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 – NEED TO SEND AS PDF TO DHS, OCC, USBP, OFO, Policy WG members
3. Email status from (b)(6), (b)(7)(C) that AC can forward to CIO (b)(6), (b)(7)(C) 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

Appointment

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

Sent: 11/15/2021 1:53:33 PM

To:

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

CC:

Subject: Canceled: Messaging Apps Policy Working Group
Location: Microsoft Teams Meeting

Start: 11/3/2021 5:30:00 PM
End: 11/3/2021 6:30:00 PM
Show Time As: Free

Recurrence: Weekly
every 2 week(s) on Wednesday from 1:30 PM to 2:30 PM

-----Original Appointment-----
From: (b)(6), (b)(7)(C)
Sent: Wednesday, October 20, 2021 3:12 PM
To: (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)

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

Cc: (b)(6), (b)(7)(C)
Subject: Messaging Apps Policy Working Group
When: Occurs every 2 week(s) on Wednesday effective 10/20/2021 until 4/6/2022 from 1:30 PM to 2:30 PM (UTC-05:00) Eastern Time (US & Canada).
Where: Microsoft Teams Meeting

All,

Following CBP's acquisition of secure messaging services through the award of a contract with Wickr, the Privacy Division will be leading an effort to develop both Privacy Compliance Documentation [Privacy Threshold Analysis (PTA) & Privacy Impact Assessment (PIA)] and a Secure Messaging Platform Policy. I will provide an outline of the PTA and PIA process as well as provide a timeline for completion.

The Privacy Division is requesting all representatives of all operational and support offices involved in the use of Wickr or other secure messaging services come prepared to discuss their offices usage of these tools. In addition, working group members should be prepared to provide their thoughts about potential policy bounds that may be necessary around the usage of the messaging Apps.

Following the meeting, I will send out meeting minutes with due outs as well as a invite for the next meeting. Please forward this invite to anyone you think I may have missed. If you would like to be removed from future messages related to this group, please let me know.

Regards,

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

Microsoft Teams meeting

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

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

Appointment

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

Sent: 1/25/2022 5:07:40 PM

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

Subject: Review Messaging App Directive

Attachments: Secure Messaging Apps Directive_20220113_for review (RIM preliminary).docx; Secure Messaging Apps Directive_20220113_for review (RIM preliminary2).docx

Location: Microsoft Teams Meeting

Start: 1/25/2022 6:00:00 PM

End: 1/25/2022 6:45:00 PM

Show Time As: Tentative

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

Attached with GREEN comments is my very initial set of comments and observations for expansion during our discussion

---

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

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

Attendees: (b)(6), (b)(7)(C)
Location: Microsoft Teams Meeting
Importance: High
Subject: Review for XD (b)(6), (b)(7)(C)
Start Time: Tue 4/5/2022 8:00:00 PM (UTC)
End Time: Tue 4/5/2022 8:30:00 PM (UTC)
Required Attendees: (b)(6), (b)(7)(C)

Secure Msging App - Update

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

From: (b)(6), (b)(7)(C)
To:
Subject: FW: Wickr User Accounts Transition to Compliance Network
Date: Wednesday, September 22, 2021 1:15:51 PM

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

This was the email sent to the folks still on the old network:

Greetings,

If you are receiving this email you have been identified as an active Wickr user. As we prepare to transition your user account to our new compliance network, please review the details below regarding your Wickr account as your current account will be deleted:

What's happening?

- We are transitioning Wickr legacy user accounts to our new Compliance network. This new compliance network allows users to take advantage of improvements within the Wickr infrastructure, as well as the removal of the configuration file requirement during enrollment or additional device logins.

What actions do you need to take?

- Be aware that your current legacy account will be deleted and all data will be removed. Please appropriately save any required data before the deletion deadline highlighted below.
- You will be sent a new token via email with instructions to sign-in into the new network.

When is it happening?

- Legacy accounts will be deleted on Sunday 9/26/21 @11:45pm
- New tokens will be sent via email from @WICKR_PROJECT_SUPPORT on Monday 9/27 @ 12am

Questions or problems?

