Privacy Impact Assessment

for the

CBP Web Emergency Operations Center (WebEOC)

DHS Reference No. DHS/CBP/PIA-065

September 13, 2021

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) Web Emergency Operations Center (WebEOC) is CBP's primary emergency notification, event tracking, and incident management system. CBP uses WebEOC for a variety of purposes across the CBP enterprise, including incident management, event tracking, workforce emergency notifications, facility and asset management during disasters, and incident simulations and exercise. Due to its customizable event tracking functionality, CBP also uses WebEOC as the intake point for CBP electronic medical records and individual health assessments of individuals in CBP custody. CBP is publishing this Privacy Impact Assessment (PIA) to provide transparency regarding WebEOC and its many uses, including as the point of collection for Electronic Medical Records (EMR) of individuals in CBP custody, and to provide notice of the privacy risks and mitigations associated with the system.

Overview

As the nation's largest law enforcement agency, CBP is responsible for securing U.S. borders while facilitating lawful travel and trade. As part of CBP's authority to protect the border and enforce applicable laws at the border, CBP is also responsible for the safety and welfare of its large, dispersed workforce, as well as those individuals in CBP custody. CBP uses a host of tools and communication platforms to ensure the CBP workforce has accurate and timely information regarding emergencies and disasters, and to manage incidents and events across the CBP enterprise.

CBP, like many other public sector organizations, uses WebEOC, a commercially available software product, for emergency response, event tracking, and incident management. WebEOC is a popular tool due to its customizable configurations that can meet various CBP program office needs. Most CBP programs use WebEOC to track significant incidents or events, but it can also be used as an event-based case management tool.

CBP deploys WebEOC within the CBP Situation Management System (SMS) information technology security boundary. The SMS supports several offices within the CBP Operational Support (OS) component, including the Information and Incident Coordination Center (IICC). The IICC is the business owner for WebEOC, despite its variety of use cases. The CBP IICC is dedicated to providing real-time law enforcement information and intelligence in order to inform CBP decision makers at all levels. To achieve the mission, IICC manages the CBP Watch (formerly known as the Commissioner's Situation Room[1] or SITROOM) and SMS. CBP Watch

[1] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE CBP SITUATION ROOM, DHS/CBP/PIA-039 (2017 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

is the primary point of contact for significant incident reporting from all CBP operational components and offices, including ports of entry, sectors, stations, air and marine branches, international offices, and CBP Headquarters. In addition, CBP Watch provides connectivity to the DHS National Operations Center (NOC) and other agencies on significant CBP events.

SMS provides CBP a solution for personnel accountability, mass notification, and incident management event tracking during a crisis. SMS was developed in response to Homeland Security Presidential Directive Five (HSPD-5)[2] and the National Incident Management System (NIMS)[3] and was created to "enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system." SMS enables CBP to make informed decisions that enhance CBP's ability to quickly respond to large-scale threats and better support the CBP mission while protecting the CBP workforce.

The SMS is comprised of three subsystems: WebEOC, WebFusion, and IWSAlerts. CBP uses SMS to: 1) monitor and record events, 2) share information within the CBP enterprise; and 3) transmit alerts to the CBP personnel (employees and contractors) through desktop popups, voice and text messages to mobile devices, email, and other devices. While most of the information within SMS is not privacy sensitive or is limited to business contact information for CBP personnel, CBP also uses WebEOC to: 1) generate incident reports which may include information about members of the public, and 2) collect, generate, maintain, and share electronic medical records for individuals in CBP custody.

WebEOC Boards

WebEOC supports CBP's emergency management processes and functions by providing users with a variety of "boards" into which they can submit information that assists CBP in tracking incidents, medical situations, assets, and resources. A "board" is a page within WebEOC where CBP personnel can easily input information that assists CBP in creating a real-time common operating picture to perform incident management, coordination, and situation awareness functions, including the collection, maintenance, and generation of records of medical screening and treatment provided to aliens and other individuals while in short-term CBP custody.

---

[2] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 5 (2003), *available at* https://www.dhs.gov/sites/default/files/publications/Homeland%20Security%20Presidential%20Directive%205.pdf.

[3] NIMS guides all levels of government, nongovernmental organizations (NGO), and the private sector to work together to prevent, protect against, mitigate, respond to, and recover from incidents. NIMS provides stakeholders across the whole community with the shared vocabulary, systems, and processes to successfully deliver the capabilities described in the National Preparedness System. NIMS defines operational systems, including the Incident Command System (ICS), Emergency Operations Center (EOC) structures, and Multiagency Coordination Groups (MAC Groups) that guide how personnel work together during incidents. NIMS applies to all incidents, from traffic accidents to major disasters.

Most boards within WebEOC are limited to either non-privacy sensitive information (such as asset management or facilities information) or to the basic CBP employee and contractor contact information populated from the CBP Active Directory. All users require a valid CBP email address to create an account in WebEOC. Additional information collected in optional data fields in the board may include work location, work department, office phone number, mobile (personal or work) phone number, supervisor name, and supervisor contact information.

Boards within WebEOC are permission-based and only accessible to those users who require access to perform their job. WebEOC users are granted access to boards based on their need to know, and access must be approved by their respective office or component supervisor. For example, the Office of Professional Responsibility (OPR) Field Reporting System board was designed specifically for OPR's Investigative Operations Division (IOD) to submit incident reports. Only those specific IOD users have access to this board within the system.

WebEOC creates boards for the following types of use cases:

1. *Significant Incidents and Events*. CBP uses WebEOC to manage and prioritize all incidents and significant events within any given incident. When a WebEOC incident is created in the system, such as a Hurricane or National Special Security Event, this board is used to capture the most pertinent information and actions taken prior to and during the incident. CBP also uses WebEOC to review publicly available information and real-time news reports regarding a specific incident.
2. *Personnel Deployment Tracking and Supply Management*. CBP IICC uses WebEOC to track and account for all CBP personnel working in support of an incident or significant event, including pre-trained, staging, pre-deployed, deployed, and demobilized personnel.
3. *Asset Management and Facilities Readiness*. IICC uses WebEOC for visibility of the operational status of all Office of Facilities and Asset Management (OFAM) buildings and facilities CBP-wide and includes reports of outages and deficiencies to minimize the impact to CBP operations.
4. *Incident Action Plans (IAP)*. IICC uses WebEOC to generate IAPs based on CBP senior leadership expectations during an incident. An IAP is a written plan that defines the incident objectives and reflects the tactics necessary to manage the incident. IAPs communicate expectations and provide clear guidance to those managing the incident.
5. *Infectious Disease Trends*. Using aggregated publicly available information that does not contain personally identifiable information (PII), CBP IICC uses WebEOC to provide situational awareness regarding aggregate current cases and trends of infectious diseases across the country. These boards are for awareness only and display live

geographic information systems (GIS) data from multiple public data sources that is refreshed hourly. Data from these public sources is not available to any other board within WebEOC.

6. *Task Tracking and Document Repository*. CBP uses several WebEOC boards to manage internal workflows and track operations tasks, requests for assistance, requests for information, and other work products.
7. *OPR Personnel Deployment, Vehicle Tracking, and Itinerary Management*. CBP OPR IOD uses WebEOC to manage OPR personnel who are currently available or on assignment.
8. *Electronic Medical Records*.[4] The WebEOC EMR board allows authorized CBP users to create a single medical record, to include medical information collected during intake and processing, medical assessments, and medical encounters, as well as medical monitoring and medication administration or treatment for individuals while in CBP custody.

