Privacy Impact Assessment

for the

Intelligence Reporting System-Next Generation

DHS Reference No. DHS/CBP/PIA-082

January 23, 2025

Homeland Security

Abstract

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) Intelligence Reporting System-Next Generation is a web-based system developed on the Automated Targeting System (ATS) platform.[1] The Intelligence Reporting System-Next Generation serves as a collaborative platform that facilitates CBP's ability to collect and amalgamate data, research subjects of interest, and create patterns and linkages across multiple databases. CBP officers, agents, and analysts use Workspaces to analyze and interpret raw, unprocessed information and create finished intelligence products and raw informational reports for operational awareness. CBP is publishing this Privacy Impact Assessment (PIA) to provide public notice about the Intelligence Reporting System-Next Generation and to assess the privacy risks and mitigation strategies associated with the system.

Overview

CBP is a federal law enforcement agency responsible for the critical mission of safeguarding our Nation's borders. CBP uses various capabilities, including analysis of intelligence information, to anticipate and adapt to the evolving operating environment more effectively. The threats CBP faces are complex and ever-changing. The CBP Intelligence Enterprise (IE)[2] focuses on amplifying CBP's collection and analysis proficiency and building its dissemination capability to enable intelligence-driven enforcement operations, near- and long-term planning, and resource allocation decisions.

"Intelligence" is processed law enforcement information about a threat, adversary, or issue of concern related to CBP's mission in the CBP operational environment.[3] CBP uses intelligence to identify information gaps, methods, trends, adversary intentions, threat capabilities, and vulnerabilities to provide decision support to CBP frontline operators and decision makers. Intelligence is derived from analysis of law enforcement information, whereas information is raw, unprocessed data that has not been analyzed or interpreted.

Intelligence plays a significant role helping accomplish the CBP border security mission

[1] *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.

[2] On August 25, 2017, the CBP Commissioner directed establishing a cohesive, threat-based, and operationally focused CBP Intelligence Enterprise. The creation of the CBP Intelligence Enterprise is an agency-wide effort comprised of offices and units that perform law enforcement intelligence activities from Air and Marine Operations, the Office of Field Operations, the Office of Intelligence, the Office of Trade, and the U.S. Border Patrol. The CBP Intelligence Enterprise enables the agency to operate under one common intelligence framework while promoting a unified approach to address current and emerging national border security issues.

[3] CBP's use of the term "intelligence" is distinguished from information collected by the Intelligence Community as authorized by Executive Order 12333 "United States Intelligence Activities," (Dec. 4, 1981) 46 Fed. Reg. 59941. CBP is not an Intelligence Community element and does not have authorities under Executive Order 12333.

by providing CBP decision makers and operators with a distinct understanding of threats and trends within a given area of responsibility. Intelligence further enables the effective planning and execution of CBP law enforcement and border security operations.

The CBP Intelligence Enterprise

The CBP Intelligence Enterprise is comprised of headquarters offices and field units across the agency that perform intelligence functions. The offices of Air and Marine Operations (AMO), Field Operations (OFO), Intelligence (OI), Trade (OT), and U.S. Border Patrol (USBP) conduct intelligence activities to provide critical information and intelligence to support CBP's collective law enforcement mission. Leveraging these offices' collective intelligence capabilities and expertise, the CBP Intelligence Enterprise cross-organizational team seeks to share knowledge, information, and capabilities across organizational boundaries to optimize CBP's collection, analysis, and dissemination of intelligence to support border security better. The Office of International Affairs (INA) supports CBP's intelligence mission by facilitating information sharing and capacity building with international partners through their attachés and advisors, which is consistent with law and CBP and DHS policy. The Office of Chief Counsel (OCC), Policy Directorate (PD), and the Privacy and Diversity Office (PDO) provide oversight and subject matter expertise on legal, privacy, and other relevant policy matters.

The CBP Intelligence Enterprise provides a formalized construct to promote unity of intelligence effort and interoperability. It jointly defines and anticipates intelligence challenges and develops unified options for actions to increase efficiencies in CBP intelligence efforts.