Please directly contact Wickr Project Support @WICKR_PROJECT_SUPPORT

From: (b)(6), (b)(7)(C)
To:
Subject: FW: Wickr User Accounts Transition to Compliance Network
Date: Wednesday, September 22, 2021 1:15:51 PM

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

This was the email sent to the folks still on the old network:

Greetings,

If you are receiving this email you have been identified as an active Wickr user. As we prepare to transition your user account to our new compliance network, please review the details below regarding your Wickr account as your current account will be deleted:

What's happening?

- We are transitioning Wickr legacy user accounts to our new Compliance network. This new compliance network allows users to take advantage of improvements within the Wickr infrastructure, as well as the removal of the configuration file requirement during enrollment or additional device logins.

What actions do you need to take?

- Be aware that your current legacy account will be deleted and all data will be removed. Please appropriately save any required data before the deletion deadline highlighted below.
- You will be sent a new token via email with instructions to sign-in into the new network.

When is it happening?

- Legacy accounts will be deleted on Sunday 9/26/21 @11:45pm
- New tokens will be sent via email from @WICKR_PROJECT_SUPPORT on Monday 9/27 @ 12am

Questions or problems?

Please directly contact Wickr Project Support @WICKR_PROJECT_SUPPORT

Department of Homeland Security
Customs & Border Protection (CBP)
Statement of Work for
Wickr Inc.
PR 2011976 , 20119757

1.0 INTRODUCTION

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.

2.0 SCOPE

This Statement of Work (SOW) describes delivery order for 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.
4. Travel of Wickr personnel to support training, deployment, and upgrades. Travel will be invoiced as time and material (T&M).

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

Per the SBIR and the Small Business Technology Transfer (SBTT) Program Policy Directive, prior Phase I and Phase II awards satisfy competition requirement for this effort. An agency that wishes to fund an SBIR Phase III project is not required to conduct another competition for the Phase III award.

A written Acquisition Plan is not required, pursuant to HSAM 3007.102(g)(9).

3.0 PERIOD OF PERFORMANCE

The period of performance for this Direct award is from September 16, 2020 through September 15th, 2025. The first Delivery Order will be September 15th, 2020 through September 15th, 2021.

4.0 DELIVERY REQUIREMENT

No partial shipments are permitted unless specifically authorized at the time of award.

Electronic Delivery of software licenses shall be made to JOSHUA.J.POWELL@cbp.dhs.gov

**SHIPMENT MUST REFERENCE GOVERNMENT PURCHASE ORDER # ON PACKING SLIPS AND BOXES. IF NOT, THE EQUIPMENT WILL BE RETURNED TO THE VENDOR.

5.0 TYPE OF TASK ORDER

This award will establish a Small Business Innovative Research (SBIR) Phase III direct contract award.

6.0 DELIVERABLES AND SUPPORT

Wickr Enterprise Package, to include the following:

- 3,000 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
CDRL002	Training Documentation	At Contract Award

7.0 INVOICING PAYMENT

Beginning April 11, 2016, payment requests for all new awards must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP). Payment terms for existing contracts and orders awarded prior to April 11, 2016 remain the same. The Contractor must use IPP for contracts and orders awarded April 11, 2016 or later, and must use the non-IPP invoicing process for those contracts and orders awarded prior to April 11, 2016.

"Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Payment documentation and process" and the applicable Prompt Payment clause included in this contract. The IPP website address is: https://www.ipp.gov.

Under this contract, the following documents are required to be submitted as an attachment to the IPP invoice:

No additional documentation is required.

To constitute a proper invoice, each invoice shall be annotated with at least the following information:

-Order number
-Description of services provided for a specified time period.
-Unit price and total amount of each item.
-Discount terms
-Company name, telephone number, taxpayer's identification number, and complete mailing address to which payment will be mailed.

The IPP was designed and developed for Contractors to enroll, access and use IPP for submitting requests for payment. Contractor assistance with enrollment can be obtained by contacting (b)(6), (b)(7)(C) or phone (b)(6), (b)(7)(C)

If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the contracting officer.