A comprehensive list of WebEOC boards, including use cases and data elements, is found in Appendix A and Appendix B of this PIA.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

CBP collects information which may be subject to further analysis in support of agency activities based on numerous authorities, including Title II of the Homeland Security Act of 2002 (Pub. L. 107-296), as amended by the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108-458, 118 Stat. 3638); the Tariff Act of 1930, as amended; the Immigration and Nationality Act ("INA"), codified at 8 U.S.C. § 1101, et seq.; the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. 110-53); the Antiterrorism and Effective Death Penalty Act of 1996 (Pub. L. 104-132, 110 Stat. 1214); SAFE Port Act of 2006 (Pub. L. 109-347); Aviation and Transportation Security Act of 2001 (Pub. L. 107-71); and 6 U.S.C. § 202.

The legal authorities for CBP's collection, use, maintenance, and dissemination of information within WebEOC boards will vary based on the purpose of the collection.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

CBP uses WebEOC for a variety of use cases. Generally, the records within WebEOC are

[4] CBP will publish a full programmatic PIA describing the Electronic Medical Records program in 2021.

collected for incident and significant event tracking, asset management, OPR case management and investigatory inquiries, and custodial medical records and health assessments.

The collection of medical information about individuals in CBP custody in the WebEOC EMR board is covered by the DHS/CBP-023 Border Patrol Enforcement Records (BPER)[5] and DHS/CBP-011 U.S. Customs and Border Protection TECS[6] system of records notices (SORN). To provide additional transparency and develop an information sharing framework for these records, CBP will publish a forthcoming Custodial Medical Records SORN.

The collection of information concerning internal affairs, specifically internal integrity or disciplinary inquiries, as well as internal reviews, inspections, or investigations conducted by CBP OPR is covered by the DHS/ALL-020 Department of Homeland Security Internal Affairs[7] SORN.

User information used to access IT resources, such as WebEOC, is covered by the DHS/ALL-004 General Information Technology Access Account Records System (GITAARS)[8] SORN.

DHS's collection and maintenance of records concerning DHS personnel for workforce accountability is covered by the DHS/ALL-014 Department of Homeland Security Personnel Contact Information[9] SORN.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

SMS, which includes WebEOC, was granted Authority to Operate (ATO) on September 11, 2019 and was previously approved for ongoing authorization. The original ATO did not permit the SMS system to include sensitive PII such as medical records or health assessments. As such, SMS has been removed from ongoing authorization, and the Office of the Chief Information Officer granted an Authority to Test (ATT) on September 11, 2020, which is valid for six months until a new ATO is completed, pending completion of this PIA.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

[5] *See* DHS/CBP-023 Border Patrol Enforcement Records (BPER), 81 Fed. Reg. 72601 (October 20, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.
[6] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 Fed. Reg. 77778 (December 19, 2008), *available at* https://www.dhs.gov/system-records-notices-sorns.
[7] *See* DHS/ALL-020 Department of Homeland Security Internal Affairs, 79 Fed. Reg. 23361 (April 28, 2014), *available at* https://www.dhs.gov/system-records-notices-sorns.
[8] *See* DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 Fed. Reg. 70792 (November 27, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.
[9] *See* DHS/ALL-014 Department of Homeland Security Personnel Contact Information, 83 Fed. Reg. 11780 (March 16, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.

As boards are developed, the CBP WebEOC Team and responsible program office will work with the CBP Records and Information Management office to identify, and if needed, produce an approved records retention schedule (or schedules) for all information collected and retained in WebEOC, including electronic medical records.

Most of the information included in WebEOC follows the DHS records schedule for situational awareness reports (Disposition Authority Number DAA-0563-2013-0002-0001): Records regarding information on emerging or potential significant incidents or events with possible operational consequences to offices or citizens must be retained for six years. These include reports and updates which outline the real or perceived dangers to areas affected by disaster(s); or which are used to identify, detect, and assess actual and potential vulnerabilities and threats to the homeland. These records may include records pertaining to law enforcement activities. However, incidents of National Significance will be included in the Secretary's Briefing Book(s), and are retained according to N1-563-07-013, Item 2.

To the extent WebEOC boards collect information on incidents that give rise to an investigation or enforcement action, CBP will retain investigative, inspection, and allegation-related files for five years after the related case is closed.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information collected and stored in WebEOC is not covered by the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The WebEOC boards collect, use, disseminate, and maintain information from CBP employees, contractors, and members of the public. The Appendices maintain a complete list of data elements collected and maintained by each WebEOC board. However, examples of information collected and maintained within WebEOC include:

- Availability of assets and supplies, including personal protective equipment;
- Presence of infectious diseases that could spread with extreme rapidity, threatening the health and life safety of the CBP personnel and surrounding community;
- Live GIS data from multiple commercially available and public data sources;

- Personnel accountability and availability for staffing or deployment purposes;
- Biographic information on CBP personnel; and
- Medical records and health interviews and assessments for individuals in CBP custody.

Most boards within WebEOC are limited to either non-privacy sensitive information (such as asset management or facilities information) or to the basic CBP employee and contractor contact information populated from the CBP Active Directory. All boards within WebEOC are permission-based and only accessible to those users who require access to perform their job.

2.2 What are the sources of the information and how is the information collected for the project?

Most information in WebEOC is manually entered by CBP personnel. Several boards have a direct ingest from publicly available data sources for mapping and geospatial data. Given the incident management, coordination, situational awareness, investigation, and operational response functions of the system, users of the WebEOC boards may use publicly available data and media websites to obtain and assess information from relevant sources that may have an immediate impact on CBP operations. CBP personnel may collect statements from witnesses, victims, and other CBP personnel while generating an incident report.

CBP contract medical providers collect health information in the WebEOC EMR board during their interaction with individuals in CBP custody. Medical information may also include prescriptions or follow-up instructions from external medical providers (such as a hospital). The WebEOC EMR board is populated with individual medical records and health assessments, and the board will also interface with a web service from the Unified Immigration Portal (UIP)[10] to import subject biographic information and link a subject's medical information with an enforcement event.

The WebEOC Infectious Disease Community Impact Tracking board displays live GIS data from multiple public data sources.[11] Data from these public sources is not available to any other board within WebEOC; and these sources do not include PII.

2.3 Does the project use information from commercial sources or

[10] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR CBP ENTERPRISE ANALYTICS (CBP EA), DHS/CBP/PIA-063 (2020), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection. Additionally, a UIP-specific PIA is forthcoming.

[11] Publicly available information sources may include the World Health Organization (WHO), Centers for Disease Control and Prevention (CDC), European Centre for Disease Prevention and Control (ECDC), 1point3acres, Worldometers.info, BreakingNewsOn (BNO), state and national government health departments, and local media reports aggregated by Johns Hopkins University.

publicly available data? If so, explain why and how this information is used.

Yes. Some WebEOC boards may use publicly available data including information obtained from the internet, news feeds, or other federal, state, local, or tribal sources to monitor events and incidents that could impact CBP operations. There exists only a unidirectional connection with the commercial and public sources and no functionality within the system to transmit information back to the original source. Commercially available information includes geographic information from Environmental Systems Research Institute (ESRI) to populate WebEOC mapping functionality with live GIS data.

Publicly available data may also be captured in the WebEOC system as an attachment. This data could include state reports/executive orders, weather service forecasts, national hurricane center reports, and county and state emergency management or public safety office reports.

Uses of publicly available information are specific to the individual WebEOC board. Any sources used outside those types listed above, such as social media, are called out in the specific board entry in the appendices of this PIA.