The CBP Intelligence Cycle

The CBP Intelligence Cycle is the process by which law enforcement information is converted into intelligence and made available to users. The CBP Intelligence Cycle has six steps: (1) planning and direction; (2) collection; (3) processing and exploitation; (4) analysis and production; (5) dissemination; and (6) consumption and feedback.

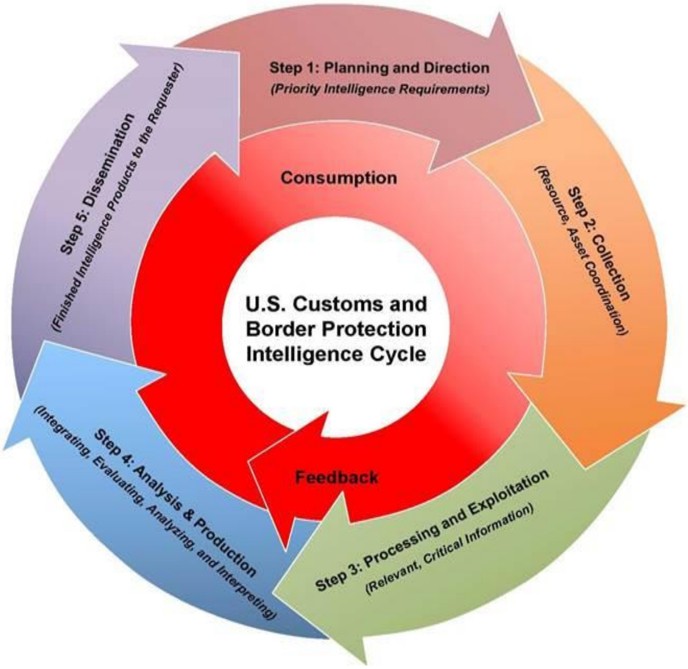
Step 1: Planning and Direction
(Priority Intelligence Requirements)
Step 2: Collection
(Resource, Asset Coordination)
Step 3: Processing and Exploitation
(Relevant, Critical Information)
Step 4: Analysis & Production
(Integrating, Evaluating, Analyzing, and Interpreting)
Step 5: Dissemination
(Finished Intelligence Products to the Requester)
Consumption
Feedback
U.S. Customs and Border Protection Intelligence Cycle

Figure 1. CBP Intelligence Cycle.
Source: CBP Office of Intelligence.

The effectiveness of the cycle is contingent upon CBP's ability to define, communicate, and implement the cycle and its companion processes. Although there are no firm boundaries delineating where each step within the intelligence cycle begins or ends, set forth below is an overview of the six steps within the cycle:

- Planning and Direction: Managing the intelligence process, from identifying the need for intelligence in the collection objectives to delivering an intelligence product to the consumer.
- Collection: Developing collection plans that task appropriate collection assets and/or resources to acquire the data and information required to satisfy collection objectives, including the identification, coordination, and positioning of assets and/or resources to satisfy collection objectives.
- Processing and Exploitation: Transforming collected data into meaningful information that can be disseminated and/or used to produce multidisciplinary intelligence products.
- Analysis and Production: Integrating, evaluating, analyzing, and interpreting information from single or multiple sources into a finished intelligence product. Finished intelligence products developed during this step provide assessments and judgments supporting border law enforcement capabilities that can predict, target, detect, and disrupt cross-border violations that threaten our national security, economy, and public safety.
- Dissemination: Reporting and providing intelligence to authorized consumers in a timely manner. Failure in this regard negates the diligent efforts accomplished in completing the previous steps of the intelligence cycle.
- Consumption and Feedback: Conversations between those providing intelligence and those consuming it are critical to meeting information requirements. The consumption and feedback step of the intelligence cycle allows intelligence producers to address scoping issues and adjust products to fit the needs of intelligence consumers.

