Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form will be used to determine whether a Privacy Impact Assessment (PIA), System of Records Notice (SORN), or other privacy compliance documentation is required under the E-Government Act of 2002, the Homeland Security Act of 2002, the Privacy Act of 1974, or DHS policy.

Please complete this form and send it to your Component Privacy Office. If you are unsure of your Component Privacy Office contact information, please visit https://www.dhs.gov/privacy-office-contacts. If you do not have a Component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
DHS Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717

PIA@hq.dhs.gov

Your Component Privacy Office will submit the PTA on behalf of your office. Upon receipt from your Component Privacy Office, the DHS Privacy Office will review this form. If a PIA, SORN, or other privacy compliance documentation is required, your Component Privacy Office, in consultation with the DHS Privacy Office, will send you a copy of the template to complete and return.

For more information about the DHS Privacy compliance process, please see https://www.dhs.gov/compliance. A copy of the template is available on DHS Connect at (b)(7)(E) [redacted] or directly from the DHS Privacy Office via email: PIA@hq.dhs.gov or phone: 202-343-1717.

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project, Program, or System Name:	**CBP Enterprise Information Lifecycle (CBP EIL)**		
Component or Office:	Customs and Border Protection (CBP)	**Office or Program:**	OIT/ECSD
FISMA Name (if applicable):	CBP Enterprise Information Lifecycle (CBP EIL)	**FISMA Number (if applicable):**	CBP-08263-MAJ-08263
Type of Project or Program:	System	**Project or program status:**	Operational
Date first developed:	August 20, 2020	**Pilot launch date:**	N/A
Date of last PTA update	November 13, 2023	**Pilot end date:**	N/A
ATO Status (if applicable):[1]	Complete	**Expected ATO/ATP/OA date (if applicable):**	February 23, 2024

PROJECT, PROGRAM, OR SYSTEM MANAGER

Name:	(b)(6) (b)(7)(C) *(CBP EIL Project Manager)*		
Office:	OIT/ECSD	**Title:**	Project Manager
Phone:	(b)(6) (b)(7)(C)	**Email:**	(b)(6) (b)(7)(C)cbp.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	(b) (6) *CBP EIL ISSO)*		
Phone:		**Email:**	(b) (6) @associates.cbp.dhs.gov

[1] The DHS OCIO has implemented a streamlined approach to authorizing an Authority to Operate (ATO), allowing for rapid deployment of new IT systems and initiate using the latest technologies as quickly as possible. This approach is used for selected information systems that meet the required eligibility criteria in order to be operational and connect to the network. For more information, see (b)(7)(E)

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Updated PTA

CBP is submitting this updated PTA to account for a new function within RelativityOne. There are no other changes to the collection, use, or maintenance of PII associated with this update.

BACKGROUND:

CBP EIL is a major application with RelativityOne as a subsystem. RelativityOne was added to the CBP EIL ATO Boundary in early 2022.

CBP Enterprise Information Lifecycle (CBP EIL)

The EIL service is a Microsoft Azure Government cloud-based service, which provides a repository for Microsoft O365 Exchange Online journaled email, and in some cases, legacy archived email data, hosted in the Peraton DC2 site. The service's scalability delivers long-term retention of structured and unstructured data including journal email for government regulatory compliance and legal requirements.

This service is compliance-ready, enabling organizations to satisfy retention and discovery requirements. The EIL capabilities include email retention compliance, legal hold, and search capabilities, as well as integrated case management which reduce cost and improve productivity. The EIL Services also has the ability to automate retention policies, ensuring consistent regulatory compliance practices across all user data.

EIL Services Search feature on-demand with policy-driven data scoping as a key element of service. Custom indexes can create on-demand allowing full-text search of target data sets scoped by custodian/ and time period. The built-in case management can search, review and export results to 3rd party eDiscovery solutions.

As that mail data flows, a copy of the data is journaled to the CBP Enterprise Information Lifecycle (CBP EIL) service for 15-year long term storage and retention for Capstone officials and 10 years for non-Capstone officials in accordance with the General Records Schedule GRS 6.1-0568-2018-0001. Refer to question #5 for the email retention periods. This project will help facilitate a modern upgrade to email journaling from CBP's recent upgrade to Microsoft Office 365 and migration of email data from the current on-premise Email Vault (E-Vault) storage to a more modern Cloud based storage solution.