2.4 Discuss how accuracy of the data is ensured.

Most records are manually created by WebEOC users. Therefore, record accuracy is dependent on the user entering the information. While most boards do not contain PII, if a user has the access and permission level to view and edit information in a board, the user may address any data inaccuracies. Some boards within the system also have to undergo supervisory approval to input data, such as the OPR boards.

For Electronic Medical Records, CBP employees or contractors collect information directly from the individual during the intake and interview process. In addition, the WebEOC EMR board will interface with UIP[12] and the Enforcement Integrated Database (EID)[13] to query and ingest subject biographic information to ensure data accuracy from the enforcement systems. The WebEOC EMR board will ingest subject biographic information and link the individual's medical information with the enforcement event. CBP supervising contract medical providers regularly perform chart reviews of medical records to ensure that the information is accurate. The CBP medical advisor also performs medical quality assurance spot checks to help identify any errors and ensure that medical records are complete. In the event that the individual in CBP custody

[12] *See supra* note 11.
[13] See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID), DHS/ICE/PIA-015 (2010 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-ice, and DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 Fed. Reg. 72080 (October 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

is transferred from one CBP facility with CBP contract medical providers to another CBP facility with CBP contract medical providers, the information collected in the WebEOC EMR board is visible to the new CBP facility and its contract medical personnel.

To every extent possible, the WebEOC fields are prepopulated data fields, and dropdown lists, check boxes, and radio buttons are used to help avoid inaccurate submissions. Each WebEOC board uses system-generated record numbers, data point filters, and a search feature to locate the appropriate record and avoid the duplication of information. In addition, spell check is automatically applied to every free text data field within the system. Through programming languages, some data fields that require only numbers such as file or case numbers will not accept letters.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that WebEOC boards may contain inaccurate information based on manual data entry.

Mitigation: This risk is partially mitigated. Despite the manual data entry, WebEOC has controls built into the system to ensure data accuracy, such as required fields to certify completeness of records and format controls. Required fields include identifying information, such as first and last name and work address. Some fields require the data to be provided in an appropriate format to reduce errors, including date fields, time fields, and employee look-up fields.

Information in the WebEOC EMR board is also collected directly from the individual to ensure data accuracy. Where possible, the WebEOC EMR board includes EID[14] generated unique identifiers in order to ensure alignment with any corresponding CBP enforcement system subject records, prevent duplication of data, and ensure data integrity. In addition to these system controls, access to each WebEOC board is limited to personnel that are properly trained in the specific rules related to the board and have the appropriate need to know.

Privacy Risk: There is a risk that electronic medical information is associated with the wrong individual.

Mitigation: This risk is mitigated. Where possible and to ensure medical information is associated with the correct individual, the WebEOC EMR board uses unique identifiers generated, collected, and retained in EID. Using a UIP web service to the Enterprise Management Information System-Enterprise Data Warehouse (EMIS-EDW),[15] the WebEOC EMR board will access these

[14] *See supra* note 13.
[15] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ASSESSMENT FOR THE ENTERPRISE MANAGEMENT

unique identifiers and the associated biographic information collected via CBP enforcement systems. This interface will help to prevent the duplication of data and ensure data integrity.

In addition, individuals in CBP custody may meet with a qualified CBP contract medical provider who completes the medical assessment. Unless the individual is unconscious or unable to provide his or her own medical information, individuals are interviewed by the CBP contract medical provider and asked to provide all health information including information about their medical history, allergies, special needs, and medications.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The information collected in WebEOC supports CBP incident management, coordination, and situational awareness. CBP uses the WebEOC to coordinate the deployment of resources and assets and to secure CBP facilities and prepare CBP personnel in advance of a known incident. WebEOC supports incident management exercises and simulations to test CBP's current response capabilities. CBP uses WebEOC to facilitate communication, share information, and coordinate operations between CBP and other DHS components, other federal, state, and local agencies.

For example, CBP OPR IOD uses WebEOC when conducting investigations into CBP personnel misconduct. In addition, CBP uses WebEOC boards to manage certain internal operations, such as the tracking of infectious diseases in the workplace, workplace violence, local emergencies, and Continuity of Operations Plan (COOP) activities and exercises.

CBP also uses the WebEOC EMR board to collect medical information for individuals in CBP custody. CBP uses the WebEOC EMR board to record medical information collected during intake and processing, medical assessments, and medical encounters, as well as medical monitoring and medication administration or treatment for individuals while in CBP custody.

See Appendix A and Appendix B for how and why each board uses the information.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities

INFORMATION SYSTEM-ENTERPRISE DATA WAREHOUSE, DHS/CBP/PIA-034 (2016), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

within the system?

No. WebEOC boards are currently available to authorized CBP personnel only.

Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: Given the disparate and varied uses of information within WebEOC, there is a risk that information within WebEOC may be used for a purpose inconsistent with original collection.

Mitigation: This risk is mitigated. WebEOC employs strict access controls and restricts access to each specific WebEOC board to CBP personnel who have need to know and receive supervisory approval. Access to one WebEOC board does not grant access to any other board. The WebEOC system uses roles to determine what information the user may view, add, or edit. Additionally, each board undergoes a privacy review to determine its compliance with the information collected and how that information is used.

Privacy Risk: There is a risk that CBP personnel may not use WebEOC information in accordance with the uses described above.

Mitigation: This risk is mitigated. All WebEOC users receive training on how to use WebEOC and the board(s) they can access. Most training is hands-on with an experienced WebEOC subject matter expert who provides instruction on how to use the WebEOC board. CBP also offers users the opportunity to participate in remote training. All WebEOC users are required to pass a single-scope background investigation before being granted access to any CBP system. Access is restricted to WebEOC boards needed perform their official duties. An audit log tracks all system activity, including the user, the date and time of action, and what action was performed. WebEOC system administrators also have the ability to view the date and time a user signs in and out of the system and the board(s) he or she accessed during the login session. Users are required to take DHS security and privacy training annually.

Privacy Risk: There is a risk that a subject's medical information could be used for a purpose beyond determining and providing medical care.

Mitigation: This risk is mitigated. Access to the WebEOC EMR board is limited to authorized CBP employees and contract medical providers tasked with the care of individuals in CBP custody. CBP will only share health information with external entities (i.e., contract medical personnel, a local hospital or other health facility, or other government agency as part of a custodial transfer) who need the information in order to provide further care to the individual. This sharing of medical information is recorded on Medical Summary Form (CBP Form 2501), which is generated and maintained in the WebEOC EMR board.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

CBP employees or contractors that use WebEOC are able to see their own contact information populating from the CBP Active Directory as part of their user profile, and they upload their own information manually into the software as part of an event or incident report as required.

CBP OPR personnel may collect information directly from the public during their investigation. While explicit notice is not provided to the individual, the exchange of information is part of the investigative process and consent is implied.

Medical information and health assessment information is collected based on both the observations of CBP employees or medical personnel and the direct responses from the individual in CBP custody. CBP employees and contract medical providers enter information in the WebEOC EMR board during this intake process. The CBP employee or contract medical provider enters observations and subject medical and health information in the WebEOC EMR board as part of the initial health questionnaire. Individuals in CBP custody are free to decline to share their medical information. If an individual chooses not to provide any health information, the CBP contract medical provider will note that fact in the individual's medical record.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Opportunities for consent or opt-out vary based on the purpose for the collection. For most PII within WebEOC, the information is either: a) collected directly from a CBP employee or contractor as part of their business contact information; b) publicly available and included as part of an incident report for situational awareness; c) part of an internal affairs investigation; or d) collected directly from a subject in custody as part of a medical assessment.

