP personnel on the process for sharing information with foreign nations, covering all applicable policies and procedures, including which CBP personnel are authorized to make foreign disclosures.

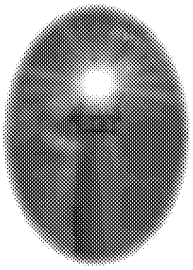
**CBP Response to Recommendation 5:** Concur. CBP's Privacy and Diversity Office, in coordination with various CBP components, will identify individuals and work units that regularly disclose PII to foreign partners, and will provide virtual training regarding all applicable policies and procedures by March 31, 2022. The Privacy and Diversity Office, in coordination with the Office of Training and Development, will also develop a new course focused on domestic and foreign information sharing in the DHS Performance and Learning Management System. CBP expects to complete these actions by December 30, 2022.

**Recommendation 6:** Take immediate action to end the use of WhatsApp for operational purposes or to ensure that WhatsApp messages are retained in compliance with legal and policy requirements including records retention schedules.

**CBP Response to Recommendation 6:** Concur. CBP's Office of Information and Technology will explore the viability of the continued operational use of WhatsApp, which will include looking for a replacement. Office of Information and Technology is currently piloting a managed messaging platform to replace WhatsApp. CBP is currently working on an operational pilot. CBP expects to complete these actions by December 31, 2021.

Please don't hesitate to let me know if you have any questions related to this request.
Thank you,

(b)(6), (b)(7)(C), CBP Chief Records Officer
Records and Information Management Program (RIM)
DHS/CBP/OIT/RIM
(C (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
RIM Website | Request RIM Service! | Email Us




RIM

NATIONAL ARCHIVES

Office *of the* Chief
Records Officer *for the*
U.S. Government

***Sent Via Email. No Hard Copy to Follow.***

October 26, 2021

(b)(6), (b)(7)(C)
Chief Information Officer
Senior Agency Official for Records Management
Customs and Border Protection
(b)(6), (b)(7)(C)
Washington, DC 20024

Dear (b)(6), (b)(7)(C)

The National Archives and Records Administration (NARA) has become aware, through multiple media reports and the recent Office of Inspector General (OIG) report, "CBP Targeted Americans with the 2018-2019 Migrant Caravan," that the Customs and Border Protection (CBP) has been using the messaging software *WhatsApp* and is deploying the encrypted messaging application *Wickr* across all components of the agency. Accordingly, I wanted to reach out to ensure that records management regulations are being adhered to and to ensure that the CBP is regulating the use of these messaging applications consistent with NARA's and the Department's records management policies. I also wanted to ensure that CBP is communicating to all employees that they cannot use these applications to circumvent their records management responsibilities and that all employees are aware that they must be retaining all messages that are federal records in accordance with agency policy and all applicable NARA-approved records schedules.

With respect to *WhatsApp*, the OIG report notes that their ability to determine whether proper processes and procedures were followed was hampered by a failure to retain communication records, including records in *WhatsApp* (page 4). Further, the OIG report states that there are "instances of CBP officers not documenting information they obtained during caravan-related inspections" (page 12); that CBP officials did not retain communication records (page 17); and that "the CBP officials failure to retain *WhatsApp* messages likely violated DHS and CBP records retention policies because the messages were information that CBP created or received in carrying out its mission and contained substantive information that was necessary to adequately and properly document the activities and functions of the CBP officials" (page 28).

Additionally, the OIG report found that during this operation, it is not even clear if CBP policies permit the use of *WhatsApp*.

With respect to *Wickr*, NARA is concerned about the use of this messaging application as it has the capability to auto-delete messages after a specified period of time has passed. In light of the information in the OIG report, NARA is concerned about agency-wide deployment of a messaging application that has this functionality without appropriate policies and procedures governing its use.

DHS employees using these applications without complying with established recordkeeping requirements expose the Department to the risk of potential unauthorized destruction of records. As a reminder, all actual or impending instances of unauthorized disposition must be reported to NARA per the requirements in 36 CFR Part 1230.

In accordance with 36 CFR Part 1230.14, CBP must respond to this letter with a report documenting the unauthorized disposition of the federal records that were identified in the OIG report. At a minimum, this report must include a complete description of the records with volume and dates if known; description of the office maintaining the records; a statement of the exact circumstances surrounding the removal, defacing, alteration, or destruction of records; a statement of the safeguards established to prevent further loss of documentation; and details of the actions taken to salvage, retrieve, or reconstruct the records. This report must also include any records management corrective actions that CBP will be required to implement as a result of the OIG investigation.

Additionally, please include in your report any documentation in the form of policies, training, approved records schedules or other resources CBP has established to mitigate the records management risk associated with the improper use of *Wickr, WhatsApp*, or similar messaging applications.

Please provide your report within 30 days of the date of this letter. I appreciate your attention to this important matter. If you have any questions or wish to discuss further, please contact me at (b)(6), (b)(7)(C)

Sincerely,

(b)(6), (b)(7)(C)

(b)(6), (b)(7)(C)
Chief Records Officer
for the U.S. Government

cc. (b)(6), (b)(7)(C), Department Records Officer, Department of Homeland Security
(b)(6), (b)(7)(C) Agency Records Officer, Customs and Border Protection

Appointment

**From:** (b)(6), (b)(7)(C)

**Sent:** 11/2/2021 11:30:48 AM

**To:** (b)(6), (b)(7)(C)

**Subject:** NARA Unauthorized Destruction Letter: WhatsApp / Wickr

**Attachments:** RE: CBP Response due Re: NARA Unauthorized Destruction Letter tied to OIG Audit - short suspense; 2021-10-26_UD-2022-0001_DHS-CBP_Open Letter-1301-1b.pdf

**Location:** Microsoft Teams Meeting

**Start:** 11/3/2021 2:00:00 PM

**End:** 11/3/2021 3:00:00 PM

**Show Time As:** Tentative

**Required Attendees:** (b)(6), (b)(7)(C)

**Please see attachments**

**Meeting Purpose:**

*** Review NARA Letter and obtain responses and/or identify additional USBP POCs based on instruction from NARA: NARA instructed DHS/CBP to provide a response that addresses the following (as contained in the attached letter):

1. Ensure that Records Management regulations are being adhered to
2. Ensure that the CBP is regulating the use of these messaging applications consistent with NARA's and the Department's records management policies
3. Ensure that CBP is communicating to all employees that they cannot use these applications to circumvent their records management responsibilities and that all employees are aware that they must be retaining all messages that are federal records in accordance with agency policy and all applicable NARA-approved records schedules
4. The final response from CBP must include:
    a. a complete description of the records with volume and dates if known
    b. a description of the office maintaining the records
    c. a statement of the exact circumstances surrounding the removal, defacing, alteration, or destruction of records
    d. a statement of the safeguards established to prevent further loss of documentation
    e. details of the actions taken to salvage, retrieve, or reconstruct the records
5. DHS/CBP's response must also include Records Management corrective actions that CBP will be required to implement as a result of the OIG investigation
6. Additionally, the response must include any documentation in the form of policies, training, approved records schedules or other resources CBP has established to mitigate the records management risk associated with the improper use of Wickr, WhatsApp, or similar messaging applications.

*** Identify which OIG Audit recommendations USBP is responding to and information from CAP that is relevant for inclusion in DHS/CBP response to NARA Letter

**Recommendation 1:** Update Customs Directive No. 4320-003, July 1990 (TECS Directive) to clarify the appropriate bases for placing lookouts and provide training to all CBP officials who have the authority to place lookouts.

**CBP Response to Recommendation 1:** Concur. CBP will update lookout placement procedures in the TECS Directive. Additionally, CBP will modify existing training to inform users that lookouts should only be created for law enforcement purposes. CBP expects to complete these actions by December 31, 2021.

**Recommendation 2:** Develop and implement procedures to ensure CBP officials update and remove lookouts in accordance with the TECS Directive.
**CBP Response to Recommendation 2:** Concur. CBP will update lookout placement procedures in the TECS Directive. In addition, CBP will issue a memorandum and muster to remind CBP officers of their responsibilities to remove and update lookouts in accordance with policy. CBP expects to complete these actions by December 31, 2021.