The EIL service is maintained by Peraton, Inc on the behalf of the DHS. The web application is hosted in an isolated Azure App Service Environment, within the Azure Government cloud, and load balances traffic for the end-user web application user interface.

The Microsoft Azure Government cloud has native security tools to prevent Distributed Denial of Service (DDoS), Anti-virus protection, Network Security Groups, Monitoring, and the Azure Key Vault for holding encryption keys and certificates. All data information traversing the Microsoft backbone to and from the customer's location is encrypted in transit using TLS 1.2 or Hypertext Transfer Protocol Secure (HTTPS). All data stored within Azure storage is encrypted at rest using Advanced Encryption Standard (AES) 256, Rivest-Shamir-Adleman (RSA) Based 2048-bit and is FIPS 140-2 compliant.

RelativityOne (CBP-08767-SUB-08263)

RelativityOne is a subsystem under CBP EIL. RelativityOne is a cloud-based document review software. RelativityOne offers case assessment, fact management, review, production, analytics, and legal hold functionalities within a suite.

RelativityOne is principally used by CBP's Office of Chief Counsel (OCC) for litigation:

- In litigation, parties may obtain discovery regarding any nonprivileged matter relevant to any party's claim or defense and proportional to the needs of the case. OCC uses RelativityOne to review, process, mark for confidentiality, redact for privilege, and ultimately produce electronically stored information as part of CBP's discovery obligations.
- OCC also uses RelativityOne to create privilege logs; in these logs, CBP expressly asserts individual privilege claims and describes the nature of each piece of privileged information to enable other parties to assess each claim.
- OCC uses RelativityOne to efficiently locate important information ahead of settlement conferences, in support of motions, and for hearings and trials.
- OCC will soon use a function within RelativityOne known as RelativityOne Legal Hold. A legal hold is a communication issued as a result of current or reasonably anticipation litigation and serves to suspend the normal disposition or processing of records. RelativityOne's Legal Hold is a complete legal hold management workflow application. OCC will utilize RelativityOne's Legal Hold to issue, track, audit, and lift legal holds in an efficient manner.

OCC shares its RelativityOne instance with CBP's Office of Professional Responsibility (OPR), CBP's Freedom of Information Act (FOIA Division), and other program offices. (b)(7)(E) [redacted] The FOIA Division uses RelativityOne to timely respond to requests for information pursuant to the Freedom of Information Act (FOIA), 5 U.S.C. § 552.

Notably, RelativityOne offers automation and artificial intelligence capabilities to help users wade through documents and otherwise maximize efficiencies. To provide select examples:

- RelativityOne can de-duplicate documents across custodians, identify documents that have already been produced, and create rules that establish what words, terms, or regular expressions will be redacted.
- RelativityOne includes a technology assisted review tool known as Continuous Active Learning ("CAL"). CAL continuously learns from reviewers' binary coding decisions, *e.g.*, responsive and nonresponsive. Once CAL is adequately trained in a particular RelativityOne workspace, it can independently make such binary coding decisions and prioritize for review those coded a desired way.
- RelativityOne includes Sentiment Analysis, an artificial intelligence tool that scores documents on the likelihood that they contain negativity, positivity, anger, or desire. Sentiment Analysis utilizes a model trained on thousands of samples of English-language text from multiple countries, and then analyzes each document on a sentence-by-sentence level and predicts which sentences contain each

of these four sentiments. Sentiment Analysis assigns each sentence a set of confidence scores that show the likelihood of the specific sentiment being present; the higher the score, the higher the chances of the sentiment being present. To provide an example, OCC may use Sentiment Analysis to efficiently identify documents from a certain timeframe that may undermine proffered testimony.