An individual or witness involved in a CBP internal affairs investigation can decline to speak with the CBP agent or officer conducting the investigation. An individual being interviewed by CBP personnel may refuse to provide their contact information to CBP. However, during the course of a normal investigative procedure, some PII may still be collected such as a license plate number if the investigation was part of a motor vehicle accident, for example. Additionally, CBP receives police reports, which may include PII for individuals involved in the incident or investigation.

Individuals in CBP custody have the right to refuse to share medical information with the CBP contract medical provider during the intake screening and any subsequent meetings with

medical personnel. When individuals refuse to provide medical information, the CBP contract medical provider will orally advise the individual that the lack of information could negatively impact the health or the medical care they receive and their refusal to provide the information will be documented.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals are not aware their information is stored in WebEOC.

Mitigation: This risk is partially mitigated. When appropriate, CBP provides notice at the time of collection from individuals and employees. Regardless of the law enforcement or border security reasons for the information collection, CBP has published SORNs for all information types, available at https://www.dhs.gov/system-records-notices-sorns.

Regarding information collected from publicly available sources, WebEOC uses publicly available information for situational awareness purposes and aside from individuals identified in news reports, this information does not contain PII.

Regarding medical information, individuals in CBP custody will provide their information (including any symptoms or known diagnoses) to either a CBP contract medical provider or a CBP employee during intake. If applicable, individuals in CBP custody also provide their medical information directly to a CBP contract medical provider who completes the medical assessment. Unless the individual is unconscious or unable to provide their own medical information, individuals are interviewed by a CBP contract medical provider and asked to provide all health information, including information about their medical history, allergies, special needs, and medications.

Section 5.0 Data Retention by the Project

5.1 Explain how long and for what reason the information is retained.

As boards are developed, the CBP WebEOC Team and responsible program office will work with the CBP Records and Information Management office to identify, and if needed, produce an approved records retention schedule for all information collected and retained in WebEOC.

Some boards may already have records retention schedules established. For example, the OPR Field Reporting System board collects information on incidents involving CBP personnel; however, the information collection may include data for members of the public, other DHS employees, and other federal employees involved in the reported incident. CBP will retain investigative, inspection, and allegation-related files for five years after the related case is closed.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is the risk that PII may be retained in the system for a longer period than is necessary for the purpose for which the information was collected.

Mitigation: This risk mitigation is in progress. CBP is actively working with the CBP Records and Information Management team to identify and apply the appropriate records retention schedule to ensure that WebEOC records are destroyed in a timely manner. At the time of the publication of this PIA, CBP has not deleted any records from WebEOC, but will begin to align WebEOC records as the records retention schedules are identified and approved by NARA.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

With the exception of the WebEOC EMR board, information within WebEOC is not disclosed outside of CBP.

As part of the normal operations, CBP shares medical information collected via the WebEOC EMR board. This medical information may be shared outside of DHS with the following:

- Outside medical providers: This includes local hospitals or medical specialists who treat individuals when CBP cannot provide the necessary treatment. CBP provides the outside medical provider with limited information about the individual including first/last name, Alien File Number (A-Number), date of birth, nationality, and gender, along with a copy of any collected medical information relevant to the treatment. CBP will use the Medical Summary Form (CBP Form 2501) to share this information with the with third party medical providers.
- Local community or foreign government medical professionals: If an individual in CBP custody is released from CBP custody or removed from the United States, the CBP contract medical provider at the facility from which the individual is leaving will prepare a Medical Summary Form (CBP Form 2501). The form lists the individual's name, A-Number, date of birth, nationality, gender, and a summary of the individual's medical information to help ensure continuity of care. When an individual carries a contagious disease that could affect the general public (e.g., tuberculosis), the Medical Summary Form (CBP Form 2501) is shared with the host country in order to enable the host country to protect the general public.

- ICE Health Services Corps (IHSC)[16] and ICE contracted medical personnel: When CBP transfers custody of an individual to ICE, CBP discloses the individual's pertinent medical information for the purposes of maintaining continuity of care. This information is transferred using the Medical Summary Form (CBP Form 2501). The form is provided via an emailed file that is appropriately password encrypted in adherence with DHS protocols for sending sensitive PII. A hard copy may also be provided in a sealed envelope with the individual.
- HHS Office of Refugee Resettlement (ORR) and HHS Public Health Services Corps (PHSC)[17] workers: When CBP transfers custody of unaccompanied alien children (UAC) to HHS ORR custody, CBP will disclose the individual's pertinent medical information to HHS ORR. To ensure continuity of care, the Medical Summary Form (CBP Form 2501) will be provided to HHS ORR in a sealed envelope. Upon transfer of the UAC, HHS PHSC would be responsible for ensuring continuity of care.
- Other law enforcement agencies: CBP occasionally transfers custody of an individuals to another law enforcement agency. To ensure continuity of care, the Medical Summary Form (CBP Form 2501) will be provided to the law enforcement agency taking custody of the individual.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Only the WebEOC EMR board will share information external to CBP. The sharing of this information with the entities outlined in Section 6.1 is covered by the DHS/CBP-023 Border Patrol Enforcement Records (BPER)[18] and DHS/CBP-011 U.S. Customs and Border Protection TECS[19] SORNs. While both of these SORNs permit disclosure of information outside of CBP, CBP is in the process of drafting a new Custodial Medical Records system of records to explicitly cover this information.

For medical information collected by the CBP Office of Field Operations (OFO) and maintained under the TECS SORN, CBP may disclose information to contract medical providers and hospitals under contract with CBP pursuant to Routine Use F: "To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS or CBP, when necessary to accomplish an

[16] The ICE Health Services Corps provides health evaluations, treatment, and services to individuals in ICE custody and held in detention facilities across the country.
[17] The HHS Public Health Services Corps may provide continued medical treatment and services to individuals transferred to ORR's custody. PHSC maintains HHS' highly qualified public health professionals.
[18] *See supra* note 5.
[19] *See supra* note 6.

agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS/CBP officers and employees." CBP may disclose medical information to ICE consistent with 5 U.S.C. 552a(b)(1) and to HHS pursuant to Routine Use G: "To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, or treaty where DHS determines that the information would assist in the enforcement of civil or criminal laws."

For medical information collected by U.S. Border Patrol (USBP) and maintained under the BPER SORN, CBP may disclose information to contact medical providers and hospitals under the contract with CBP pursuant to the same Routine Use F noted above. CBP may disclose medical information to ICE consistent with 5 U.S.C. 552a(b)(1) to and HHS pursuant to Routine Use P. "To federal, state, local, territorial, tribal, and foreign law enforcement or custodial agencies for the purpose of placing an immigration detainer on an individual in that agency's custody, or to facilitate the transfer of custody of an individual from CBP to the other agency. This will include the transfer of information about unaccompanied minor children to the U.S. Department of Health and Human Services (HHS), Office of Refugee Resettlement (ORR), to facilitate the custodial transfer of such children from CBP to HHS."

To the extent other information may be disclosed outside of WebEOC, additional routine uses govern the sharing parameters. Sharing of business contact information used to access IT resources, such as WebEOC, is covered by the GITAARS[20] SORN. Sharing of DHS personnel information related to incident responses is covered by the DHS Personnel Contact Information[21] SORN.

6.3 Does the project place limitations on re-dissemination?

Any information disclosed from WebEOC is shared in a manner consistent with the applicable SORN covering those records. Generally, CBP does not externally disclose information from WebEOC; however, as part of the Electronic Medical Records program, CBP does share information to ensure that individuals in CBP custody receive medical treatment and continuity of care following transfer, and to ensure the receiving government or organization is aware of any public health risks. When sharing with outside medical providers, these providers are covered by the Health Information Privacy and Portability Act (HIPAA) and are limited in the dissemination of data without prior authorization from the individual.