**Recommendation 3:** Develop and issue a policy regarding asking, advising, or otherwise communicating with foreign governments about denying entry to U.S. citizens. At a minimum, the policy should specify the appropriate circumstances for such communications, who is authorized to approve such communications, and the procedures to follow when making such communications.
**CBP Response to Recommendation 3:** Concur. CBP will revise Directive No. 4320-025A, "Disclosure of Official Information to Foreign Authorities," dated April 2014, by adding a provision on sharing U.S. persons' information with foreign governments. CBP component offices will collaborate to revise and issue the policy. CBP expects to complete these actions by July 29, 2022.

**Recommendation 4:** Conduct a review of all instances in which CBP, as part of its response to the migrant caravan, disclosed U.S. citizens' Sensitive Personally Identifiable Information to Mexican officials, between October 2018 and March 2019, to identify any instances that did not comply with foreign disclosure requirements and take remedial actions. Remedial actions may include rescinding requests to deny entry to U.S. citizens, retroactively instructing foreign authorities to hold CBP information in confidence and use CBP information only for the purpose for which CBP provided it, ensuring disclosures are properly documented in CBP's systems of records, and any other steps necessary to ensure that all foreign disclosures comply with *CBP Directive No. 4320-025A, Disclosure of Official Information to Foreign Authorities*, *DHS Sensitive Systems Policy Directive 4300A, DHS Handbook for Safeguarding Sensitive Personally Identifiable Information*, and all other applicable policies
and procedures.
**CBP Response to Recommendation 4:** Concur. CBP will identify and review disclosures of U.S. citizens' Personally Identifiable Information to Mexican officials that occurred as part of its response to the migrant caravans between October 2018 and March 2019, to ensure compliance with foreign disclosure requirements (specifically established policies and delegations of authority). To the extent remedial actions are required, CBP will remediate each noncompliant disclosure. CBP expects to complete these actions by March 31, 2022.

**Recommendation 5:** Provide training to all CBP personnel on the process for sharing information with foreign nations, covering all applicable policies and procedures, including which CBP personnel are authorized to make foreign disclosures.
**CBP Response to Recommendation 5:** Concur. CBP's Privacy and Diversity Office, in coordination with various CBP components, will identify individuals and work units that regularly disclose PII to foreign partners, and will provide virtual training regarding all applicable policies and procedures by March 31, 2022. The Privacy and Diversity Office, in coordination with the Office of Training and Development, will also develop a new course focused on domestic and foreign information sharing in the DHS Performance and Learning Management System. CBP expects to complete these actions by December 30, 2022.

**Recommendation 6:** Take immediate action to end the use of WhatsApp for operational purposes or to ensure that WhatsApp messages are retained in compliance with legal and policy requirements including records retention schedules.
**CBP Response to Recommendation 6:** Concur. CBP's Office of Information and Technology will explore the viability of the continued operational use of WhatsApp, which will include looking for a replacement. Office of

Information and Technology is currently piloting a managed messaging platform to replace WhatsApp. CBP is currently working on an operational pilot. CBP expects to complete these actions by December 31, 2021.

---

# Microsoft Teams meeting

**Join on your computer or mobile app**
Click here to join the meeting

**Or call in (audio only)**
(b)(6), (b)(7)(C) United States, Arlington
Phone Conference ID: (b)(6), (b)(7)(C)
Find a local number | Reset PIN

This Teams Meeting is hosted on a U.S. Government information system and is provided for U.S. Government-authorized use only. Unauthorized or improper use or access of this system may result in disciplinary action as well as civil and criminal penalties.

Learn More | Meeting options

---

Message

**From:** USBP-AUDIT-TEAM (b)(6), (b)(7)(C) (b)(6), (b)(7)(C)

**Sent:** 11/1/2021 8:16:01 PM

**To:** (b)(6), (b)(7)(C)

**CC:** USBP-AUDIT-TEAM (b)(6), (b)(7)(C) (b)(6), (b)(7)(C)

**Subject:** RE: CBP Response due Re: NARA Unauthorized Destruction Letter tied to OIG Audit - short suspense

**Flag:** Follow up

Good afternoon (b)(6), (b)(7)(C)

The USBP SME would be (b)(6), (b)(7)(C), and he is available Wednesday starting at 10am. Of course, USBP Audit Liaison Team would attend the meeting as well, whenever you are able to schedule it.

If you have any further questions, please let me know.

Thank you!

(b)(6), (b)(7)(C)
Assistant Chief
Policy and Compliance Division
Strategic Planning and Analysis Directorate (SPAD)
U.S. Border Patrol Headquarters
(b)(6), (b)(7)(C)
Audit Group Mailbox (b)(6), (b)(7)(C)

**From:** (b)(6), (b)(7)(C)
**Sent:** Monday, November 1, 2021 2:29 PM
**To:** USBP-AUDIT-TEAM (b)(6), (b)(7)(C)

(b)(6), (b)(7)(C)

**Cc:** (b)(6), (b)(7)(C)

(b)(6), (b)(7)(C)

(b)(6), (b)(7)(C) CBPRECORDSMANAGEMENT

(b)(6), (b)(7)(C)

**Subject:** CBP Response due Re: NARA Unauthorized Destruction Letter tied to OIG Audit - short suspense

Good afternoon,
CBP RIM is seeking assistance from USBP in responding to a NARA Letter regarding the use of WhatsApp and Wickr and possible unauthorized destruction of records.

Laurence Brewer Chief Records Officer for the US Government sent a letter (*see attached*) to (b)(6), (b)(7)(C) Chief Information Officer (CIO), DHS Senior Agency Official for Records Management (SAORM), and (b)(6), (b)(7)(C) CBP Chief Records Officer (CRO), regarding CBP's planned deployment of Wickr and information that NARA received in the Office of Inspector General (OIG) report, "CBP Targeted Americans with the 2018-2019 Migrant Caravan" (link to the report: OIG-21-62 - CBP Targeted Americans Associated with the 2018-2019 Migrant Caravan (dhs.gov)) regarding the use of WhatsApp and possible unauthorized destruction of records.

**Request:**
With input from USBP and other CBP Offices, CBP RIM is compiling the DHS/CBP response to the NARA letter. We were given your names as **POCs for USBP** by the *OIT Audit & Assessment Management Branch (OIT-AAMB),* (b)(6), (b)(7)(C) *Branch Chief*. Per the information below, CBP RIM is seeking your assistance to (1) provide input to address the NARA Letter to include unauthorized destruction and (2) provide specific information related to the use of and retention practices for records created by WhatsApp and Wickr. We are also seeking to talk with the USBP POCs that participated in the OIG audit interviews and/or are working on remediation responses to the six recommendations that OIG cited in their report.

CBP has been given a short suspense for responding to the NARA Letter. Are you (or the appropriate POCs / SMEs) available to meet for approximately 1 hour during any of the following times:
Tuesday – 11/2/21 9am – 10am ~or~ 12:00 – 2:30pm
Wednesday – 11/3/21 10am – 11:30 ~or~ 2pm – 4pm

**Background**:
The National Archives and Records Administration (NARA) indicated in their letter that they became aware, through multiple media reports and the recent Office of Inspector General (OIG) report, "CBP Targeted Americans with the 2018-2019 Migrant Caravan," that CBP has been using the messaging software WhatsApp and is deploying the encrypted messaging application Wickr across all components of the agency.

*** NARA instructed DHS/CBP to provide a response that addresses the following (as contained in the attached letter):

1. Ensure that Records Management regulations are being adhered to
2. Ensure that the CBP is regulating the use of these messaging applications consistent with NARA's and the Department's records management policies
3. Ensure that CBP is communicating to all employees that they cannot use these applications to circumvent their records management responsibilities and that all employees are aware that they must be retaining all messages that are federal records in accordance with agency policy and all applicable NARA-approved records schedules
4. The final response from CBP must include:
    a. a complete description of the records with volume and dates if known
    b. a description of the office maintaining the records
    c. a statement of the exact circumstances surrounding the removal, defacing, alteration, or destruction of records
    d. a statement of the safeguards established to prevent further loss of documentation
    e. details of the actions taken to salvage, retrieve, or reconstruct the records
5. DHS/CBP's response must also include Records Management corrective actions that CBP will be required to implement as a result of the OIG investigation
6. Additionally, the response must include any documentation in the form of policies, training, approved records schedules or other resources CBP has established to mitigate the records management risk associated with the improper use of Wickr, WhatsApp, or similar messaging applications.