2. From whom does the Project, Program, or System collect, maintain, use, or disseminate information? *Please check all that apply.*	☐ This project does not collect, collect, maintain, use, or disseminate any personally identifiable information[2] ☒ Members of the public ☒ U.S. Persons (U.S citizens or lawful permanent residents) ☒ Non-U.S. Persons ☒ DHS Employees/Contractors (list Components): DHS CBP ☒ Other federal employees or contractors (list agencies): This could include any and all federal agencies and contractors.
2(a) Is information meant to be collected from or about sensitive/protected populations?	☒ No ☐ 8 USC § 1367 protected individuals (e.g., T, U, VAWA)[3] ☐ Refugees/Asylees ☐ Other. Please list:

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

[3] This involves the following types of individuals: T nonimmigrant status (Victims of Human Trafficking), U nonimmigrant status (Victims of Criminal Activity), or Violence Against Women Act (VAWA). For more information about 1367 populations, please see: DHS Management Directive 002-02, Implementation of Section 1367 Information Provisions, *available at*
(b)(7)(E)

3. What specific information about individuals is collected, maintained, used, or disseminated?

CBP Enterprise Information Lifecycle (CBP EIL)

CBP Enterprise Information Lifecycle does not collect PII as a default, but users of the system may choose to store PII in the CBP Microsoft Office 365 email system which gets archived into the system for long term retention. The system processes and stores all email communications sent and received by users– these may contain sensitive PII and FOUO. The specific type of information about individuals that is collected, generated, or retained is CBP Microsoft Office 365 email archiving and journaling.

PII and non-PII email data is maintained within the EIL storage, encrypted with DHS issued certificates. As a collaborative environment, this information includes, but is not limited to: Email Addresses, phone numbers, full name, Business Address, city, state, postcode and Personal Picture(s). In addition to DHS CBP Computer Host Names and IP's.

Access to uploaded PII is limited by the specific permissions set for each individual account.

RelativityOne

RelativityOne is used as a document review and processing platform and may contain PII stored within the documents uploaded into RelativityOne. Such information may include, but is not limited to, PII related to CBP personnel, personnel from DHS or other components, personnel from other state and/or federal agencies, or members of the public.

Similarly, a legal hold may contain the same information (including but not limited to, PII related to CBP personnel, personnel from DHS or other components, personnel from other state and/or federal agencies, or members of the public), which is gleaned from existing CBP documents. Additionally, a legal hold disseminated through RelativityOne will contain the name(s) and e-mail address(es) of the recipient(s), who is a CBP employee or contractor. The recipient will acknowledge receipt of the legal hold using RelativityOne and the acknowledgment will be logged in RelativityOne to generate the above-referenced audit trails.

3(a) Does this Project, Program, or System collect, maintain, use, or disseminate Social Security numbers (SSN) or other types of stand-alone sensitive information?[4] If applicable, check all that apply.

[4] Sensitive PII (or sensitive information) is PII that if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. More information can be found in the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information, *available at* https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information.

☒ Social Security number ☒ Alien Number (A-Number) ☒ Tax Identification Number ☒ Visa Number ☒ Passport Number ☒ Bank Account, Credit Card, or other financial account number ☒ Driver's License/State ID Number	☒ Social Media Handle/ID ☒ Biometric identifiers *(e.g., FIN, EID)* ☒ Biometrics.[5] *Please list modalities (e.g., fingerprints, DNA, iris scans): Click here to enter text.* ☐ Other. *Please list: Click here to enter text.*
3(b) Please provide the specific legal basis for the collection of SSN:	N/A - DHS EIL or RelativityOne will not be used to collect SSNs (or other types of stand-alone sensitive information), but records uploaded into CBP EIL RelativityOne may contain this information.
3(c) If the SSN is needed to carry out the functions and/or fulfill requirements of the Project, System, or Program, please explain why it is necessary and how it will be used.	
N/A - SSNs are not needed to fulfill the requirements of this project but note that SSNs may be already included in documents uploaded into CBP EIL and RelativityOne.	
3(d) If the Project, Program, or System requires the use of SSN, what actions are being taken to abide by Privacy Policy Instruction 047-01-010, *SSN Collection and Use Reduction*,[6] which requires the use of privacy-enhancing SSN alternatives when there are technological, legal, or regulatory limitations to eliminating the SSN? Note: *even if you are properly authorized to collect SSNs, you are required to use an alternate unique identifier. If there are technological, legal, or regulatory limitations to eliminating the SSN, privacy-enhancing alternatives should be taken, such as masking, truncating, or encrypting the SSN, or blocking the display of SSNs in hard copy or digital formats.*	
N/A	

[5] If related to IDENT/HART and applicable, please complete all Data Access Request Analysis (DARA) requirements. This form provides privacy analysis for DHS' IDENT, soon to be HART. The form replaces a PTA where IDENT is a service provider for component records. PRIV uses this form to better understand how data is currently shared, will be shared and how data protection within IDENT will be accomplished. IDENT is a biometrics service provider and any component or agency submitting data to IDENT is a data provider.