6.4 Describe how the project maintains a record of any disclosures

[20] *See supra* note 8.
[21] *See supra* note 9.

outside of the Department.

Disclosure of medical information is recorded on Medical Summary Form (CBP Form 2501), which is generated and maintained in the WebEOC EMR board. Notes about the treatment, such as when it occurred, and results are also maintained. The information disclosures outside of DHS for all other WebEOC boards must be accounted for in a paper or electronic record that includes the date, nature and purpose of each disclosure, and the name and address of the individual agency to which disclosure is made.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the individual's medical information shared outside of CBP may not be handled appropriately by the entity receiving the information.

Mitigation: This is risk is mitigated. CBP implements a rigorous approval process for sharing information with external entities. A Memorandum of Understanding (MOU) or an Interagency Service Agreement (ISA) is completed between the two entities (i.e., CBP and the external entity) outlining strict guidelines for how the information should be handled. In the event of a request for information or ad hoc information disclosure, CBP has robust internal procedures governing the disclosure of information to external entities.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

An individual may request information about his or her records stored by WebEOC through DHS procedures at Part 5, Title 6 of the Code of Federal Regulations implemented pursuant to the Freedom of Information Act (FOIA) (5 U.S.C. § 552) and the Privacy Act of 1974 (5 U.S.C. § 552a(d)). Privacy Act access rights are limited though to individuals that are U.S. citizens or aliens lawfully admitted for permanent residence (legal permanent residents, also known as LPRs).

Procedures for individuals to request access to their information, which may have been collected or maintained in WebEOC or in another CBP system, are identified in the cited SORN(s). Requests for access to the information contained in a request for information can be made to CBP's FOIA Office via FOIA online or by mailing a request to:

U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) Division
1300 Pennsylvania Avenue NW, Room 3.3D
Washington, D.C. 20229

When seeking records from WebEOC or any other CBP system of records, the request must

conform to Part 5, Title 6 of the Code of Federal Regulations. An individual must provide his or her full name, current address, and date and place of birth. He or she must also provide:

- An explanation of why the individual believes DHS would have information on him or her;
- Details outlining when her or she believes the records would have been created;
- And if the request is seeking records pertaining to another living individual, it must include a statement from that individual certifying his/her agreement for access to his/her records.

The request must include a notarized signature or be submitted pursuant to 28 U.S.C. § 1746, which permits statements to be made under penalty of perjury as a substitute for notarization. Without this information, CBP may not be able to conduct an effective search and the request may be denied due to lack of specificity or lack of compliance with applicable regulations. Although CBP does not require a specific form, guidance for filing a request for information is available on the DHS website at http://www.dhs.gov/file-privacy-act-request and at http://www.dhs.gov/file-foia-overview.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals who are U.S. citizens or LPRs who wish to correct inaccurate information may submit a Privacy Act Amendment request through the same access process explained in Section 7.1.

7.3 How does the project notify individuals about the procedures for correcting their information?

This PIA and the associated SORNs provide notice of FOIA and Privacy Act procedures to request access to or correction of an individual's records.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals are not aware of their ability to make record access requests for records in WebEOC.

Mitigation: This risk is mitigated. As with any records maintained by CBP, individuals are encouraged to file a request for access, correction, or amendment should they believe CBP maintains incorrect information. CBP provides broad redress opportunities where appropriate and to the extent possible regarding law enforcement sensitive information. Individuals who believe CBP has any records related to them can file a request per the procedures above. For individuals who are not subject to the redress provisions of the Privacy Act, CBP reviews and resolves all

requests for redress on a case-by-case basis.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

User access to the information in WebEOC is authenticated via CBP Active Directory. Access control is role-based, and data is restricted and will only be accessible if a specific user has a "need to know," has been approved for access to the data, and has met all training requirements. Periodic reviews are conducted on the application of user roles, and further administrative actions, such as granting access, removing access, or altering roles for those who already have access, are conducted.

All WebEOC boards perform some level of auditing. WebEOC logs display all notes in chronological order with the oldest on top, and users are not permitted to delete or edit these notes. If a CBP contract medical provider makes a mistake with a note or needs to correct something that is inaccurate in the WebEOC EMR board, the CBP contract medical provider must make the correction by adding an amended note to the notes log. Each note is marked with the name of the user who created the entry and/or amended it as well as the time and date when note was created and/or amended. This feature helps to ensure the integrity of the information that is in the notes of individual records.

The WebEOC EMR board does not permit users to delete entries. In order to correct an incorrect entry, the CBP contract medical provider must notate the error in the record found to be inaccurate before creating a new record with the corrected information.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All CBP personnel must take annual privacy and security training and review and sign the DHS Rules of Behavior. In addition, CBP personnel take specific WebEOC training as part of an introduction to the system, which explains the system structure, information retention, user permissions, and roles.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

The following procedures are in place to ensure that access to information in WebEOC is limited to authorized CBP personnel:

- Access to WebEOC requires a CBP Active Directory account and requires the user to log into a CBP Intranet-accessible computer;[22]
- A system access request must be completed, signed, and approved by the requester and requester's supervisor prior to the creation or distribution of personnel security data, to avoid accidental, inappropriate, or unauthorized use of the data;
- WebEOC user accounts are individually approved by a WebEOC Administrator before they are provisioned; and
- Access to information is role-based and granted based on a "need to know;" users have access to a limited subset of data based on the concept of least privilege/limited access.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All MOUs are reviewed by the respective program manager, the CBP Privacy Officer, and the Office of Chief Counsel before being sent to DHS for formal review.

Contact Official

Bradford Slutsky
Director
Information and Incident Coordination Center
Office of Operations Support
U.S. Customs and Border Protection

Responsible Official

Debra L. Danisek
Privacy Officer
Privacy and Diversity Office
Office of the Commissioner
U.S. Customs and Border Protection
(202) 344-1610

Approval Signature

[22] Requirements for obtaining access to CBP Information Technology Systems are documented in CBP Handbook, HB 1400-05D, "Information Systems Security Policies and Procedures Handbook," version 6.01, dated May 17, 2016.

[Original signed copy complete and on file with the DHS Privacy Office]

_____

Dena Kozanas
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

Appendix A: WebEOC Boards

CBP Employee & Contractor Information Only

Last Updated: October 30, 2020

Most boards within WebEOC are limited to either non-privacy sensitive information (such as asset management or facilities information) or basic CBP employee and contractor contact information populated from the CBP Active Directory. All users require a valid CBP email address to create an account in WebEOC. Additional information collected incidentally in optional data fields in these types of boards may include work location, work department, office phone number, mobile (personal or work) phone number, supervisor name, and supervisor contact information. No other PII is collected or retained in these boards.

1. Asset Management Board

The WebEOC Asset Management Board used by the CBP IICC was created as one of the core WebEOC boards and used across CBP for incident response. The Board allows for the recording, tracking, and justification for the deployment of logistics and assets, including air, maritime, land, and team asset deployments.

CBP Offices (e.g., Ports of Entry, Offices, and/or Emergency Operations Centers) use the Asset Management Board to enter, locate, and obtain assets during an incident. As an incident-independent board, all WebEOC users have access to the Asset Management Board and have the capability to enter assets as a means to track those items and make available to other users.

This board does not include PII beyond basic user contact information.