**Key NARA Letter citations from OIG report**:
Further, the OIG report states that there are "instances of CBP officers not documenting information they obtained during caravan-related inspections" (page 12); that CBP officials did not retain communication records (page 17); and that "the CBP officials failure to retain *WhatsApp* messages likely violated DHS and CBP records retention policies because the messages were information that CBP created or received in carrying out its mission and contained substantive information that was necessary to adequately and properly document

the activities and functions of the CBP officials" (page 28). This violation of policy resulted in what NARA identified as *unauthorized destruction* of records caused by use of WhatApp and Wickr.

The OIG identified the following 6 **Recommendations** within their audit report:

**Recommendation 1:** Update Customs Directive No. 4320-003, July 1990 (TECS Directive) to clarify the appropriate bases for placing lookouts and provide training to all CBP officials who have the authority to place lookouts.
**CBP Response to Recommendation 1:** Concur. CBP will update lookout placement procedures in the TECS Directive. Additionally, CBP will modify existing training to inform users that lookouts should only be created for law enforcement purposes. CBP expects to complete these actions by December 31, 2021.

**Recommendation 2:** Develop and implement procedures to ensure CBP officials update and remove lookouts in accordance with the TECS Directive.
**CBP Response to Recommendation 2:** Concur. CBP will update lookout placement procedures in the TECS Directive. In addition, CBP will issue a memorandum and muster to remind CBP officers of their responsibilities to remove and update lookouts in accordance with policy. CBP expects to complete these actions by December 31, 2021.

**Recommendation 3:** Develop and issue a policy regarding asking, advising, or otherwise communicating with foreign governments about denying entry to U.S. citizens. At a minimum, the policy should specify the appropriate circumstances for such communications, who is authorized to approve such communications, and the procedures to follow when making such communications.
**CBP Response to Recommendation 3:** Concur. CBP will revise Directive No. 4320-025A, "Disclosure of Official Information to Foreign Authorities," dated April 2014, by adding a provision on sharing U.S. persons' information with foreign governments. CBP component offices will collaborate to revise and issue the policy. CBP expects to complete these actions by July 29, 2022.

**Recommendation 4:** Conduct a review of all instances in which CBP, as part of its response to the migrant caravan, disclosed U.S. citizens' Sensitive Personally Identifiable Information to Mexican officials, between October 2018 and March 2019, to identify any instances that did not comply with foreign disclosure requirements and take remedial actions. Remedial actions may include rescinding requests to deny entry to U.S. citizens, retroactively instructing foreign authorities to hold CBP information in confidence and use CBP information only for the purpose for which CBP provided it, ensuring disclosures are properly documented in CBP's systems of records, and any other steps necessary to ensure that all foreign disclosures comply with *CBP Directive No. 4320-025A, Disclosure of Official Information to Foreign Authorities*, *DHS Sensitive Systems Policy Directive 4300A, DHS Handbook for Safeguarding Sensitive Personally Identifiable Information*, and all other applicable policies
and procedures.
**CBP Response to Recommendation 4:** Concur. CBP will identify and review disclosures of U.S. citizens' Personally Identifiable Information to Mexican officials that occurred as part of its response to the migrant caravans between October 2018 and March 2019, to ensure compliance with foreign disclosure requirements (specifically established policies and delegations of authority). To the extent remedial actions are required, CBP will remediate each noncompliant disclosure. CBP expects to complete these actions by March 31, 2022.

**Recommendation 5:** Provide training to all CBP personnel on the process for sharing information with foreign nations, covering all applicable policies and procedures, including which CBP personnel are authorized to make foreign disclosures.
**CBP Response to Recommendation 5:** Concur. CBP's Privacy and Diversity Office, in coordination with various CBP components, will identify individuals and work units that regularly disclose PII to foreign partners, and will provide virtual training regarding all applicable policies and procedures by March 31, 2022. The Privacy and Diversity Office, in coordination with the Office of Training and Development, will also develop a

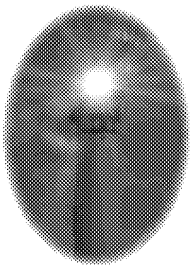
new course focused on domestic and foreign information sharing in the DHS Performance and Learning Management System. CBP expects to complete these actions by December 30, 2022.

**Recommendation 6:** Take immediate action to end the use of WhatsApp for operational purposes or to ensure that WhatsApp messages are retained in compliance with legal and policy requirements including records retention schedules.

**CBP Response to Recommendation 6:** Concur. CBP's Office of Information and Technology will explore the viability of the continued operational use of WhatsApp, which will include looking for a replacement. Office of Information and Technology is currently piloting a managed messaging platform to replace WhatsApp. CBP is currently working on an operational pilot. CBP expects to complete these actions by December 31, 2021.

Please don't hesitate to let me know if you have any questions related to this request.
Thank you,

(b)(6), (b)(7)(C), CBP Chief Records Officer
Records and Information Management Program (RIM)
DHS/CBP/OIT/RIM
(C) (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
RIM Website | Request RIM Service! | Email Us



Shine a Light

Suicide Prevention and Awareness

**National Suicide Prevention Lifeline**
800-273-8255
**CBP Employee Assistance Program**
800-755-7002

Message

**From:** CBPRECORDSMANAGEMENT (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
**Sent:** 3/24/2022 6:38:25 PM
**To:** (b)(6), (b)(7)(C)
**CC:** RIM RAT (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
**Subject:** LRIM APPROVAL NEEDED: Emessaging Record Retention Schedule 234
**Attachments:** DAA-0568-2022-0005 v3.pdf; cbp_0234 eMessaging2 DDsigned Bisness owner signed 032322.pdf

3/24/2022

CBP RIM has developed the Electronic Messaging Schedule. Please see the below analysis with attachments. If you approve, please sign the 234 Form. We will follow-up with you by 3/31/22 if a response is not received.

Result Options:
Schedule Developed (Non-IT System)

- 234 Signatures: CRO, Privacy, OCC, Business Owner, LRIM

Title: Electronic Messaging Records

Approvals Required for Retention:

- Chief Records Officer: (b)(6), (b)(7)(C) signed
- Privacy: (b)(6), (b)(7)(C) signed
- Chief Counsel: (b)(6), (b)(7)(C) signed
- Business Owner: (b)(6), (b)(7)(C) signed
- LRIM: (b)(6), (b)(7)(C)

CBP RIM Team Analysis:
CBP RIM developed an electronic messaging records schedule as a part of the ERM Program Plan and in response to the NARA Unauthorized Disposal Letter regarding Wickr and WhatsApp. The scope includes any electronic messaging not covered by other schedules or integrated into IT system functions. The retention was based on Capstone email roles and retentions.

Analysis Outcome:
CBP RIM drafted a schedule DAA-0568-2022-0005. The schedule contains a permanent schedule item for messages of Capstone Officials (60 top roles within the agency) and a temporary item for all other messages (10 year retention).

(b)(6), (b)(7)(C)
Senior Records Information Management Advisor
Capitol Advisors on Technology, LLC
Records and Information Management
OIT | CBP | DHS
Cell (b)(6), (b)(7)(C)

DEPARTMENT OF HOMELAND SECURITY
U.S. Customs and Border Protection

# RECORDS AND SYSTEMS RETENTION SCHEDULE APPROVAL

CBP Record Series or Electronic Information System Name:
Electronic Messaging Records

## SECTION TO BE FILLED OUT BY CBP RIM PROGRAM

Name of CBP RIM Scheduler (Last, First, Middle Initial):
(b)(6), (b)(7)(C) (b)(6), (b)(7)(C)

**Select One:**

A) ☐ The CBP RIM Program reviewed this system with System Subject Matter Experts and has determined that the system is covered by existing NARA-approved schedules (list provided separately).

B) ☐ The CBP RIM Program reviewed this system with System Subject Matter Experts and has developed a retention schedule for all unscheduled records held within the system (draft schedule provided separately).