8.0 POINTS OF CONTACT

Contracting Officer: David Seay
DHS/U.S. Customs and Border Protection
Office of Acquisition
1331 Pennsylvania Ave.
Washington, DC 20229
Email: (b)(6), (b)(7)(C)

COR:

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

Technical POCs:

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

National Finance Center:
(b)(7)(E)

9.0 ENTERPRISE ARCHITECTURE (EA) COMPLIANCE

The Offeror shall conform to the Federal Enterprise Architecture (FEA) model and the DHS and CBP versions of the FEA model, as described in their respective EAs. All models will be submitted using Business Process Modeling Notation (BPMN 1.1 or BPMN 2.0 when available) and the CBP Architectural Modeling Standards. Universal Modeling Language (UML2) may be used for infrastructure only. Data semantics shall be in conformance with the National Information Exchange Model (NIEM). Development solutions will also ensure compliance with the current version of the DHS and CBP target architectures.

Where possible, the Offeror shall use DHS/CBP approved products, standards, services, and profiles, as reflected by the hardware, software, application, and infrastructure components of the DHS/CBP TRM/standards profile. If new hardware, software, or infrastructure components are required to develop, test, or implement the program, these products will be coordinated through the DHS and CBP formal Technology Insertion (TI) process (to include a trade study with no less than four alternatives, one of which reflecting the status quo and another reflecting multi-agency collaboration). The DHS/CBP TRM/standards profile will be updated as TIs are resolved.

All developed solutions shall be compliant with the Homeland Security (HLS) EA.

All IT hardware and software shall be compliant with the HLS EA.

Compliance with the HLS EA shall be derived from and aligned through the CBP EA. Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval, and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.

Development of data assets, information exchanges, and data standards will comply with the DHS Data Management Policy MD 103-01. All data-related artifacts will be developed and validated according to DHS Data Management Architectural Guidelines.

Applicability of Internet Protocol version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS EA (per OMB Memorandum M-05-22, August 2, 2005), regardless of whether the acquisition is for modification, upgrade, or replacement. All EA related component acquisitions shall be IPv6 compliant, as defined in the USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance, defined in the USGv6 Test Program.

10.0 INFORMATION SECURITY

The Contractor must comply with administrative, physical and technical security controls to ensure that the Government's security requirements are met. During the course of this task order, Contractor must not use, disclose, or reproduce data, which bears a restrictive legend, other than as required in the performance of this SOW.

10.1 DHS SECURITY POLICY TERMS AND CONDITIONS

All hardware, software, and services provided under this task order must be compliant with DHS 4300A DHS Sensitive System Policy and the DHS 4300A Sensitive Systems Handbook.

10.2 COMPLIANCE WITH DHS SECURITY POLICY

All hardware, software, and services provided under this task order must be compliant with DHS 4300B DHS Sensitive System Policy and the DHS 4300B Sensitive Systems Handbook.

10.3 SENSITIVE PII DATA

When a contractor on the behalf of CBP, handles Sensitive PII data, stores and transmits, the contractor will Accredit (ATO) this information system to the (HHM) FIPS level.

10.4 HSAR 3052.204-70 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (JUN 2006)

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within 60 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include—

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e)Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

(End of clause)

3052.204-71 Contractor employee access. (JUN 2006)

(a) *Sensitive Information*, as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's

employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Representative (COR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COR in writing as necessary for performance of the work under this contract. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS Component.
It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee,
with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) The individual must be a legal permanent resident of the U. S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;

(2) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and

(3) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

11.0 ACCESSIBILITY REQUIREMENTS (SECTION 508)

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable EIT accessibility standards have been identified:

Section 508 Applicable EIT Accessibility Standards
36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

36 CFR 1194.31 Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Section 508 Applicable Exceptions

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any

selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

From: (b)(6), (b)(7)(C)
To:
Cc:
Subject: RE: Question regarding recovery of Wickr chat messages.
Date: Friday, April 23, 2021 5:07:02 PM

Thank you so much. I believe you have answered our questions. We appreciate your help.

(b)(6), (b)(7)(C)
Labor and Employee Relations Specialist
Customs and Border Protection
Human Resources Policy & Programs Directorate
Office: (b)(6), (b)(7)(C)
Cell Phone: (b)(6), (b)(7)(C)
Fax: (b)(6), (b)(7)(C)

From: (b)(6), (b)(7)(C)
Sent: Friday, April 23, 2021 2:03 PM
To: (b)(6), (b)(7)(C)
Cc: (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
Subject: Re: Question regarding recovery of Wickr chat messages.

Hi. I have at least part of the answer. I should have sent to you. The system is like any other CBP system and/or communication. It is subject to record retention policy.