Information Systems Supporting the Intelligence Enterprise

CBP developed the Intelligence Reporting System-Next Generation to facilitate collaboration across the Agency using shared electronic Workspaces to create and disseminate actionable intelligence and informational products to CBP frontline operators, analysts, and decision makers.[4] Developed on the Automated Targeting System platform,[5] the Intelligence Reporting System-Next Generation streamlines CBP users' ability to generate intelligence reports and informational products (collectively called IPs) due to the direct access it provides to existing Automated Targeting System data sources. The Intelligence Reporting System-Next Generation enables collaboration and information sharing while maintaining the data security and integrity of the underlying Automated Targeting System data. The Intelligence Reporting System-Next Generation allows analysts to view Automated Targeting System source data within Intelligence Reporting System-Next Generation Workspaces and intelligence reports and informational products without removing or changing the underlying source data in the Automated Targeting System.

The Intelligence Reporting System-Next Generation is CBP's primary authoring tool for unclassified intelligence reports and informational products. It provides collaborative Workspaces for multiple users across CBP to work on intelligence projects simultaneously, and standardized templates in a unified reporting system. Additionally, finished intelligence reports and informational products created in the Intelligence Reporting System-Next Generation are published directly into the Analytical Framework for Intelligence (AFI)[6] for dissemination to individuals who have the requisite need to know.

Data Accessible by the Intelligence Reporting System-Next Generation

The Intelligence Reporting System-Next Generation uses the same federated search functionality that is based in the Automated Targeting System.[7] This function allows users to search across many different systems, consistent with their mission authorities and need to know, to provide a consolidated view of data about a person or an entity. While the Automated Targeting System Privacy Impact Assessment and subsequent updates provide the list of records commonly

[4] The Intelligence Reporting System-Next Generation is available to CBP and authorized DHS Component and other government agency users who demonstrate a mission need consistent with their authorities. The Intelligence Reporting System-Next Generation is limited to users in DHS Components and other government agency users who analyze criminal information and intelligence and author related intelligence reports and information products.

[5] The Automated Targeting System is a decision support tool aggregating data from various CBP systems to compare traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based scenarios and assessments. 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.

[6] The Analytical Framework for Intelligence provides enhanced search and analytical capabilities to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and aids in the enforcement of customs, immigration, and other laws enforced by DHS at the border. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ANALYTICAL FRAMEWORK FOR INTELLIGENCE, DHS/CBP/PIA-010 (2012 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[7] Super Query allows users to search data across many different databases and systems to provide a consolidated view of data about a person or entity.

referred to as "ATS holdings," below is a general list of searchable data sources via the Intelligence Reporting System-Next Generation.

- Official Record: The Automated Targeting System maintains the official record for Passenger Name Records (PNR);[8] Importer Security Filing (10+2 documentation) and express consignment manifest information;[9] results of Cargo Enforcement Exams; Document and Media exploitation (DOMEX);[10] data from the combination of license plate, Department of Motor Vehicle (DMV) registration data, and biographical data associated with a border crossing; certain law enforcement and/or intelligence data, reports, and projects developed by CBP users that may include public source information; and certain information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department.

- Inclusion of Data from other CBP systems: The Automated Targeting System maintains copies of key elements of certain databases to minimize the impact of processing searches on the operational systems and to act as a backup for certain operational systems, including but not limited to: CBP's Automated Commercial Environment (ACE);[11] Overstay Leads from Arrival and Departure Information System (ADIS);[12] Automated Export System (AES);[13] Advance Passenger Information System (APIS);[14] Border Crossing Information (BCI);[15] Electronic System for Travel Authorization (ESTA);[16] Electronic Visa Update System (EVUS);[17] Global Enrollment

[8] Collected by CBP pursuant to its statutory authority, 49 U.S.C. § 44909, as implemented by 19 CFR 122.49d.

[9] Advance information about cargo and related persons and entities for risk assessment and targeting purposes.