[6] *See* https://www.dhs.gov/publication/privacy-policy-instruction-047-01-010-ssn-collection-and-use-reduction.

4. How does the Project, Program, or System retrieve information?	☒ By a unique identifier.[7] Please list all unique identifiers used: Individuals will be able to search CBP EIL and RelativityOne by any term or identifier. ☒ By a non-unique identifier or other means. Please describe: Individuals will be able to search CBP EIL and RelativityOne by any term or identifier.
5. What is the records retention schedule(s) for the information collected for each category type (include the records schedule number)? *If no schedule has been approved, please provide proposed schedule or plans to determine it.* *Note: If no records schedule is in place or are unsure of the applicable records schedule, please reach out to the appropriate Records Management Office.*[8]	**CBP Enterprise Information Lifecycle (CBP EIL) records are covered under:** **GRS 6.1 item 10 *Email and other electronic messages of Capstone officials:* Permanent. cut-off at the end of the employee tenure. Transfer after 25 years or after declassification review (when applicable), whichever is later.** **GRS 6.1 Item 11 *Email and other types of electronic messages of non-Capstone officials*: Temporary: cut-off at end of employee tenure and destroy when 10 years old.** **GRS 6.1 Item 11 *Email and other types of electronic messages of VIP non-Capstone officials*: Temporary. Hold email and other types of electronic messages for length of employee tenure. When tenure ends, follow retention for non-capstone officials.** GRS 4.2 item 20 *Access and disclosure request files*: Temporary. Destroy 6 years after final agency action or 3 years after final adjudication by the courts, whichever is later, but longer retention is authorized if required for business use.

[7] Generally, a unique identifier is considered any type of "personally identifiable information," meaning any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

[8] *See* (b)(7)(E) [redacted]

5(a) How does the Project, Program, or System ensure that records are disposed of or deleted in accordance with the retention schedule (e.g., technical/automatic purge, manual audit)**?**	TBD – System capability to delete records may require development and will require configuration. This effort is in progress. In compliance with chain of custody all data is stored in Azure Blob. Note: Ensure no data is deleted from the system until system capability is in place to properly dispose of or delete in accordance with the retention schedule, Capstone. Any records created in RelativityOne will be preserved, whether in RelativityOne itself or through movement to a storage repository.

6. Does this Project, Program, or System connect, receive, or share PII with any other DHS/Component projects, programs, or systems?[9]	☐ No. ☒ Yes. If yes, please list: CBP Microsoft Office 365 CAPSTONE RelativityOne does not itself connect, receive, or share PII with any other DHS/Component projects, programs, or systems. Employees and contractors of DHS/Components may, however, encounter PII contained in documents in RelativityOne when performing document review in RelativityOne.
7. Does this Project, Program, or System connect, receive, or share PII with any external (non-DHS) government or non-government partners or systems?	☒ No. ☐ Yes. If yes, please list:
8. Is this sharing pursuant to new or existing information sharing agreement (MOU, MOA, LOI, RTA, etc.)? *If applicable, please provide agreement as an attachment.*	N/A Please describe applicable information sharing governance in place: N/A

[9] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in IACS.

9. Does the Project, Program, or System or have a mechanism to track external disclosures of an individual's PII?	☒ No. What steps will be taken to develop and maintain the accounting: There is no specific content looking to flag PII, store PII, or retrieve PII based on any search criteria other than emails sent or received by an individual. Per NIST SP 800-53 Rev. 4, Appendix J, AR-8: Organizations are not required to keep an accounting of disclosures when the disclosures are made to individuals with a need to know, are made pursuant to the Freedom of Information Act, or are made to a law enforcement agency pursuant to 5 U.S.C. § 552a(c)(3). ☐ Yes. In what format is the accounting maintained: Click here to enter text.