The messages would be in the compliance module but they do disappear and or delete from your devices.

This may not answer your question fully. I am trying to learn more but the wickr expert is on leave until next week.

So we are happy to let you try it out etc. but not sure I have the full answer for you.

Let me know what else you need. Thanks.

(b)(6), (b)(7)(C)
Senior Portfolio Manager
CBP Office of Innovation (INVNT)
CBP Headquarters
US Customs and Border Protection
(b)(6), (b)(7)(C)
Email: (b)(6), (b)(7)(C)

On Apr 23, 2021, at 4:58 PM, (b)(6), (b)(7)(C) (b)(6), (b)(7)(C) wrote:

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

Happy Friday!

I just wanted to follow up with you regarding Wickr. Were you able to find out if OIT can retrieve messages that are burned on receipt or deleted?

Thank you,

(b)(6), (b)(7)(C)
Labor and Employee Relations Specialist
Customs and Border Protection
Human Resources Policy & Programs Directorate
Office: (b)(6), (b)(7)(C)
Cell Phone: (b)(6), (b)(7)(C)
Fax: (b)(6), (b)(7)(C)

From: (b)(6), (b)(7)(C)
Sent: Friday, April 16, 2021 9:39 AM
To: (b)(6), (b)(7)(C)
Cc (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
Subject: RE: Question regarding recovery of Wickr chat messages.

Hi, OK thanks. Wickr is secure and encrypted. Will find out the answer to your question. I know there is a "burn upon receipt" type of message as well a regular delete, but not sure about retrievable, will find out and get back to you. Thanks, (b)(6), (b)(7)(C)

(b)(6), (b)(7)(C)
Sr. Portfolio Manager
CBP Office of Innovation (INVNT)
CBP Office of the Commissioner
U.S. Customs and Border Protection
Mobile: (b)(6), (b)(7)(C)
Email: (b)(6), (b)(7)(C)
<image001.png>

From: (b)(6), (b)(7)(C)
Sent: Friday, April 16, 2021 12:37 PM
To: (b)(6), (b)(7)(C)

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

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

Subject: RE: Question regarding recovery of Wickr chat messages.

We have 10 employees on our team, but it is possible our director might want to extend it to the entire LER Field. Not sure of those numbers, but maybe around 80 or 90.

We frequently discuss our cases in chat, and are concerned that even if we delete a chat, it will remain out there for OIT to retrieve. This is concerning because should the case go before a 3rd party, those chats would be discoverable. Can you tell us would OIT still be able to retrieve messages that are deleted, and is Wickr secure?

Thank you so much for your assistance.

(b)(6), (b)(7)(C)
Labor and Employee Relations Specialist
Customs and Border Protection
Human Resources Policy & Programs Directorate
Office: (b)(6), (b)(7)(C)
Cell Phone: (b)(6), (b)(7)(C)
Fax: (b)(6), (b)(7)(C)

From: (b)(6), (b)(7)(C)
Sent: Friday, April 16, 2021 9:29 AM
To: (b)(6), (b)(7)(C)
Cc: (b)(6), (b)(7)(C)

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

Subject: RE: Question regarding recovery of Wickr chat messages.

Hi, Depending on how many licenses, there will probably be no cost.

(b)(6), (b)(7)(C)
Sr. Portfolio Manager
CBP Office of Innovation (INVNT)
CBP Office of the Commissioner
U.S. Customs and Border Protection
Mobile: (b)(6), (b)(7)(C)
Email: (b)(6), (b)(7)(C)
<image001.png>

From: (b)(6), (b)(7)(C)
Sent: Friday, April 16, 2021 12:21 PM

To: (b)(6), (b)(7)(C)
Cc: (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
Subject: RE: Question regarding recovery of Wickr chat messages.

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

Thank you so much for reaching out to us.

I have copied a few of my co-workers who may have some questions for you.

Can you tell us how we go about getting a license and what the cost would be?

Thank you,

(b)(6), (b)(7)(C)
Labor and Employee Relations Specialist
Customs and Border Protection
Human Resources Policy & Programs Directorate
Office: (b)(6), (b)(7)(C)
Cell Phone: (b)(6), (b)(7)(C)
Fax: (b)(6), (b)(7)(C)

From: (b)(6), (b)(7)(C)
Sent: Friday, April 16, 2021 8:13 AM
To: (b)(6), (b)(7)(C)
Subject: FW: Question regarding recovery of Wickr chat messages.