C) ☐ The CBP RIM Program reviewed the provided records series with Subject Matter Experts and has determined that the records are covered by existing NARA-approved schedules (list provided separately)

D) ☒ The CBP RIM Program developed these record series with Subject Matter Experts and has drafted a retention schedule for NARA submission (draft schedule provided separately)

DAA-0568-2022-0005 v3

(b)(6), (b)(7)(C)
Chief Records Officer Signature:

## SECTION TO BE FILLED OUT BY STAKEHOLDERS

I have reviewed the provided draft retention schedule and approve of the description(s) and retention period(s). I support submitting this retention schedule to the National Archives and Records Administration for approval. By providing my signature, I understand that these records cannot be dispositioned until NARA has approved this schedule.

| | |
|---|---|
| (b)(6), (b)(7)(C)<br>Business Owner Signature | LRIM Signature |
| (b)(6), (b)(7)(C)<br>Chief Counsel Representative Signature | LRIM Signature<br>*(Optional- if more than one office is involved)* |
| (b)(6), (b)(7)(C)<br>Privacy Representative Signature | LRIM Signature<br>*(Optional- if more than one office is involved)* |

Message

**From:** (b)(6), (b)(7)(C)

**Sent:** 4/15/2021 2:22:27 PM

**To:** (b)(6), (b)(7)(C)

**Subject:** original WICKR SOW

**Attachments:** Draft Wickr SOW_06232020.final Updated 06282020.docx

(b)(6), (b)(7)(C)

Could you please send us the original WICKR SOW, the one which goes until 9/2021?

The only one I have is "Draft Wickr SOW_06232020.final Updated 06282020.docx"

Or is this the current one?

Attached

(b)(6), (b)(7)(C)
Director, Mobility and Collaboration Branch (MCB)
DHS | CBP | ES | OIT | ENTSD
Work: (b)(6), (b)(7)(C)
Mobile: (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)

Message

**From:** (b)(6), (b)(7)(C)

**Sent:** 4/8/2021 9:50:26 PM

**To:**

**CC:** (b)(6), (b)(7)(C)

**Subject:** Part 1 Email Correspondence with WICKR 1/1/2019-4/8/2021

**Attachments:** Re: CBP - Infos Re (b)(6), (b)(7)(C) email; Re: CBP - Infos Re: (b)(6), (b)(7)(C) email; Re: CBP - Infos Re (b)(6), (b)(7)(C) email; Re: CBP - Infos Re: (b)(6), (b)(7)(C) email; Re: CBP - Infos Re: (b)(6), (b)(7)(C) email; CBP - Infos Re: (b)(6), (b)(7)(C) email; Re: WICKR Weekly Sync Up; Re: WICKR Weekly Sync Up; Re: WICKR Discussion on HA; Re: WIKR HA and DR; Re: WIKR HA and DR; Re: WIKR HA and DR; Call today - Nov 18th?; Fwd: Deliverable today - Wickr version numbers and refresh times; Re: Wickr Post Meeting Discussion; Re: Wickr Post Meeting Discussion; Re: Wickr T3 follow-up call next week; Re: FW: Wickr T3 follow-up call next week; Re: WICKR Weekly Sync Up; Declined: WICKR Weekly Sync Up (CBP @ Wed Apr 7, 2021 10am - 11am (PDT) (b)(6), (b)(7)(C) (CBP) (Webex link in notes); Wickr & (b)(6), (b)(7)(C) (CBP) (Webex link in notes); Invitation: Wickr & (b)(6), (b)(7)(C) (CBP) @ Fri Mar 19, 2021 8am - 9am (PDT) (b)(6), (b)(7)(C); Declined: WICKR Weekly Sync Up @ Wed Mar 3, 2021 10am - 11am (PST) (b)(6), (b)(7)(C) CTR)); Declined: WICKR Weekly Sync Up @ Wed Feb 24, 2021 10am - 11am (PST) (b)(6), (b)(7)(C) (CTR)); Declined: WICKR Weekly Sync Up @ Wed Apr 14, 2021 10am - 11am (PDT) (b)(6), (b)(7)(C) (CTR)); Declined: WICKR Weekly Sync Up @ Wed Dec 30, 2020 10am - 11am (PST) (b)(6), (b)(7)(C) (CTR)); Declined: WICKR Weekly Sync Up @ Wed Dec 23, 2020 10am - 11am (PST) (b)(6), (b)(7)(C) (CTR)); Declined: WICKR Weekly Sync Up @ Wed Dec 16, 2020 10am - 11am (PST) (b)(6), (b)(7)(C) (CTR)); Declined: WICKR Weekly Sync Up @ Wed Dec 2, 2020 10am - 11am (PST) (b)(6), (b)(7)(C) (CTR)); Tentatively Accepted: WICKR Weekly Sync Up @ Wed Dec 2, 2020 10am - 11am (PST) (b)(6), (b)(7)(C) (CTR)); Accepted: WICKR Discussion on HA @ Tue Dec 1, 2020 11am - 11:30am (PST) (b)(6), (b)(7)(C) (CTR)); Accepted: WICKR Weekly Sync Up @ Weekly from 10am to 11am on Wednesday (PST) (b)(6), (b)(7)(C) (CTR)); Accepted: WICKR Weekly Sync Up @ Wed Nov 25, 2020 10am - 11am (PST) (b)(6), (b)(7)(C) (CTR)); Accepted: WICKR Weekly Sync Up @ Weekly from 10am to 11am on Wednesday (PST) (b)(6), (b)(7)(C) (CTR)); Declined: WICKR Weekly Sync Up @ Wed Nov 11, 2020 10am - 11am (PST) (b)(6), (b)(7)(C) (CTR)); Declined: WICKR Weekly Sync Up @ Wed Nov 4, 2020 10am - 11am (PST) (b)(6), (b)(7)(C) (CTR)); Declined: WICKR Weekly Sync Up @ Wed Oct 21, 2020 10am - 11am (PDT) (b)(6), (b)(7)(C) (CTR)); Declined: WICKR Weekly Sync Up @ Wed Oct 7, 2020 10am - 11am (PDT) (b)(6), (b)(7)(C) (CTR)); Declined: WICKR Weekly Sync Up @ Wed Sep 16, 2020 10am - 11am (PDT) (b)(6), (b)(7)(C) (CTR)); Declined: WICKR Weekly Sync Up @ Wed Sep 9, 2020 10am - 11am (PDT) (b)(6), (b)(7)(C), (b)(6), (b)(7)(C) (CTR)); Declined: WICKR Weekly Sync Up @ Wed Sep 30, 2020 10am - 11am (PDT) (b)(6), (b)(7)(C) (CTR)); Accepted: WICKR Re-Authentication @ Wed May 27, 2020 8am - 9am (PDT) (b)(6), (b)(7)(C) Accepted: WICKR Weekly Sync Up @ Weekly from 10am to 11am on Wednesday (PDT) (b)(6), (b)(7)(C) Accepted: WICKR Weekly Sync Up @ Wed May 20, 2020 10am - 11am (PDT) (b)(6), (b)(7)(C); Accepted: WICKR Weekly Sync Up @ Wed May 13, 2020 10am - 11am (PDT) (b)(6), (b)(7)(C); Accepted: WICKR Weekly Sync Up @ Wed May 6, 2020 10am - 11am (PDT) (b)(6), (b)(7)(C) (CTR)); Accepted: WICKR Weekly Sync Up @ Weekly from 11am to 12pm on Wednesday (MST) (b)(6), (b)(7)(C) (CTR)); Accepted: WICKR Troubleshooting Ports with DHS and Vendor @ Mon May 11, 2020 11am - 12:30pm (MDT) (b)(6), (b)(7)(C) (CTR)); Accepted: WICKR Weekly Sync Up @ Weekly from 11am to 12pm on Wednesday (MDT) (b)(6), (b)(7)(C) (CTR)); Declined: WICKR Weekly Sync Up @ Weekly from 1pm to 2pm on Wednesday (EDT) (b)(6), (b)(7)(C) (CTR)); Tentatively Accepted: WICKR Weekly Sync Up @ Weekly from 1pm to 2pm on Wednesday (EST) (b)(6), (b)(7)(C) (CTR)); Tentatively Accepted: WICKR Weekly Sync Up @ Weekly from 1pm to 2pm on Wednesday (EDT) (b)(6), (b)(7)(C) (CTR)); Tentatively Accepted: WICKR Weekly Sync Up @ Weekly from 1pm to 2pm on Wednesday (EST) (b)(6), (b)(7)(C) (CTR)); Accepted: WICKR Weekly Sync Up @ Weekly from 1pm to 2pm on Wednesday (EST) (b)(6), (b)(7)(C) (CTR)); Declined: WICKR Weekly Sync Up @ Wed Oct 28, 2020 1pm - 2pm (EDT) (b)(6), (b)(7)(C) (CTR)); FW: Updated invitation: DHS CBP New UI Feedback @ Tue May 5, 2020 4:30pm - 5pm (EDT) (rojelio.r.ruiz@cbp.dhs.gov); Accepted: WICKR Weekly Sync Up @ Weekly from 1pm to 2pm on Wednesday (EST) (b)(6), (b)(7)(C) (CTR)); Declined: WICKR Weekly Sync Up @ Wed Feb 3, 2021 1pm - 2pm (EST) (b)(6), (b)(7)(C) (CTR)); Accepted: WICKR Weekly Sync Up @ Weekly from 1pm to 2pm on Wednesday (EDT) (b)(6), (b)(7)(C) (CTR)); Accepted: Follow up on v729 @ Tue Sep 22, 2020 12pm - 1pm (EDT) (b)(6), (b)(7)(C) (CTR)); CBP -WICKR Call 13 AUG; Re: Request for Input-RBAC and Wickr Guard; Testing of New Infra; Re: Canceled: WICKR Weekly Sync Up; ATAK meeting; Wickr &