[10] CBP conducts searches of electronic devices consistent with CBP Directive 3340-049A, *Border Search of Electronic Devices*, available at https://www.cbp.gov/document/directives/cbp-directive-no-3340-049a-border-search-electronic-devices/

[11] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED COMMERCIAL ENVIRONMENT (ACE), DHS/CBP/PIA-003 (2006 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[12] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ARRIVAL AND DEPARTURE INFORMATION SYSTEM (ADIS), DHS/CBP/PIA-024 (2007 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[13] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, INTRODUCTION TO THE AUTOMATED EXPORT SYSTEM (AES) (2023), *available at* https://www.cbp.gov/trade/aes/introduction.

[14] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ADVANCE PASSENGER INFORMATION SYSTEM (APIS), DHS/CBP/PIA-001 (2005 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[15] *See* DHS/CBP-007 Border Crossing Information (BCI), 81 Fed. Reg 89957 (December 13, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

[16] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC SYSTEM FOR TRAVEL AUTHORIZATION (ESTA), DHS/CBP/PIA-007 (2008 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[17] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT

System (GES);[18] I-94 data, Non-Immigrant Information System (NIIS);[19] Seized Asset and Case Tracking System (SEACATS);[20] TECS (not an acronym);[21] data from electronic devices;[22] the Department of Justice's (DOJ) National Crime Information Center (NCIC) and Federal Bureau of Investigation (FBI) Interstate Identification Index (III) hits for manifested travelers;[23] the U.S. Citizenship and Immigration Services' (USCIS) Central Index System (CIS) data received through TECS, and special protected classes[24] data; the U.S. Immigration and Customs Enforcement's (ICE) Student and Exchange Visitor Program (SEVP)[25] and Enforcement Integrated Database (EID),[26] which includes Criminal Arrest Records and Immigration Enforcement Records (CARIER);[27] Electronic Questionnaires for Investigations Processing (e-QIP);[28] historical National Security Entry-Exit Registration System (NSEERS); Flight Schedules and Flight Status OAG data; Social Security Administration (SSA) Death Master File;[29] Terror Screening Data Set (TSDS), which

Assessment for the Electronic Visa Update System (EVUS), DHS/CBP/PIA-033 (2016 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[18] *See* U.S. Department of Homeland Security, U.S. Customs and Border Protection, Privacy Impact Assessment for the Global Enrollment System (GES), DHS/CBP/PIA-002 (2006 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[19] *See* DHS/CBP-016 Nonimmigrant Information System, 80 Fed. Reg 13398 (March 13, 2015), *available at* https://www.dhs.gov/system-records-notices-sorns.

[20] *See* U.S. Department of Homeland Security, U.S. Customs and Border Protection, Privacy Impact Assessment for the Seized Asset and Case Tracking System (SEACATS), DHS/CBP/PIA-040 (2017 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[21] *See* U.S. Department of Homeland Security, U.S. Customs and Border Protection, Privacy Impact Assessment for the TECS System: Platform, DHS/CBP/PIA-021 (2016 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[22] CBP Directive No. 3340-049A, *Border Searches of Electronic Devices* (January 2018), *available at* https://www.cbp.gov/document/directives/cbp-directive-no-3340-049a-border-search-electronic-devices.

[23] *See* U.S. Department of Justice, Privacy Impact Assessment for the National Crime Information Center (NCIC), *available at* https://www.fbi.gov/file-repository/pia-ncic-020723.pdf/view, and

[24] Special protected classes of individuals include nonimmigrant status for victims of human trafficking, nonimmigrant status for victims of crimes, and relief for domestic violence victims.

[25] *See* U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement, Privacy Impact Assessment for the Student and Exchange Visitor Program (SEVP), DHS/ICE/PIA-001 (2020 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-ice.

[26] *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 (2019 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-ice.

[27] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 Fed. Reg 72080 (October 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

[28] *See* U.S. Department of Homeland Security, U.S. Customs and Border Protection, Electronic Questionnaires for Investigations Processing (e-QIP), available at https://careers.cbp.gov/s/applicant-resources/e-qip.