Hello,

Happy to try and answer your questions about Wickr- I manage the program right now. Thanks, (b)(6), (b)(7)(C)

(b)(6), (b)(7)(C)
Sr. Portfolio Manager
CBP Office of Innovation (INVNT)
CBP Office of the Commissioner
U.S. Customs and Border Protection
Mobile: (b)(6), (b)(7)(C)
Email: (b)(6), (b)(7)(C)
<image001.png>

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

Sent: Friday, April 16, 2021 11:05 AM
To: (b)(6), (b)(7)(C)
Cc: (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
Subject: FW: Question regarding recovery of Wickr chat messages.

FYI, this request may come your way.

(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, April 16, 2021 11:05 AM
To: (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
Cc: (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
Subject: RE: Question regarding recovery of Wickr chat messages.

The Office of Innovation currently funds and would need to authorize the use of existing WICKR licenses. Please contact (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C) to discuss the feasibility of this and if additional licenses are required.

1 license works on Mobile and Desktop.

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: Thursday, April 15, 2021 12:57 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: Question regarding recovery of Wicker chat messages.

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

I can't speak too in-depth about mobile applications and I've not received any requests on Wickr previously.
I'm going to have to phone a friend, so to speak. :)

I've cc'd the Director for Mobility Communication Branch (b)(6), (b)(7)(C) to advise us with any guidance related to Wickr application.

Thanks!

(b)(6), (b)(7)(C), **CISSP-ISSMP**
(b)(6), (b)(7)(C)
OIT Field Support Directorate
Information Systems Security Manager
US Customs and Border Protection
(b)(6), (b)(7)(C)

From (b)(6), (b)(7)(C)
Sent: Thursday, April 15, 2021 9:17 AM
To: (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
Cc: (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
Subject: RE: Question

Sirs,

I looked up Wickr on the TRM and it says it is permitted on Androids and Iphones. I did not see Desktops. Can you confirm LER's question bellow?

Thanks,

(b)(6), (b)(7)(C)
Field Technology Officer – Central Arizona
Office of Information and Technology, CBP
Department of Homeland Security
(b)(6), (b)(7)(C) Office
Mobile
(b)(6), (b)(7)(C)

** Technology Service Desk Information **
Phone Number: (b)(6), (b)(7)(C)
Name in Global Address List: CBP Technology Service Desk
Email Address: (b)(6), (b)(7)(C)

<image002.png>

From: (b)(6), (b)(7)(C)
Sent: Wednesday, April 14, 2021 3:24 PM
To: (b)(6), (b)(7)(C)
Cc: (b)(6), (b)(7)(C)
(b)(6), (b)(7)(C)
Subject: RE: Question

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

To add to our question below, have you heard about this?

- Certain employees in CBP have received permission to download Wickr enterprise and you can chat, video conference, group messaging. It is the most encrypted thing out there. El Paso Borstar has it already and HQ BP. The government currently purchased 1000 licenses. This is something LER. OPR and OCC need for sure. Goes onto your desktop and cell phones.

Thank you,

(b)(6), (b)(7)(C)
Labor and Employee Relations Specialist

Customs and Border Protection
Human Resources Policy & Programs Directorate
Office: (b)(6), (b)(7)(C)
Cell Phone: (b)(6), (b)(7)(C)
Fax: (b)(6), (b)(7)(C)

From: (b)(6), (b)(7)(C)
Sent: Wednesday, April 14, 2021 12:46 PM
To: (b)(6), (b)(7)(C)
Cc: (b)(6), (b)(7)(C)

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

Subject: Question

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

We often use chat to discuss cases. Now that we use Microsoft Teams instead of Skype, can you tell me if OIT/FOIA would be able to retrieve comments that we delete about cases? This would be important for us should a case go before a 3rd party.

Thank you so much. We appreciate your help.

(b)(6), (b)(7)(C)
Labor and Employee Relations Specialist
Customs and Border Protection
Human Resources Policy & Programs Directorate
Office: (b)(6), (b)(7)(C)
Cell Phone: (b)(6), (b)(7)(C)
Fax: (b)(6), (b)(7)(C)

Attachment 1
NARA Case ID UD-2022-0001
Unauthorized Disposition Report
CBP Records and Information Management
December 2021

Introduction

This report constitutes U.S. Customs and Border Protection's (CBP) response to NARA's Letter regarding CBP's use of WhatsApp and Wickr and unauthorized disposition of certain records.