(b)(6), (b)(7)(C) (CBP) (Webex link in notes); Accepted: Wickr & (b)(6), (b)(7)(C) (CBP) (Webex link in notes); (b)(6), (b)(7)(C) email; Re: Client side certificate auth; WICKR App; Canceled: WICKR Weekly Sync Up; Canceled: WICKR Weekly Sync Up; Canceled: WICKR Weekly Sync Up; RE: WICKR Discussion on HA; WICKR Discussion on HA; WICKR Discussion on HA; WICKR Discussion on HA; WICKR Weekly Sync Up; RE: Global Federation Documentation; WICKR Weekly Sync Up; Canceled: WICKR Weekly Sync Up; Follow up on v729; Global Federation Documentation; Re: Urgent: DTLS Connection Failures; WICKR ; WICKR Follow Up WebEx; WICKR CBP; Request for Input-RBAC and Wickr Guard; Canceled: WICKR Weekly Sync Up; FW: SFO WICKR Follow up/App Demo; RE: FW: Wickr T3 follow-up call next week; FW: Wickr T3 follow-up call next week; Update Re-Authentication

Hi (b)(6), (b)(7)(C)

I went thought my sent, receive, and archive folders to pull all correspondence between me and WICKR.

Thanks,

(b)(6), (b)(7)(C) PMP, ITIL V3
Project Manager
SECTEK
Secure. Connect. Evolve.
Customs and Border Protection / Department of Homeland Security
Enterprise Networks & Technology Support Directorate (ENTSD)
Network Architecture & Engineering Division (NAED)
ENTSD/OIT/CBP/DHS
Desk:TBD
Mobile: (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)

Message

**From:** (b)(6), (b)(7)(C)
**Sent:** 3/10/2021 9:48:34 PM
**To:**
**CC:** (b)(6), (b)(7)(C)
**Subject:** Re: CBP - Infos Re: (b)(6), (b)(7)(C) email

(b)(6), (b)(7)(C),

If you or (b)(6), (b)(7)(C) have a webex link to use I can add to the invite.

(b)(6), (b)(7)(C)
VP Corp Dev & Customer Success
(b)(6), (b)(7)(C)
Download Wickr Pro

On Mar 10, 2021, at 12:40 PM, (b)(6), (b)(7)(C) wrote:

Great. I'll send an invite

(b)(6), (b)(7)(C)
VP Corp Dev & Customer Success
(b)(6), (b)(7)(C)
Download Wickr Pro

On Mar 10, 2021, at 12:25 PM, (b)(6), (b)(7)(C) (b)(6), (b)(7)(C) wrote:

Ok

Get Outlook for iOS

**From:** (b)(6), (b)(7)(C)
**Sent:** Wednesday, March 10, 2021 3:04:39 PM
**To:**
**Cc:** (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
**Subject:** Re: CBP - Infos Re: (b)(6), (b)(7)(C) email

Looks like next Friday is our best bet - same time if that works(?)

(b)(6), (b)(7)(C)
VP Corp Dev & Customer Success
(b)(6), (b)(7)(C)

(b)(6), (b)(7)(C)
Download Wickr Pro

On Mar 10, 2021, at 10:46 AM, (b)(6), (b)(7)(C) (b)(6), (b)(7)(C) > wrote:

Sounds good.
How would next Tuesday around 11am work?
You can teach me all the secrets too ....

Thanks,

(b)(6), (b)(7)(C)

**From:** (b)(6), (b)(7)(C)
**Sent:** Wednesday, March 10, 2021 1:32 PM
**To:** (b)(6), (b)(7)(C) (b)(6), (b)(7)(C)
**Cc:** (b)(6), (b)(7)(C) (b)(6), (b)(7)(C)
**Subject:** Re: CBP - Infos Re: (b)(6), (b)(7)(C) email

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact the CBP Security Operations Center with questions or concerns.

Hey (b)(6), (b)(7)(C)

Our emails passed by each other in the ether :)

We outsourced the FIPS testing to Leidos - you'll see in the NIST record the details. We don't swap the FIPS out on the fly - it's hard-coded into the Ent clients, etc

Re: "Global Federation" between Wickr Ent (solution you have deployed) and Wickr Me & Wickr Pro — everything still remains end-to-end encrypted. All products use the same E2EE protocols. And, yes, we can definitely set-up a tech discussion on how this all works. Shoot over some dates/time next week and I'll schedule a call.

Cheers!

(b)(6), (b)(7)(C)
VP Corp Dev & Customer Success
**(b)(6), (b)(7)(C)**
Download Wickr Pro

On Mar 10, 2021, at 10:23 AM, (b)(6), (b)(7)(C) (b)(6), (b)(7)(C) > wrote:

Thanks (b)(6), (b)(7)(C)

(b)(6), (b)(7)(C)

Attaching some links and documents for you:

1. Anything you want to know about our encryption is located here including ability to review our code on Git + our Messing white paper.

2. Wickr's FIPS certification for Wickr Enterprise

3. 3rd Party Audits are located on the same page and titled Customer Promises...you can get all current and historical reports. Q1'21 Report is being finalized and will appear soon

Compliance Installation and overview document attached:

<Compliance_Service_Deploy_3.9 (1).pdf>

Happy to set-up a separate call via (b)(6), (b)(7)(C) to discuss any/all questions you have.

Regards,

(b)(6), (b)(7)(C)
VP Corp Dev & Customer Success
**(b)(6), (b)(7)(C)**
Download Wickr Pro

On Mar 10, 2021, at 10:16 AM, (b)(6), (b)(7)(C) **(b)(6), (b)(7)(C)** wrote:

In the CC line.

Thanks,

(b)(6), (b)(7)(C) PMP, ITIL V3
Project Manager
<image001.jpg><image002.png>
Customs and Border Protection /
Department of Homeland Security
Enterprise Networks & Technology
Support Directorate (ENTSD)
Network Architecture & Engineering
Division (NAED)
ENTSD/OIT/CBP/DHS

Desk:TBD
Mobile: (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)

Appointment

**From:** Google Calendar on behalf of (b)(6), (b)(7)(C)
**Sent:** 5/11/2020 4:24:04 PM
**To:** (b)(6), (b)(7)(C)
**Subject:** Accepted: WICKR Troubleshooting Ports with DHS and Vendor @ Mon May 11, 2020 11am - 12:30pm (MDT) (b)(6), (b)(7)(C)
**Attachments:** invite.ics
**Location:** WebEx

**Start:** 5/11/2020 5:00:00 PM
**End:** 5/11/2020 6:30:00 PM
**Show Time As:** Tentative

**Recurrence:** (none)



**csiens@wickr.com has accepted this invitation.**

## WICKR Troubleshooting Ports with DHS and Vendor

When Mon May 11, 2020 11am – 12:30pm Mountain Time - Denver

Where WebEx (map)

Calendar (b)(6), (b)(7)(C)

Who
- (b)(6), (b)(7)(C)

-- Do not delete or change any of the following text. --

When it's time, join your Webex meeting here.