10. Does this Project, Program, or System use or collect data involving or from any of the following technologies:	☐ Social Media ☐ Advanced analytics[10] ☐ Live PII data for testing ☒ No
11. Does this Project, Program, or System use data to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly indicative of terrorist or criminal activity on the part of any individual(s) (i.e., data mining)?[11] This does not include subject-based searches.	☒ No. ☐ Yes. If yes, please elaborate: *Click here to enter text.*

[10] The autonomous or semi-autonomous examination of Personally Identifiable Information using sophisticated techniques and tools to draw conclusions. Advanced Analytics could include human-developed or machine-developed algorithms and encompasses, but is not limited to, the following: data mining, pattern and trend analysis, complex event processing, machine learning or deep learning, artificial intelligence, predictive analytics, big data analytics.

[11] Is this a program involving pattern-based queries, searches, or other analyses of one or more electronic databases, where—
(A) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals;

11(a) Is information used for research, statistical, or other similar purposes? If so, how will the information be de-identified, aggregated, or otherwise privacy-protected?	☒ No. ☐ Yes. If yes, please elaborate: *Click here to enter text.*
12. Does the planned effort include any interaction or intervention with human subjects[12] via pilot studies, exercises, focus groups, surveys, equipment or technology, observation of public behavior, review of data sets, etc. for research purposes	☒ No. ☐ Yes. If yes, please reach out to the DHS Compliance Assurance Program Office (CAPO) for independent review and approval of this effort.[13]
13. Does the Project, Program, or System provide role-based or additional privacy training for personnel who have access, in addition to annual privacy training required of all DHS personnel?	☐ No. ☒ Yes. If yes, please list: For role-based training, there is the annual privilege user training. General users are required to take the annual privacy and security awareness training provided within DHS PALMS site. RelativityOne does not provide any additional privacy training for personnel who have access.
14. Is there a FIPS 199 determination?[14]	☐ No. ☒ Yes. Please indicate the determinations for each of the following: Confidentiality:

(B) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and
(C) the purpose of the queries, searches, or other analyses is not solely—
(i) the detection of fraud, waste, or abuse in a Government agency or program; or
(ii) the security of a Government computer system.

[12] Human subject means a living individual about whom an investigator conducting research: (1) obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; or (2) obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens.

[13] For more information about CAPO and their points of contact, please see: https://www.dhs.gov/publication/compliance-assurance-program-office or (b) (7)(E) [redacted]. For more information about the protection of human subjects, please see DHS Directive 026-04: https://www.dhs.gov/sites/default/files/publications/mgmt/general-science-and-innovation/mgmt-dir_026-04-protection-of-human-subjects_revision-01.pdf.

[14] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

	☐ Low ☐ Moderate ☒ High ☐ Undefined Integrity: ☐ Low ☐ Moderate ☒ High ☐ Undefined Availability: ☐ Low ☐ Moderate ☒ High ☐ Undefined