The letter concerned CBP's planned deployment of Wickr and information contained in the Office of Inspector General (OIG) report, "CBP Targeted Americans with the 2018-2019 Migrant Caravan" (OIG-21-62 - CBP Targeted Americans Associated with the 2018-2019 Migrant Caravan (dhs.gov)) regarding CBP's use of WhatsApp and unauthorized disposition of records.

I. Unauthorized Disposition Report

a. **Description of the records with volume and dates if known.**

CBP Response: A complete description of the records with volume and dates is unknown. Records included but are not limited to communications between CBP and local Mexican officials.

b. **Description of the office maintaining the records.**

CBP Response: CBP does not currently centrally manage WhatsApp records.

c. **A statement of the exact circumstances surrounding the removal, defacing, alteration, or destruction of records.**

CBP Response: Given the widespread use of WhatsApp from October 2018 to February 2019 as indicated in the OIG-21-62 Report, an unknown number of WhatsApp messages were deleted or lost from the devices of several CBP Officials supporting the San Diego Emergency Operations Center (EOC). Though the exact circumstances are not known, the OIG Report indicates that (at least) four CBP officials communicated with the Mexican government using WhatsApp and that none of the four officials retained all their relevant WhatsApp messages. In some instances, the messages were deleted by CBP Officials and in another instance the messages were lost as a result of a government issued mobile phone upgrade.

d. **A statement of the safeguards established to prevent further loss of documentation.**

CBP Response: CBP is currently taking action to establish safeguards to prevent the future loss of messages, including restricting CBP staff access to WhatsApp, records retention training, and

investigating tools that automatically capture and manage WhatsApp messages. See Section II below, CBP's Records Management Corrective Actions.

e. **Details of the actions taken to salvage, retrieve, or reconstruct the records.**

CBP Response: Due to the nature of WhatsApp functionality, there is no practical way to salvage, retrieve, or reconstruct these records.

II. CBP Records Management Corrective Actions

CBP will develop a Corrective Action Plan to address the actions identified below. CBP RIM will provide regular status updates to the NARA Records Management Oversight and Reporting Lead managing CBP's open case of Unauthorized Disposition.

Action 1. Update the approval process for user access to messaging applications.

CBP has restricted users' ability to download WhatsApp. User requests are required to complete an approval process to gain access to WhatsApp. As part of the approval process users will receive specific messaging retention guidance.

To-date, CBP OIT has proactively blocked 41 other known messaging applications from being downloaded onto user devices.

Action 2. CBP will instruct all users about their records management obligations and the consequences of unauthorized disposition.

CBP leadership will issue formal instructions to all CBP users detailing their obligation to retain messages and other records according to DHS and CBP policy. The instruction will include the consequences of unauthorized disposition and notification obligations if it occurs.

Action 3. CBP will require WhatsApp users to manually capture and store messages in an official CBP account.

CBP has developed and will distribute updated guidance on how to manually capture WhatsApp messages. This will ensure that all WhatsApp 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 4. CBP's Office of Information and Technology (OIT) is exploring the viability of the continued operational use of WhatsApp, including looking for a replacement. OIT is conducting a managed messaging platform pilot to replace WhatsApp.

CBP is piloting an enterprise instance of the Wickr messaging application. The Enterprise version of Wickr captures all messages to and from CBP personnel and stores them in a CBP controlled repository. This version captures messages from Wickr even if they have been configured for immediate deletion. The repository contains compliance functionality, allowing retention periods to be configured for messages. This is currently the Wickr version in use at CBP and all messages are retained indefinitely until CBP implements a NARA-approved retention schedule.

CBP is also exploring acquisition and implementation of technology to capture WhatsApp messages and store them in a central repository capable of applying retention rules to messages based on an approved schedule. This solution will allow continued use of WhatsApp in instances where necessary for CBP's mission while applying all appropriate retention rules and functionality to prevent unauthorized disposition. Once the technology is acquired and implemented, CBP will implement the appropriate NARA-approved retention schedule.