Meeting number (access code): (b)(6), (b)(7)(C)
Meeting password: (b)(6), (b)(7)(C)

Join meeting

Join by phone
Tap to call in from a mobile device (attendees only)
(b)(6), (b)(7)(C)
Global call-in numbers

Join from a video system or application
Dial (b)(6), (b)(7)(C)

Join using Microsoft Lync or Microsoft Skype for Business
Dial (b)(6), (b)(7)(C)

If you are a host, go here to view host information.

Need help? Go to http://help.webex.com

Message

**From:** (b)(6), (b)(7)(C)

**Sent:** 4/16/2021 7:33:31 PM

**To:** (b)(6), (b)(7)(C)

**CC:** (b)(6), (b)(7)(C)

**Subject:** 2012-1093: Wickr Software Licenses - Director & XD Approval

**Attachments:** 20121093 - IGCE V2 - Wickr Software Licenses 04132021.xls; 20121093 - SOW V5 - Wickr Software Licenses 041321.docx; 20121093 ES - Wickr Software Licenses 041321.docx; 20121093 MR V2 - Wickr Software Licenses 040521.docx; 2012-1093 - IGCE Summary - Wickr Software Licenses 041421.doc; 2012-1093 - ITAR Checklist V2 - Wickr Software Licenses 041521.xlsx; 2012-1093 - PSC Exemption - WICKR 041321.docx; 20121093 - BOM - Wickr Software Licenses.xlsx

**Flag:** Read

(b)(6), (b)(7)(C)

Can you please provide a JEFO and Checklist for this procurement?

(b)(6), (b)(7)(C)

FMB is pending the information from MCB to create/submit the SDR to obtain the funding for this procurement.

Please let me know if you have any questions.

Thanks

(b)(6), (b)(7)(C)
Office of Information and Technology/ENTSD
Enterprise Services
US Customs and Border Protection (CBP)
Department of Homeland Security
(b)(6), (b)(7)(C) – Office
- Mobile
(b)(6), (b)(7)(C)

# Document Produced in Native Format

# U.S. Customs and Border Protection
# Office of Information and Technology
# Executive Summary

## Division Information:

**Division: Mobility and Collaboration Branch (MCB)**

**Division Director:** (b)(6), (b)(7)(C)

**Title of Procurement: Wickr Software Licenses**

**Purchase Requisition: 2012-1093**

## Executive Summary:

Description:

Wickr is an instant messaging application which provides users with a secure messaging platform that enables voice and video chat, as well as file, video and photo transfers. For example, CBP requires a secure messaging application to meet multiple use-cases across all components. In particular CBP users require the ability to securely share operationally relevant information between field users, between primary and secondary inspection areas in Ports of Entry, the ability to communicate with agency counterparts while on foreign assignment, and the ability to distribute strategic communications from senior leadership to the officer and agent level. CBP-approved users of Wickr will be able to access the application from mobile devices, laptops and workstations. This will allow for greater coordination at the operational and strategic planning level, as well as tactical coordination when needed.

The scope of this delivery order shall include several areas of capabilities:

1. The renewal of the existing Wickr user licenses and the ability to increase the number of CBP licenses available for users. The renewal period shall start at the end of the existing license period.
2. Professional Service Support hours to be provided by Wickr.
3. Options for future development to support operational use cases such as:
    a. The development of Wickr plugin to integrate with Team Awareness Kit (TAK) for both iPhone and Android.
    b. Integrated Auth support for Macintosh OS X & Windows integrated AUTH clients using Azure as the Identity Provider (IDP).
4. Provide a solution to support High Availability (HA) and minimize the infrastructure downtime. The current environment is utilizing Docker Containers which does not allow for HA. The Docker Containers need to be migrated to Kubernetes Containers which would provide HA.
5. Create role base access controls (RBAC) with in the Wickr backend portal, Admin console, and replicated dashboard.
6. Currently both internal and external users are required to use a configuration file to onboard when launching Wickr. Develop a seamless workflow that does not

require a configuration file to onboard both internal and external federation of agencies.

Out-Year Strategy
The current procurement is for the licenses, support and professional services of ongoing support of the current Wickr secure messaging platform. Licenses will likely need to be renewed in the outyears as the need for mobile capabilities increases.

10% Reduction Effort:
This procurement is to renew existing Wickr software licenses. There are no areas available for reduction in this effort.

Impact Statement:
CBP utilizes Wickr as its secure messaging platform that enables voice and video chat, as well as file, video and photo transfers. Failure to renew the existing licenses will severely impact the ability to monitor and support mission requirements for mobile devices, laptops and workstations.

## Financial summary:

| | | | |
|---|---|---|---|
| **Request $:** | $942,275.00 | **Bus. Plan Org ID #:**<br>**Formulation $:** | |
| **Type of Funding:** | Transfer in via SDR | **TEPV:** | $942,275.00 |
| **Previous Year Funding:** | $714,600.00 | **Contract Type:**<br>**(FFP, LH, T&M, Cost Reimbursable, Hybrid, etc.)** | FFP |
| **Contract Vehicle:**<br>**(EAGLE, TABBS, PACTs, TACCOM, DHS ELA BPA, FSII, GSA IT Schedule, CBP IDIQ, CBP BPA, Open Market, etc.)** | FSII | **Options:** | |
| **Requirement POP Start:** | 9/16/2021 | **Requirement POP End:** | 9/15/2022 |
| **Total POP (including option periods):** | 9/16/2021 – 9/15/2022 | **FY22 Projected Out-Year Cost:** | $989,388.75 |

**Market Research Report**
Department of Homeland Security
Customs and Border Protection
Enterprise Networks and Technology Support Directorate
**Wickr Software Licenses**
**PR # 2012-1093**
**April 5, 2021**

---

## I. Authority

Market research is required in accordance with:

- FAR 7.102, Acquisition Planning Policy
- FAR 10.001, Market Research Policy

## II. Background Information

CBP is deploying a secure, multi-capability messaging capability that will enable CBP officers, agents, and staff to communicate in an ultra-secure, yet auditable manner. To support this requirement, CBP is engaging with Wickr Inc. to leverage their software capabilities.

The CBP Office of Information and Technology (OIT) has a significant need to procure Wickr Software. Wickr is an instant messaging application which provides users with a secure messaging platform that enables voice and video chat, as well as file, video and photo transfers. For example, CBP requires a secure messaging application to meet multiple use-cases across all components. In particular CBP users require the ability to securely share operationally relevant information between field users, between primary and secondary inspection areas in Ports of Entry, the ability to communicate with agency counterparts while on foreign assignment, and the ability to distribute strategic communications from senior leadership to the officer and agent level. CBP-approved users of Wickr will be able to access the application from mobile devices, laptops and workstations. This will allow for greater coordination at the operational and strategic planning level, as well as tactical coordination when needed.

The scope of this delivery order shall include several areas of capabilities:

1. The renewal of the existing Wickr user licenses and the ability to increase the number of CBP licenses available for users. The renewal period shall start at the end of the existing license period.
2. Professional Service Support hours to be provided by Wickr.
3. Options for future development to support operational use cases such as:
    a. The development of Wickr plugin to integrate with Team Awareness Kit (TAK) for both iPhone and Android.
    b. Integrated Auth support for Macintosh OS X & Windows integrated AUTH clients using Azure as the Identity Provider (IDP).
4. Provide a solution to support High Availability (HA) and minimize the infrastructure downtime. The current environment is utilizing Docker Containers which does not allow for HA. The Docker Containers need to be migrated to Kubernetes Containers which would provide HA.

5. Create role base access controls (RBAC) with in the Wickr backend portal, Admin console, and replicated dashboard.
6. Currently both internal and external users are required to use a configuration file to onboard when launching Wickr. Develop a seamless workflow that does not require a configuration file to onboard both internal and external federation of agencies.

The contractor shall have total program responsibility for ensuring that the requirements in this SOW are met.

This procurement will be competed through First Source II (FSII) vendors. The contract will be firm fixed price.