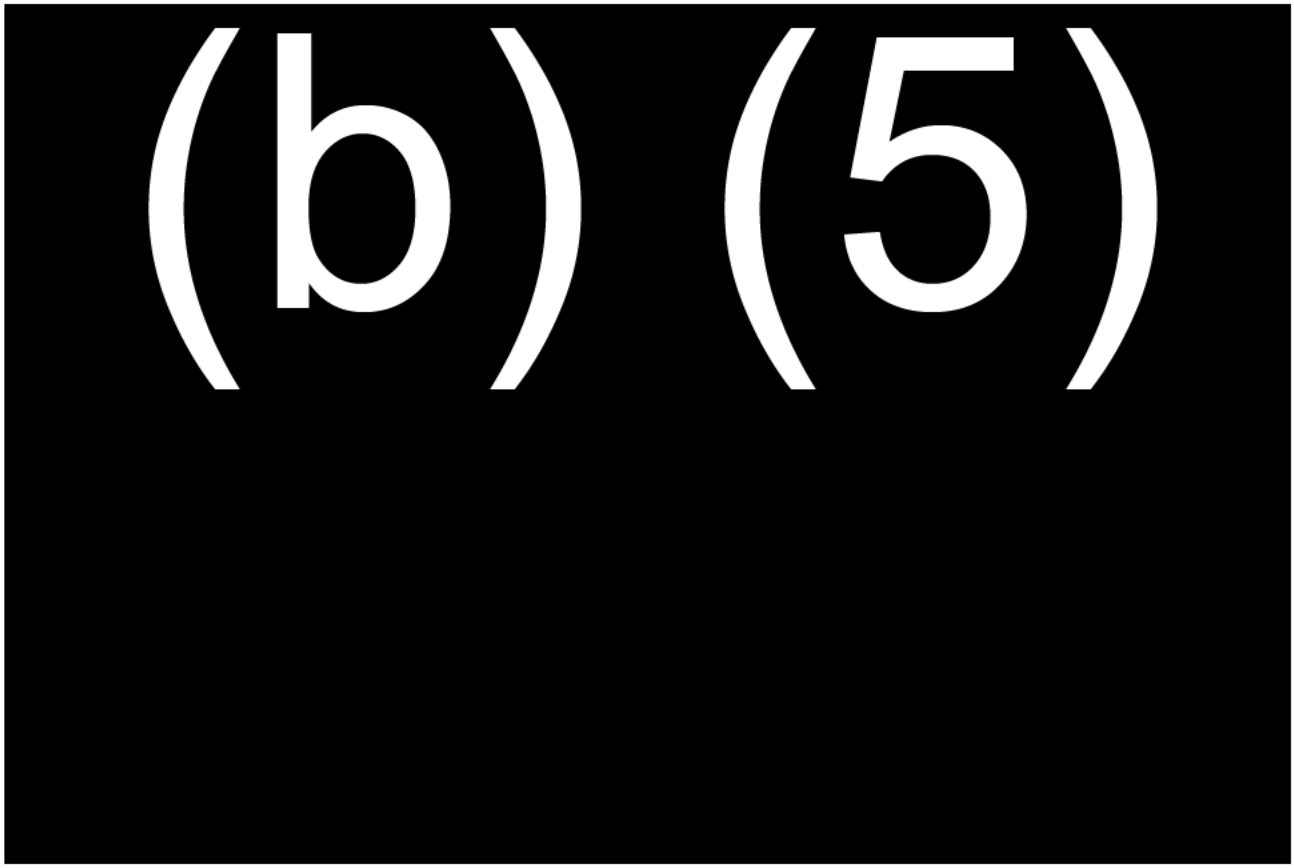
PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b)(6) (b)(7)(C)
PRIVCATS ID Number:	
Date submitted to Component Privacy Office:	July 7, 2024
Concurrence from other Component Reviewers involved (if applicable):	N/A
Date submitted to DHS Privacy Office:	*July 28, 2024*

Component Privacy Office Recommendation:
Please include recommendation below, including what new privacy compliance documentation is needed, as well as any specific privacy risks/mitigations, as necessary.

(b) (5)



(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b) (6)
DHS Privacy Office Approver (if applicable):	Click here to enter a date.
Workflow Number:	**0017680**
Date approved by DHS Privacy Office:	July 29, 2024
PTA Expiration Date	July 29, 2027