CBP will only consider messaging applications for which appropriate retention and compliance solutions are available.

Action 5. 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 CBP stakeholders with equity in the schedule to ensure the retention meets business needs and is implementable. As part of gathering this feedback, CBP RIM will determine if other instances of messaging-related unauthorized disposition have occurred, investigate, and report actual or impending instances consistent with regulations. CBP RIM intends to submit this schedule for NARA approval during Fiscal Year 2022.

Action 6. CBP will develop and implement a CBP Messaging Application Use Directive.

CBP has established a Messaging Applications Policy Working Group to define a comprehensive Secure Messaging Platform policy. This working group includes participants from across CBP.

III. Supplemental Policies and Training Documentation Summary

1. DHS "Records Management for Everyone" mandatory training- CBP Employees are required to take annual records management training developed by DHS. That training reminds 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).
2. DHS Policy Directive 141-03
3. CBP's Records and Information Management (RIM) Directive (2110-040) and updated Records and Information Management Handbook (HB 2100-05B) (Part 3, Section M)

See Attachment 2 for additional detail.

Conclusion

This report has provided CBP's response to NARA's Letter regarding the use of WhatsApp and Wickr and possible unauthorized disposition of records. CBP has detailed the corrective actions in response, including messaging application controls and technical solutions, electronic messaging policy, continued investigation into other messaging application records retention gaps or additional unauthorized disposition, heightened user awareness, and supplemental training. CBP RIM will provide regular status updates to the NARA Records Management Oversight and Reporting Lead managing CBP's open case of Unauthorized Disposition.

Unauthorized Disposition Report

- 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;
  - details of the actions taken to salvage, retrieve, or reconstruct the records.

Mitigation Documentation

Polices and Training

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.*

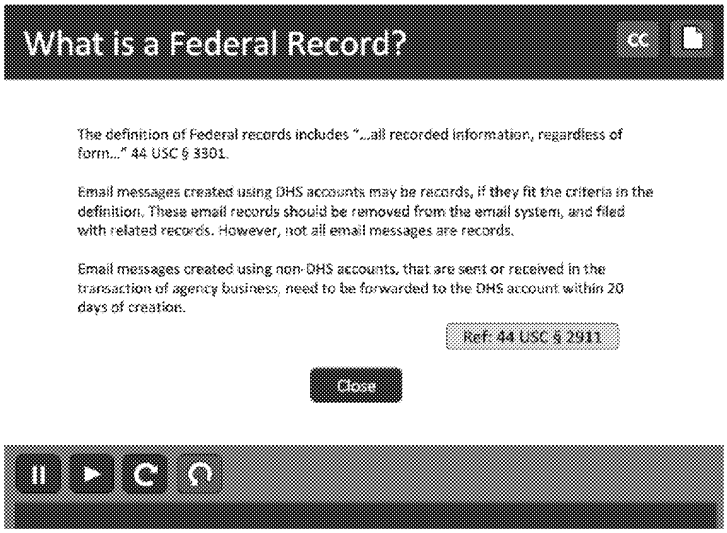
CBP published a new Records Management Directive and updated the Records and Information Management Handbook in June of 2019. CBP RIM is currently reviewing and updating both documents with publication expected in 2022.

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.*
>   - *All CBP employees are responsible for managing the creation and retention of documents created or transmitted on email systems.*

- *Email creators and recipients must decide whether a particular message is appropriate for preservation. In making these decisions, all personnel should exercise the same judgment they use when determining whether to retain and file records in any format.*
    - *This does not require preservation of every email message.*
    - *Its purpose is to ensure preservation of those messages that contain information necessary for adequate and proper documentation of CBP policies, programs, business process transactions, and activities.*

CBP RIM has developed a "RIM 101" training deck that is available to all CBP employees 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. The 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 101 training).



DHS RIM is actively working to update this training.

WhatsApp users' records management guidance comes from the polices outlined in the CBP RIM Directive and Handbook. Since all Wickr messages are centrally stored and managed, there is not any specific records management guidance that is provided to Wickr users when installing or using the application.

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 ensure that the proper records management requirements are included in the policy.