The market research for the was conducted in February 2021 and is anticipated to be **$942,275.00.**

The AAP # for this procurement is **P2021054245.**

The Point of Contact (POC) for this procurement is:

| Name | Title | Office | Telephone | E-mail Address |
|---|---|---|---|---|
| (b)(6), (b)(7)(C) | Technical POC | OIT/ENTS/NAED | (b)(6), (b)(7)(C) | (b)(6), (b)(7)(C) |

## III. Initial Requirements (as identified by the program office)

The contractor shall provide the following in order to support CBP OIT's infrastructure environment:

- Secure messaging software to include
  - Between 4,000 and 21,000 user licenses based on operational need.
  - Integration of Wickr client and ADFS version 5.0
  - Training and training documentation
  - Professional services not to exceed 300 hours annually
  - 24/7/365 Concierge Support services

This requirement is for a software solution that a single vendor can supply.

| Contract Line Item Number (CLIN) | Subject Line Item Number (SLIN) | Scope | Type | Quantity |
|---|---|---|---|---|
| 0001 | | **Software System Subscription (per unit, per year)** | | |
| | 0001A | Wickr Enterprise Licenses | Each | 4,000 |
| | 0001B | Wickr Enterprise Compliance Module | Each | 4,000 |
| | | | | |
| 0002 | | **Professional Services** | | |
| | 0002A | Professional Service Hours above Level III support for system management. (300 hours) | Hours | 300 |

Wickr Enterprise Package, to include the following:

- 4,000 user licenses.
- Training and training documentation
- Professional services not to exceed 300 hours annually
- 24/7/365 Help-desk support services

**Contract Data Requirements**

| | | |
|---|---|---|
| CDRL001 | System Data: Messages, Files, Metadata, etc.. | As Requested, At Contract Completion |
| CDRL002 | Installation and Software Documentation | At Contract Award |
| CDRL003 | Optional Platform Development | Contract Award |
| CDRL004 | Training Documentation | At Contract Award |

**Description of the Government's requirement in terms of:**

**Cost-effectiveness Issues Associated with the Requirements**

This procurement is to provide a instant messaging application which provides users with a secure messaging platform that enables voice and video chat, as well as file, video, and photo transfers.

**Schedule Requirements**

The period of performance for these licenses, support and professional services will be **9/16/2021 – 9/15/2022**.

## IV. Participants in Market Research

The Market Research was performed by the below team members. The analyst assembled the pricing for the maintenance based on similar purchases made for other projects through CBP suppliers and assembled the IGCE.

| Name | Title | Office | Telephone | E-Mail Address | Role in Market Research |
|---|---|---|---|---|---|
| (b)(6), (b)(7)(C) | COR | OIT/ENTSD | (b)(6), (b)(7)(C) | | Content creator |
| | Technical POC | OIT/ENTSD /NAED | | | SME |
| | Analyst | OIT/ENTSD /AQM | | | Analyst |

## V. Market Research Techniques and Sources

Describe techniques and sources used during market research. The following table may help structure and summarize the techniques used in the market research effort.

| Check if part of research | Sources Used in Market Research | Details of Research/Comments |
|---|---|---|
| | DHS advance acquisition plan reviewed | |
| X | Acquisition history reviewed | Referenced FY20<br>PR#2011-9757<br>PO#04C20P0538 |
| X | Other recent market research reviewed | |
| X | Interviewed knowledgeable individuals in industry | |
| X | Interviewed knowledgeable individuals in Government | Gathered information from engineers and SMEs |
| X | Government databases reviewed | |
| | Commercial databases reviewed | |
| | Participated/attended tradeshows and industry conferences | |
| | Professional journals reviewed | |
| X | Source lists of DHS and other Government agencies reviewed | |
| | Catalog and product literature reviewed | |
| | Participated in DHS small business vendor outreach sessions | |
| | Reviewed requirements with Small Business Specialist | |
| X | Reviewed existing DHS-wide and Multi-Component Contract Vehicles with DHS Strategic Sourcing Program Office and/or on DHS Enterprise-wide Contract Vehicle Portal | FSII supply sources |
| | Other: Researched major competitors and products | |

| Check if part of research | Sources Used in Market Research | Details of Research/Comments |
|---|---|---|
| | **Priority Sources Reviewed** | |
| | Services: Procurement list maintained by the Committee for Purchase from People who are Blind or Severely Disabled (AbilityOne) (formerly Javits-Wagner-O'Day (JWOD) Program at: http://www.AbilityOne.gov | |
| | Services: Federal Supply Schedules | |
| | Services: Federal Prison Industries | |
| | Mandatory sources reviewed (per FAR Part 8) if applicable for:<br>➢ Public utility services<br>➢ Printing and related supplies | |

| | | |
|---|---|---|
| | ➢ Leased motor vehicles<br>➢ Helium<br>➢ Strategic and critical materials from inventories exceeding Defense National Stockpile Requirements | |
| | Services: Commercial sources (includes educational and non-profit institutions) | |
| | Other: First Source II Vendors | |
| | **References/Sources Checked** | |
| X | Existing intra-/inter-agency contract vehicles, e.g. Interagency Contract Directory at: https://www.contractdirectory.gov/contractdirectory/ and DHS's Enterprise-wide Contract Vehicle Portal at: http://dhsconnect.dhs.gov/org/comp/mgmt/cpo/oss/Pages/StrategicSourcing.aspx | http://dhsconnect.dhs.gov/org/comp/mgmt/cpo/oss/Documents/Strategic%20Sourcing/Department-wide-Component-wide%20Contract%20Vehicles%20-%20Currently%20In%20Place/CWMS/main.htm |
| | System for Award Management (SAM) at: https://www.sam.gov/portal/public/SAM/) | |
| | Department of Labor Service Contract Act (SCA) and Davis-Bacon Act (DBA) wage determination information at: www.wdol.gov | |
| | Past Performance Information Retrieval System (PPIRS) at: www.ppirs.gov or Contractor Performance Assessment Reporting System (CPARS) at http://www.cpars.csd.disa.mil/cparsmain.htm | |
| | Other: | |

## VI. Identify Product/Services and Sources Able to Meet the Requirement

As Wickr provides professional services to assist with instant messaging application, it is recommended that this procurement be competed utilizing the First Source II contract vehicle. All of the products listed in the BOM are commercially available. First Source II vendors would be offered a fair opportunity to bid on this requirement.

In support of obtaining the Approval to Operate (ATO), the Contractor shall provide documentation on security controls and assist with addressing security findings.

Professional services personnel MUST submit his/her Background Investigation (BI) paperwork in e-QIP (Electronic Questionnaires for Investigations Processing) for CBP clearance and systems access within 15 days of award.

There are several third-party vendors that provide the required Wickr licenses, support, and professional services. The following the First Source II vendors that were found during this market research:

**FY21 Quotes Received**

1. V3Gate - $1,059,356.00
2. C&C International - $1,087,600.00
3. Merlin - $1,704,960.00
4. iGov - $942,275.00

**Information obtained from each source contacted**

Market research (reviewing catalogs and other generally available product literature published by manufacturers, distributors, and dealers or available on-line) has indicated that comparable products exist in the commercial marketplace.

## VII. Description of the Commercial Marketplace

Market research indicates that the government's requirements in the SOW will be met by First Source II vendors.

## VIII. Prevalent Business Practices

Government requirements and regulations will dictate the business practices and terms and conditions during the period of performance of this program. The First Source II has included standard terms and conditions and industry business practices for this requirement.

**Description of generally accepted business practices that differ from standard Government practices**

No unusual or unique business practices have been identified through this market research.

**Contract Financing**

Contract financing is not applicable in this procurement.

## IX. Pricing and Market Issues

An IGCE was prepared in support for this procurement. Price sources from First Source II will assure current market pricing. Pricing is presumed to be fair and reasonable.

## X. Other Considerations

All companies must also abide by Section 508 applicability for Electronic and Information Technology as outlined in the Statement of Work (SOW).

## XI. Market Analysis Summary

Based on the requirements, the First Source II contract vehicle is an appropriate tool for this procurement.