2. Battle Rhythm Board

The CBP IICC uses the Battle Rhythm Board to create incident information logs in WebEOC using an electronic form that captures the following information: event details, the name of the person who entered the data, date, time, and a field for graphics (e.g., hurricane tracking maps). The board provides a summary of all upcoming and reoccurring scheduled meetings and coordinated events. This board is incident-dependent and requires users to manually enter the meeting information. Any user with access to the incident has permission to view, edit, and/or participate in the meetings.

This board does not include PII beyond basic user contact information.

3. Deployment Tracking Board

The CBP IICC uses the Deployment Tracking Board to track and account for all CBP personnel working in support of an incident or significant event, including pre-trained, staging, pre-deployed, deployed, and demobilized personnel. The board is incident-dependent and a new entry is recorded each time an individual or a group of individuals is set to deploy to a region in support of an incident or significant event.

The information collection does not include PII.

4. Document Library

The CBP IICC uses the WebEOC Document Library across CBP offices and components as a repository for IICC documents and files and provides users a common repository that memorializes any type of file for tracking, archival, and potential auditing purposes. The Document Library can support any file type including images, emails, documents, and videos. The board may be used for daily operations or to archive and store documents pertaining to a specific incident or event. The Document Library is incident-dependent, meaning that any users who have access to the incident can upload documents and access the information.

This board does not include PII beyond basic user contact information.

5. Field Reporting

The CBP IICC uses the WebEOC Field Reporting Board to provide visibility of the operational status of all Office of Facilities and Asset Management (OFAM) buildings and facilities CBP-wide and includes reports of outages and deficiencies to minimize the impact to CBP operations. Designated CBP personnel located at each facility manually report the information in the board, which quickly displays the current operational status of the CBP facility: green to indicate Operational Normal, orange to indicate Partially Operational, and red to indicate Not Operational.

This board does not include PII beyond basic user contact information.

6. Incident Action Plan (IAP) Builder

The IAP Builder is the vehicle used by CBP senior leaders of an incident to communicate their expectations and provide clear guidance to those managing the incident. An IAP is a written plan that defines the incident objectives and reflects the tactics necessary to manage the incident. The CBP Management Branch uses the IAP Builder to compile and consolidate all Incident Command System (ICS) Forms into one concise board, allowing for a more fluid process in IAP reporting. ICS Forms were previously within WebEOC in an individual format, requiring the user to go into each specific ICS form, complete the form, and locate the next ICS form. The IAP Builder enables the user to select all relevant ICS forms necessary, at the point in which the IAP is created. All WebEOC users with access to the corresponding incident may view the IAP.

Information entered into the ICS forms will include the name and telephone numbers of CBP personnel generating the IAP and those CBP personnel assigned to manage the incident. The incident details are available to users while the incident remains active and become unavailable when the incident becomes inactive.

This board does not include PII beyond basic user contact information.

7. CBP Incident Personnel Board and CBP Supply Tracker Board

All CBP components use the CBP Incident Personnel and CBP Supply Tracker Boards to track personnel assigned to a specific incident and the availability of supplies, consumables, and personal protective equipment (PPE).

The CBP Incident Personnel Board tracks CBP personnel assisting in a specific incident. This board allows for all CBP personnel assisting in the incident to sign in or sign out, indicating their availability throughout that work day/shift. The board captures the user's WebEOC role, name, contact phone number, location (whether remote or on-site), organization, email address, and date. This board is incident-dependent, which means that users will only see CBP personnel who signed in to the CBP Incident Personnel Board for that specific incident.

The Supply Tracker Board tracks all supplies, consumables, and PPE available to each incident. The Supply Tracker Board is also incident-dependent, tracking all supplies, consumables and PPE that have been ordered, checked out, and assigned to the incident. Users may add a specific type of supply, consumable, or PPE as needed. CBP personnel can view all supplies, consumables, and PPE on hand for their location.

This board does not include PII beyond basic user contact information.

8. Infectious Disease Case Summary Board

The CBP IICC uses the Infectious Disease Case Summary Board as a tool for CBP to track aggregate data during real-time information for an outbreak of an infectious disease, such as COVID-19, and the number of personnel affected within CBP facilities. The board will track aggregate data providing CBP with situational awareness to help determine the impact of the infectious disease on CBP operations. After a CBP employee or contractor reports the known or suspected exposure to an infectious disease (e.g., COVID-19), the responsible CBP supervisor manually enters and tracks the status and impact of the incidents in the board. No PII about individuals who have tested positive for an infectious disease is collected or maintained in the board; rather, the number of cases in each stage is recorded.

The Infectious Disease Case Summary Board tracks the following information per entry:

- Jurisdiction (CBP facility);
- Number of Presumptive Cases;
- Number of Confirmed Cases;
- Number of Fatalities;
- Number of Recovered Personnel;
- Number of Personnel in Mandatory Quarantine;
- Number of Personnel in Voluntary Quarantine;
- Number of Personnel Hospitalized;
- Number of Personnel Released from Quarantine; and
- Total Number of Personnel.

This board does not include PII beyond basic user contact information of the CBP supervisor who created the incident.

9. Infectious Disease Community Impact Tracking

The CBP IICC uses the CBP Infectious Disease Community Impact Tracking Board to closely monitor and visually display real-time data related to COVID-19 and other infectious diseases to assist CBP personnel tracking the pandemic and further understand the potential impact on CBP operations. It can be used by any component or office within CBP.

Like the CBP Infectious Disease Case Summary Board, CBP uses the board to provide situational awareness regarding current cases, but across the country rather than at the facility level. The board displays live GIS data from multiple public data sources and the information is

refreshed hourly. Data from these public sources is not available to any other board within WebEOC.

The public data sources for this board include the following:

- World Health Organization (WHO);
- Centers for Disease Control and Prevention (CDC);
- European Centre for Disease Prevention and Control (ECDC);
- 1point3acres;
- Worldometers.info;
- BreakingNewsOn (BNO); and
- State and national government health departments, and local media reports aggregated by Johns Hopkins University.

No PII is collected, maintained, or generated in this board. The Infectious Disease Community Impact Tracking Board displays the following aggregate information:

- Number of cases by state (confirmed, death, tested, hospitalized);
- Number of cases by county;
- Number of confirmed cases;
- Number of deaths;
- Number of U.S. recovered individuals;
- Counties reporting cases (percentage per state);
- Number of tested individuals;
- Number of hospitalized individuals; and
- Last updated date and time.

10. PTA Tracker

The CBP IICC utilizes the WebEOC PTA Tracker board to track and record the submissions of privacy compliance documentation (to include PTAs, PIAs, and SORNs). The PTA

Tracker board is being used as means to easily view the status of all current and completed privacy compliance documentation.

This board does not include PII beyond basic user contact information.

11. Resource Request Board

The CBP Office of Field Operations (OFO), the U.S. Border Patrol (USBP), the Air and Marine Operations (AMO), the Enterprise Services (ES), and the Operations Support (OS) use CBP Resource Request Board to make the requests for action of other CBP components using the Resource Requests Board. For example, using the board, USBP may request resources from AMO. The board displays a banner directing users to enter or attach documents, which may contain PII for individuals outside of DHS employees or contractors.

This board does not include PII beyond basic user contact information. Please note that this board may contain this type of PII from individuals outside of CBP.

12. Task Tracking

The CBP IICC uses the Task Tracking Board to track all incidents and incident responses across CBP. The board tracks all operations tasks, requests for assistance, and requests for information, but will not include requests for PII. The Task Tracking Board includes an email notification feature within the board, enabling CBP personnel who are entering a task into the board to send an email notification to the CBP personnel responsible for the task.