Records Management Corrective Actions for the OIG Investigation

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

> ***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: CBP RIM will develop a retention schedule that covers Messaging Applications and submit to NARA for approval

CBP RIM is currently performing an internal review of the proposed retention schedule that covers the records created by messaging applications. As part of this review, CPB RIM will also gather feedback from affected parties (such as CPB OIT) to ensure the schedule is appropriate and implementable within the organization. It is the intent of CPB RIM to submit this schedule for NARA approval during the current fiscal year.

Action 2: CBP will provide updated guidance to WhatsApp users about archiving messages

Until the deployment of the technology to capture the WhatsApp messages is finalized (see Action 3), CBP WhatsApp users will be reminded of the requirement to manually capture messages and store them in an official CBP account as directed in the CBP Records Management Handbook (Part 3, Section M). CBP RIM will work with CBP OIT to develop updated guidance and documentation on how to manually capture the messages from WhatsApp. This will ensure that users are aware of the records management policies that regulate the 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. As part of this notification process, users will be required to acknowledge that they have received the guidance and will adhere to it.

Action 3: CBP RIM will work with CBP OIT to implement the approved retention schedule for Wickr and WhatsApp messages in the appropriate technology.

CBP is responding to the OIG Audit Recommendation 6 on two fronts. The first front 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 which allows retention periods to be configured for messages. CBP RIM will work with CBP OIT to implement the appropriate schedule after the CBP Messaging schedule is approved by NARA. This is currently the version in use at CBP and all messages are currently retained indefinitely until such time as CBP RIM has an approved retention schedule to implement.

The second front involves the implementation of technology to capture messages from WhatsApp 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 messaging schedule. This solution will allow the continued use of WhatsApp in instances where it is necessary while being able to apply 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 CBPOIT to implement the appropriate retention rules.

Action 4: CBP will send reminders to all users about employee obligations for managing records on non-official accounts and the consequences of unauthorized disposition

CBP RIM will 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. In addition, the messaging will also include references to the consequences of unauthorized disposition and notification obligations when it occurs. The message will be sent by the appropriate authority within CBP.

Message

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

Sent: 4/20/2021 2:31:08 PM

To:

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

Subject: Re: Question about Wickr deleted/burned message retention

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

I need to confirm with (b)(6), (b)(7)(C) who is currently out of the office till May 3, 2021. The Wickr messages are stored in the SQL database. However a tool needs to be built to extract the messages. This is scheduled to be built next month when we start engineering the WICKR FED solution. If a message is sent via burn on read or deleted is will still have a copy within the database. What we don't have at the moment is a way to extract the messages from the DB.

Thanks,

(b)(6), (b)(7)(C) PMP, ITIL V3
Project Manager
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)

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

Sent: Tuesday, April 20, 2021 9:45:25 AM

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

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

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

Subject: Question about Wickr deleted/burned message retention

(b)(6), (b)(7)(C) – Hope you both are well!

I am hoping that you can help me answer a question regarding the Wickr application and how it deals with deleted/burned messages.

Our question: if a user sends a message that they request be burned on receipt, or if a user deletes a message, is this message retained somewhere on the backend for some period of time? If yes, how long is the deleted/burned message retained? Our team wants to make sure the application is complying with CBP's records retention policies.

Thanks for your help!

Best,

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

Emerson Whitney (Contractor)
Deloitte Consulting LLP
Supporting CBP OIT
U.S. Customs & Border Protection
Mobile: (b)(6), (b)(7)(C)
Email: (b)(6), (b)(7)(C)
Alt Email: (b)(6), (b)(7)(C)

Message

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

Sent: 4/20/2021 1:45:25 PM

To:

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

Subject: Question about Wickr deleted/burned message retention

(b)(6), (b)(7)(C) – Hope you both are well!

I am hoping that you can help me answer a question regarding the Wickr application and how it deals with deleted/burned messages.

Our question: if a user sends a message that they request be burned on receipt, or if a user deletes a message, is this message retained somewhere on the backend for some period of time? If yes, how long is the deleted/burned message retained? Our team wants to make sure the application is complying with CBP's records retention policies.

Thanks for your help!

Best,

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

(b)(6), (b)(7)(C) Contractor)
Deloitte Consulting LLP
Supporting CBP OIT
U.S. Customs & Border Protection
Mobile: (b)(6), (b)(7)(C)
Email: (b)(6), (b)(7)(C)
Alt Email: (b)(6), (b)(7)(C)