The following table provides a checklist for Market Analysis Summary information:

| Yes | No | Market Analysis Summary |
|---|---|---|
| X | | Are there products/services and sources capable of satisfying the Government's requirements? |
| X | | Are commercial items available to meet requirements? |
| | X | Are commercial items available that could be modified to meet requirements? |
| | X | Are commercial items available that could meet requirements if the requirements are modified to a reasonable extent? |
| | X | Are available items used exclusively for Governmental purposes? |
| | | If commercial items are not available, are non-developmental items available to meet requirements? |
| | | If commercial items are not available, are non-developmental items available that could be modified to meet requirements? |
| | | If commercial items are not available, are non-developmental items available that could be modified to meet requirements if the requirements are modified to a reasonable extent? |
| X | | Could commercial items or non-developmental items be incorporated at the Component level? |
| X | | Provided: Customary industry terms and conditions including warranties, buyer financing, discounts |
| | X | Provided: Requirements of any laws and regulations unique to the item being acquired |
| X | | Provided: Extent of competitive environment |
| | | Provided: Environmental considerations and concerns |
| | | Provided: SAFETY Act consideration/applicability |
| X | | Provided: Distribution and support capabilities of potential vendors, including alternative arrangements and cost estimates |
| X | | Provided: Size and status of potential sources (including small business status and if use of source is required by FAR Part 8) |
| X | | Provided: Identify available commercial items and describe the respective merits and shortcomings of each |
| | | Provided: Description of any market conditions that may be time sensitive or changes in supply or demand, technology, laws, and supplier costs, etc. |
| X | | Provided: Identification of potential sources. Description of capabilities of individual vendors, pricing information; delivery schedules, and standard terms and conditions, such as incentives and warranties |
| | | Provided: Any market surveys developed by industry or other federal agencies |
| | | Provided: Pricing issues, price ranges, and price variations |

| | | |
|---|---|---|
| | | Provided: Description of industry/market trends – technical/pricing/business, etc. |
| | | Provided: Buy American Act Consideration |
| | | Provided: Trade Agreements Act Consideration |
| | | Provided: Other: Specify |

Document Produced in

Native Format

**Acquisition Alert 19-11**
**Attachment 2: Inherently Governmental and Critical Functions Product Service Code Exemption Memo**

| | |
|---|---|
| MEMORANDUM FOR: | Contracting Activity |
| FROM: | Requirements Official |
| SUBJECT: | Inherently Governmental and Critical Functions Product Service Code (PSC) Exemption Memorandum |
| PR Number: | PR # 2012-1093 |
| Name of Requirement: | Wickr Software Licenses |
| Exempt PSC and Description: | 7D20 - IT and Telecom - Service Delivery Management (hardware and Perpetual License Software) |
| NAICS: | 541511 – Applications software programming services, customer |

The requirements in the attached procurement request package are on the PSC Exemption List and do not require an Inherently Governmental and Critical Functions Analysis.

The requirements official has reviewed Federal Acquisition Regulation (FAR) 7.503(c) for examples of functions considered inherently governmental and FAR 7.503(d) for examples of functions generally not considered inherently governmental. None of the functions to be performed in the resultant contract action is inherently governmental.

_____
Requirements Official Signature:
(b)(6), (b)(7)(C)
Task Manager
Mobility and Collaboration Branch

_____
Date

Message

**From:** (b)(6), (b)(7)(C)

**Sent:** 4/19/2021 5:39:03 PM

**To:** (b)(6), (b)(7)(C)

**CC:** ENTS-FMT [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=c5d60f0e72d44f6fbdf7239caafcc08b-ENTS-FMT_Co]

**Subject:** RE: SDR

**Attachments:** 20121093 - WICKR SW Licenses IGCE_v1 04162021.xls

**Flag:** Read

Hi (b)(6), (b)(7)(C)

This is what I came up with. I added an increased from last year's pricing to come up with the latest estimate. I think you had asked a question in regards to the cost of hosting the application, but I do not know what that costs is. The attached is only for the software licenses and professional support.


(b)(6), (b)(7)(C)
Enterprise Networks and Technology Support Directorate
Office of Information and Technology
Enterprise Services
Customs and Border Protection
Department of Homeland Security
Cell – (b)(6), (b)(7)(C)




**From:** (b)(6), (b)(7)(C)

**Sent:** Monday, April 19, 2021 1:36 PM

**To:** (b)(6), (b)(7)(C)

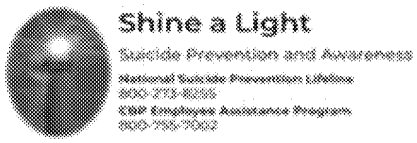
**Cc:** ENTS-FMT <ENTSFMT@cbp.dhs.gov>

**Subject:** FW: SDR

Hi (b)(6), (b)(7)(C)

Do you have the input for Wickr so that we can begin working on the SDR? Also, please see below as an FYSA.


(b)(6), (b)(7)(C)
DHS/CBP/OIT/ENTSD
Financial Management Branch
Office:
Mobile: (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
ENTS-FMT: ENTSFMT@cbp.dhs.gov




**From:** (b)(6), (b)(7)(C)
**Sent:** Monday, April 19, 2021 1:33 PM
**To:** (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
**Cc:** (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
**Subject:** RE: SDR

(b)(6), (b)(7)(C)

As the anticipated costs for the SDR may include both the software licenses (Material Group 315B), plus services of travel NTE, I'm not sure if the SDR fields have ways to show those differences. If not, I suggest to include them in the narrative field.

We'll keep our eyes open for the SDR. Let us know if you have any other questions.

Thanks,
(b)(6), (b)(7)(C)

**From:** (b)(6), (b)(7)(C)
**Sent:** Monday, April 19, 2021 1:13 PM
**To:** (b)(6), (b)(7)(C)
**Cc:** (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
**Subject:** RE: SDR

(b)(6), (b)(7)(C) - not a problem. We'll sign the SDR when it comes across

(b)(6), (b)(7)(C) (CC'd) take care of the financial / business side of INVNT and can provide you the required info when the time comes.

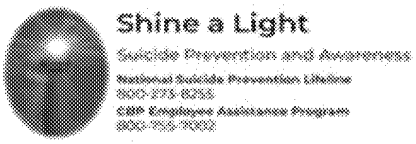
Best
(b)(6), (b)(7)(C)

**From:** (b)(6), (b)(7)(C)
**Sent:** Monday, April 19, 2021 1:08 PM
**To:** (b)(6), (b)(7)(C)
**Cc:** (b)(6), (b)(7)(C)
**Subject:** RE: SDR

Hi (b)(6), (b)(7)(C)

(b)(6), (b)(7)(C) are working on the Wicker requirements. An SDR is forthcoming for this support. Unfortunately we are not able to use the funding string unless an SDR is approved as the lines will require OC's Budget Officer involvement to release. I will reach out to (b)(6), (b)(7)(C) to get an update on their progress.

(b)(6), (b)(7)(C)
DHS/CBP/OIT/ENTSD
Financial Management Branch
Office: (b)(6), (b)(7)(C)
Mobile
(b)(6), (b)(7)(C)
ENTS-FMT: ENTSFMT@cbp.dhs.gov




**From:** (b)(6), (b)(7)(C)
**Sent:** Monday, April 19, 2021 11:54 AM
**To:** (b)(6), (b)(7)(C)
**Cc:** (b)(6), (b)(7)(C)
**Subject:** RE: SDR

Thanks (b)(6), (b)(7)(C)

(b)(6), (b)(7)(C) – we could do an SDR (harder) or you could merely cite our funding line for Wickr (way easier). There is serious talk of funding sweeps in the next month. Would like to load up the PR asap. Happy to chat about it!

Best
(b)(6), (b)(7)(C)

**From:** (b)(6), (b)(7)(C)
**Sent:** Monday, April 19, 2021 11:45 AM
**To:** (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
**Subject:** SDR

Hi (b)(6), (b)(7)(C)

Per our conversation last Thursday, you said a need to complete the PRs. I assume you meant the Service Delivery Request (SDR). I talked to ENTSD Financial Management Team Supervisor, (b)(6), (b)(7)(C) and she will reach out to you for more information. Thank you.

V/R

(b)(6), (b)(7)(C)
Director
Network Services (Engineering & Operations)
DHS|CBP|ES|OIT|ENTSD
(b)(6), (b)(7)(C)
Phone: 571-319-1847

# Document Produced in Native Format

# Document Produced in Native Format

Document Produced in

Native Format