This board does not include PII beyond basic user contact information.

13. Vehicle Tracker

The CBP Vehicle Tracker Board is used to track and account for CBP vehicles as part of daily operations or during an incident. Any CBP component may use this board as part of their processes and procedures for tracking vehicles assigned to the component. This board is incident-dependent and requires users to manually enter information.

This board does not include PII beyond basic user contact information.

14. Personnel Accountability

The CBP IICC uses the WebEOC Personnel Accountability Board to track and account for the safety and welfare of CBP personnel, as well as their status (e.g., employees okay, employees

not okay, employees not responded, employees evacuated) during a significant event (e.g., flooding, hurricane, casualty). The board allows for one attachment to be uploaded when creating a record, to provide additional insight or supporting documentation to the entry. When creating a record, no CBP employee names or PII are logged – the board is solely capturing the number of employees. Supervisors and other employees all have the ability to create, edit, view, and delete records as appropriate. Additionally, the Personnel Accountability Board has no connection to any other board or system.

This board does not include PII beyond basic user contact information.

Appendix B: WebEOC Boards
Information Collected from Members of the Public

Last Updated: October 30, 2020

1. OPR Field Reporting System

The Office of Professional Responsibility (OPR) Investigative Operations Division (IOD) uses WebEOC within its daily operations for incident reporting purposes. IOD is primarily responsible for conducting investigations into allegations of criminal and serious misconduct on the part of CBP employees and contractors. The OPR Field Reporting System board is used as the primary platform for IOD employees to capture reports regarding those investigations.

The board contains consistent data fields, which allow CBP to create a uniform report from the entries added by OPR field personnel. OPR IOD Special Agents gather information and documentation from other federal, state, and local law enforcement authorities, CBP employees, witnesses, and other sources during an investigation. The software will streamline the reporting process by providing users multiple drop-down lists for agency position, status, office, and similar categories. Upon entry into WebEOC, the report will be immediately visible to other authorized OPR IOD personnel logged into the system. The board will be accessible exclusively to OPR IOD personnel based on the permission level access controls set up in the system. OPR IOD employees and supervisors located in the same office will be able to view and contribute to each other's reports. These permissions will ensure that the information within this board is restricted to OPR personnel with a need to perform their duties.

The reports generated contain incident information about CBP employees and may also include information about members of the public. Reports contain details about each incident, including a timeline of events, description, and incident category (e.g., Fatality, Shooting, Assault, Traffic Crash, Prison Rape Elimination Act (PREA), OPR Significant Case).

Although some incidents reported may lead to a CBP employee misconduct investigation, the WebEOC OPR Field Reporting System board is not considered an extension of JICMS.[23] The information collection for each incident is not routinely entered into JICMS; however, OPR IOD

[23] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE JOINT INTEGRITY CASE MANAGEMENT SYSTEM (JICMS), DHS/CBP/PIA-044) (2017), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

will use information collected within this board to manually initiate a case in JICMS if the case warrants an investigation.

OPR captures the following data within the board:

- CBP Special Agent in Charge (SAC) Office;
- OPR Special Agent Name (reporter of information includes CBP employee name, username, and position);
- Incident Classification (Drop-Down Menu Options: Critical Incident Report, Sensitive Close Hold, Sensitive OPR Only, Daily Field Report);
- Incident Summary (including attachments, photos, relevant documentation);
- Subject Type (CBP Employee, Civilian, Non-Citizen/Undocumented Alien (UDA));
- First Name, Last Name, Middle Name;
- Position (e.g., CBP Watch Commander, CBP Officer, Border Patrol Agent);
- Enter on Duty (EOD) Date (applicable to CBP Employees Only);
- Post of Duty (POD);
- Date of Birth (DOB);
- Port of Entry (POE);
- Country of Birth/Country of Citizenship (COB/COC);
- A-Number;
- JICMS History (if applicable to the individual); this section will allow the Agent to include up to ten previous JICMS records. Each record is manually inputted by the Agent (no connection to JICMS system) and will include:
  - JICMS Case Number;
  - Case Title;
  - Status of Case;
  - Case Outcome/Disposition.
- Medical Information (if applicable), including:
  - Subject Status (Drop-Down Menu Options: Treated/Released, Non-Life-Threatening Condition, Serious Life-Threatening Condition, Deceased);

- Hospital;
- Provider of Medical Assistance;
- Medical Details;
- Medical Examiner Office;
- Autopsy Date;
- Preliminary Cause of Death; and
- Medical Examiner Cause of Death.

- Any related attachments (photos, medical information, or relevant documentation, which may include additional PII); and
- Criminal History (if applicable).

2. Significant Events

The CBP IICC uses the Significant Events board to capture all significant events within any given incident. When a WebEOC incident is created in the system, such as a Hurricane or National Special Security Event, this board is used to capture the most pertinent information and actions taken prior to and during the incident. Any CBP WebEOC user with access to the board and the associated incident has the ability to create, edit, view, and delete records. On the Display View, the header includes a Privacy disclaimer stating the following: *"Disclaimer: To protect privacy, please refrain from uploading attachments with any Personally Identifiable Information (PII) into the Significant Events Board."* WebEOC users have the ability to include up to four attachments and a brief description per record pertaining to the significant event being created. Although the information in this board is connected to specific incidents, the board does not interface with any other WebEOC board or system to send or receive information. WebEOC users manually update the board to record significant events within any given incident.

The Significant Events board displays the following information:

- Record # (automatically-generated WebEOC record number for tracking purposes);
- Updated date (date and time the record was updated);
- Initial date (date and time the record was created);
- Type (Drop-down list for the category the record most closely matches);
- Description (free text field for a full description of the event); and

- Priority (Drop-down list – low, medium, high, and flash).

The Significant Events board may collect the following PII on members of the public who are involved in the incident (e.g., witnesses, suspects):

- Name;
- Date of birth;
- Vehicle License Plate;
- Gender;
- Race;
- Age; and
- Physical description including weight, height, and clothing.

3. Twitter Board

The CBP IICC uses the WebEOC Twitter board to provide WebEOC users with situational awareness and real-time information from the public during an incident. The Twitter board may be used by any CBP office and may be adjusted to display any Twitter account or username. Currently, the only instance of the Twitter board has been configured for all CBP Headquarters WebEOC positions and displays the following four separate Twitter accounts:

- Metropolitan Police Department (@DCPoliceDept);
- CityIntel (@Cityintel1);
- District Department of Transportation (@DDOTDC); and
- U.S. Customs and Border Protection (@CBP).

The board is for display purposes only and there is no function for users to input or delete any information. The agency's messages, or tweets, contain links to other Twitter usernames or hashtags, but those Twitter links do not open due to the security controls of CBP.

4. Electronic Medical Records (EMR) Board

Once fully implemented, the WebEOC EMR board allows authorized CBP users to create a single medical record that includes medical information collected during intake and processing, medical assessments, medical encounters, as well as medical monitoring and medication administration or treatment for individuals while in CBP custody.

The WebEOC EMR board will be implemented in multiple phases. Phase 1 involves piloting and testing the WebEOC EMR board at the USBP Rio Grande Valley (RGV) Sector and Brownsville and Laredo Ports of Entry (POE). **CBP will publish a new programmatic CBP Electronic Medical Records PIA prior to beginning Phase 2.**

During Phase 1, USBP agents in the RGV Sector will leverage the Subject Identification (SID)[24] wristband pilot in RGV to establish a link between the individual's biographic information in e3[25] and his or her medical information in WebEOC EMR. This will facilitate identification of the individual for the purposes of providing follow-up medical actions. The Office of Field Operations (OFO) officers at the Brownsville and Laredo POEs will not use wristbands but instead will manually enter a system-generated unique identifier to link the individual's medical record to his or her enforcement record in Unified Secondary (USEC),[26] which is part of the CBP Automated Targeting System (ATS)[27] security boundary.