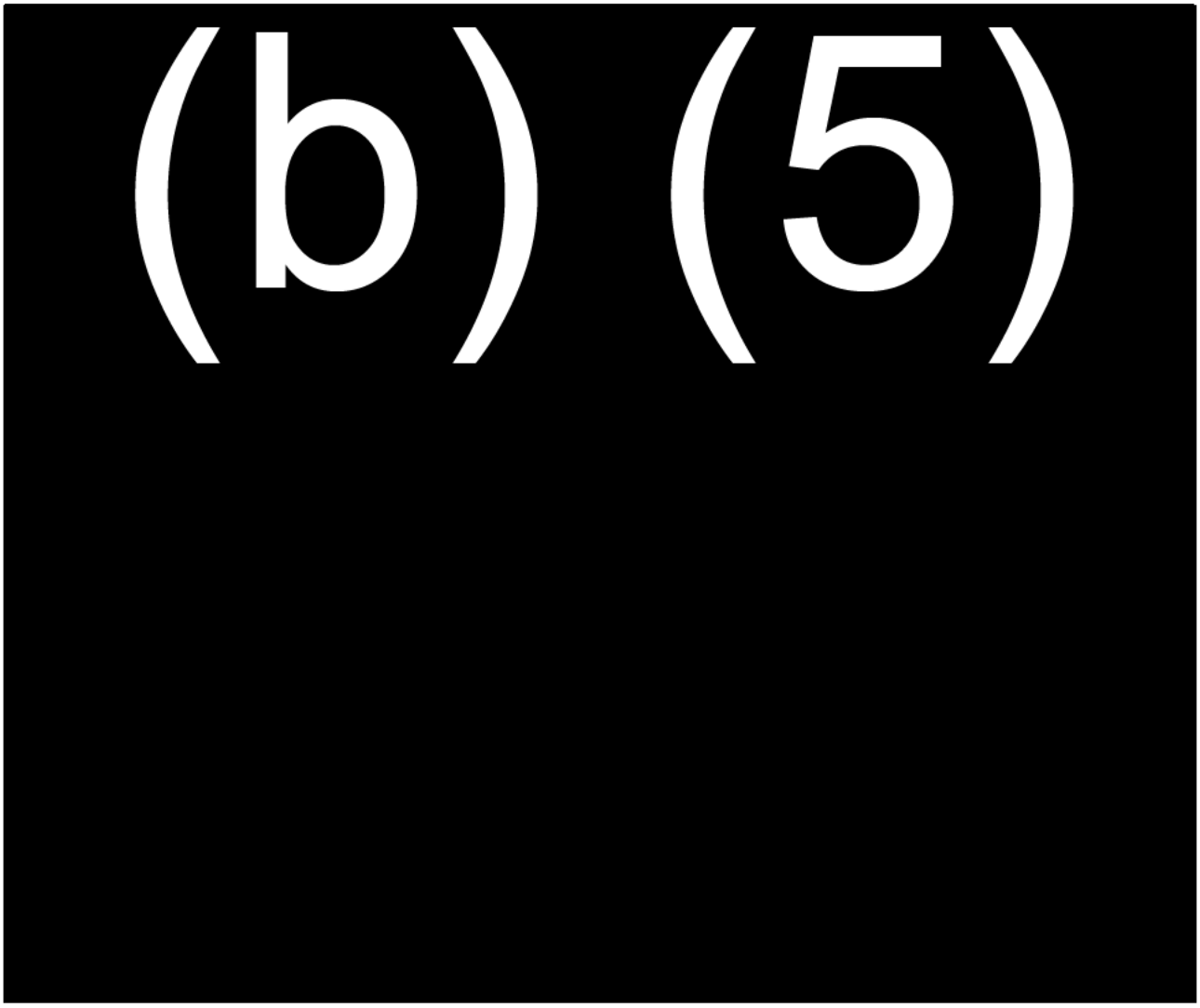
DESIGNATION

Privacy Sensitive System:	Yes
Category of System:	System If "other" is selected, please describe: *Click here to enter text.*

Determination:	☒ Project, Program, System in compliance with full coverage ☐ Project, Program, System in compliance with interim coverage ☐ Project, Program, System in compliance until changes implemented ☐ Project, Program, System not in compliance
PIA:	**System covered by existing PIA** DHS/ALL/PIA-059 Employee Collaboration Tools; DHS/ALL/PIA-073 Electronic Discovery (eDiscovery) Tools
SORN:	**System covered by existing SORN** DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), November 27, 2012, 77 FR 70792; DHS/ALL-001 Department of Homeland Security (DHS) Freedom of Information Act (FOIA) and Privacy Act (PA) Record System, February 4, 2014, 79 FR 6609; DHS/ALL-020 Department of Homeland Security Internal Affairs, April 28, 2014, 79 FR 23361; DHS/ALL-028 Department of Homeland Security Complaint Tracking System, July 21, 2009, 74 FR 35877

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above, and any further action(s) that must be taken by Component.

(b) (5)


(b) (5)