During intake and processing, CBP agents and officers collect the individual's biographic information and enter it in the CBP law enforcement system of record. During Phase 1, CBP agents and officers or contract medical practitioners will complete the Alien Initial Health Questionnaire (CBP Form 2500) during intake and processing. A positive response on CBP Form 2500 will result in a referral to the CBP contract medical staff who will initiate the medical record in the WebEOC EMR, log the medical assessment, and all follow-up medical care. During Phase 1, the responses to CBP Form 2500 will be collected and retained in the CBP law enforcement system and will not be transmitted to the WebEOC EMR board.

Using the system-generated unique identifier and a web service in UIP,[28] this biographic data will be transmitted from Enterprise Management Information System-Enterprise Data Warehouse (EMIS-EDW)[29] to the WebEOC EMR board. This biographic information will be used

---

[24] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE CBP PORTAL (E3) TO ENFORCE, DHS/CBP/PIA-012 (2017 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[25] *See supra* note 27.
[26] Historically, CBP officers have used a TECS subsystem called the Consolidated Secondary Inspection Service (CSIS) to manage referrals of travelers for secondary inspection. CSIS may transmit relevant inspection and traveler information it captured to the Secure Integrated Government Mainframe Access (SIGMA), a secondary inspection immigration event management tool and a module of the Automated Targeting System (ATS). Unified Secondary is replacing and combining functionality of CSIS and SIGMA into one comprehensive secondary inspection tool. Unified Secondary is housed within the ATS information security boundary. The Unified Secondary PIA is forthcoming.
[27] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM, DHS/CBP/PIA-006 (2007 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[28] *See supra* note 13.
[29] *See supra* note 15.

to populate the individual's profile in the WebEOC EMR board, thus reducing data redundancy and input errors:

- Individual's Name (Last, First, MI);
- Gender;
- Date of Birth/Age;
- A-Number;
- Country of Citizenship;
- Event Number; and
- Book In/Book Out dates.

At minimum, all individuals in CBP custody under the age of 18 will receive a health interview and medical assessment[30] upon intake into CBP custody. Additionally, when medically warranted, individuals of any age in CBP custody will receive a medical assessment[31] or medical encounter[32] performed by a CBP contract medical provider. The WebEOC EMR board will also track all medical monitoring or the administration of medications or treatment for individuals in CBP custody receiving such medical actions. In some circumstances, medical treatments and the administration of medications may be performed by a qualified CBP agent or officer.

When an individual is transferred from CBP custody, Medical Summary Form (CBP Form 2501) is generated. The Medical Summary Form is a summary of the individual's medical information (e.g., known conditions, issues, medications prescribed) along with individual's biographic information and facility referral information. The CBP Form 2501 may be shared with ICE, HHS ORR, or a local medical treatment facility when custody of an individual is transferred. CBP Form 2501 may be shared through hard copy, or an electronic file can be generated and attached to a password-protected email. Additionally, to help ensure continuity of care, the individual may be provided with a hardcopy of the CBP Form 2501.

The following medical information will be collected and retained in the WebEOC EMR board:

- Vital Signs (e.g., temperature, respiratory rate (RR) heart rate (HR), blood pressure (BP), provider);

[30] *See* CBP Directive No. 2210-004, on file with the CBP Privacy Office.
[31] In CBP's case, a medical assessment is a visual and physical inspection of a person in custody, usually conducted by a lower level care provider, noting deviations from the norm and a statement of the individual's mental and physical condition that can be amendable to or resolved by appropriate actions of the provider.
[32] A medical encounter is defined as an interaction between a patient and healthcare provider(s) for the purpose of providing healthcare service(s) or assessing the health status of a patient.

- Medical History (current illness/injury/health concern, past medical history, medications, allergies);
- Mental Health Evaluation (results);
- Ask/Observe (a summary of what the provider asked the individual, their responses, and any observations the provider may have);
- Physical Exam (results);
- Review of Systems (results);
- Admission/Disposition;
- Subjective Notes (current illness/injury/health, past medical history, medications);
- Objective (general, eyes, respiratory, cardiovascular (CVD), gastrointestinal (GI), extremities, skin, other);
- Additional Observations Notes;
- Plan;
- Provider's objective for how to treat the patient (diagnosis, may be multiple);
- Medication (Dosage/Frequency/Instructions/Date and Time Administered/Provider Name);
- Disposition (Medically cleared for travel/transfer/release or Referred to Local Medical Treatment Facility);
- Position (CBP agent/officer or contract medical provider); and
- CBP personnel or contract medical provider name.

The Medical Summary Form (CBP Form 2501) includes the following information:

- CBP Location;
- Medical Issues Identified;
- Medical Conditions or Exposure;
- Referred to Medical Facility (Yes/No);
- Referred to Medical Facility Description;
- Medications Prescribed;
- Medications Prescribed Follow on Description;

- Provider User Name;
- Position Name; and
- Form Submitted (Date).

The following information is collected and retained about the board user:

- Hash ID;
- Optional - Name (typically collected as part of account creation);
- Optional – Email;
- Optional - Office Phone;
- Optional - Mobile Phone;
- Optional - Supervisor Name;
- Optional - Supervisor Email; and
- Optional - Supervisor Phone.

5. Incident Response Tracking Tool Board

CBP will use the WebEOC Incident Response Tracking Tool Board to enable assigned field personnel to effectively track incident responses and operational tasks in various international locations across CBP. This board incorporates an Enterprise Geospatial Information Services (eGIS)[33] functionality to increase situational awareness and operational efficiency among field personnel. CBP's use of the board is for a multi-component response effort that can be used for any incident. Any CBP WebEOC user with access to the board and the associated incident has the ability to view the information, but a select group of individuals will be able to create, edit, and delete records. On the Display View, the header includes a Privacy disclaimer stating the following: *"Disclaimer: To protect privacy, please refrain from uploading attachments with any Personally Identifiable Information (PII) into the Incident Response Tracking Tool Board."* WebEOC users have the ability to include attachments and a brief description per record pertaining to the incident being created.

This board does not collect PII beyond basic CBP user contact information and may contain this type of PII from individuals outside of CBP.

[33] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ENTERPRISE GEOSPATIAL INFORMATION SERVICES, DHS/CBP/PIA-041 (2020), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

CBP captures the following data within the board:

- Record # (automatically-generated WebEOC record number for tracking purposes);
- NIMS/ICS defined Incident Locations and their associated Information (Street Address, City/State, Country/Region, Zip Code);
- Operational/Mobilization Status;
- General numbers of employees assigned to that specific location;
- Equipment Information;
- Onsite motor-pool numbers;
- Operational Shifts for each Location; and
- Any related attachments (including reports, rosters, equipment lists, which may include additional PII).

The following information is collected and retained about the board user:

- First Name, Last Name, Middle Name;
- Position;
- Agency/Office Name; and
- Phone Number.

The Incident Response Tracking Tool board may collect the following PII on individuals who are involved in the incident, such as other DHS Component personnel and other Federal agency personnel:

- First Name, Last Name, Middle Name;
- Position;
- Agency/Office Name;
- Phone Number;
- Email address; and
- Incident Specific Location/Address.