[29] *See* U.S. Social Security Administration, SSA Death Information, *available at* https://www.ssa.gov/dataexchange/request_dmf.html.

the Automated Targeting System ingests from the Watchlist Service (WLS);[30] Non-immigrant and Immigrant Visa data from Department of State (DOS) Consular Consolidated Database (CCD), Refused Visa data from the Consular Consolidated Database, and the Consular Electronic Application Center (CEAC);[31] and Secure Flight Passenger Data (SFPD) and Master Crew List/Master Non-Crew List data from the Transportation Security Administration (TSA).[32]

- Pointer System: The Automated Targeting System accesses and uses additional databases without ingesting the data, including: CBP's Arrival and Departure Information System (ADIS);[33] U.S. Border Patrol's Enforcement Tracking System (BPETS);[34] Enterprise Geospatial Information Services (eGIS);[35] e3 Biometrics System;[36] U.S. and Non-U.S. Passport Service through TECS; Department of State Consular Consolidated Database; commercial data aggregators (such as LexisNexis); ICE's Enforcement Integrated Database (EID); DHS Automated Biometric Identification System (IDENT);[37] National Law Enforcement Telecommunications System (NLETS), Department of Justice's National Crime Information Center and the results of queries in the FBI's Interstate Identification Index; Interpol; the National Insurance Crime Bureau's (NICB) private database of stolen vehicles; and United States Citizenship and Immigration Services' (USCIS) Person Centric Query System (PCQS).[38] In some instances, users of the Intelligence Reporting System-Next

[30] *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(e), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[31] *See* U.S. DEPARTMENT OF STATE, PRIVACY IMPACT ASSESSMENT FOR THE CONSULAR ELECTRONIC APPLICATION CENTER (CEAC) (2021 and subsequent updates), *available at* https://www.state.gov/wp-content/uploads/2021/06/Consular-Electronic-Application-Center-CEAC-PIA.pdf.

[32] *See* U.S. TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR THE SECURE FLIGHT PROGRAM, DHS/TSA/PIA-018 (2007 and subsequent updates), *available* at https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

[33] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ARRIVAL AND DEPARTURE INFORMATION SYSTEM (ADIS), DHS/CBP/PIA-024 (2007 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[34] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, U.S. BORDER PATROL, PRIVACY IMPACT ASSESSMENT FOR THE BORDER PATROL ENFORCEMENT TRACKING SYSTEM (BPETS/BPETS2), DHS/CBP/PIA-046 (2017 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

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

[36] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR CBP PORTAL (E3) TO ENFORCE/IDENT, DHS/CBP/PIA-012 (2012 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[37] *Ibid.*

[38] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY

Generation may determine that the data retrieved in a query was not of value to the particular intelligence report or informational product they are constructing, and it would be discarded. Where information retrieved in this manner is determined to be of value, it could be manually added to an Intelligence Reporting System-Next Generation workspace for later inclusion in a report or product.

- Data Manually Processed: The Automated Targeting System manually processes certain datasets to identify national security and public safety concerns and correlate records. Currently, DHS conducts this process for those records in ADIS that have been identified as individuals who may have overstayed their permitted time in the United States.

Based on user access provisioning to the underlying source datasets above, Intelligence Reporting System-Next Generation users conduct queries across these datasets as part of their research and analysis. This processing and exploitation of existing and accessible data maintained by CBP assists Intelligence Reporting System-Next Generation users in developing and producing intelligence reports and informational products. Intelligence Reporting System-Next Generation users review the search results, which will include responsive data from the datasets above to which a user has access, and determine which responsive information is relevant to their assigned intelligence research priority.

The Intelligence Reporting System-Next Generation Workspace

The Intelligence Reporting System-Next Generation Workspace is the primary collaboration function in the system and serves as a platform for users to gather, analyze, and share structured (*e.g.*, dates, names) and unstructured data (*e.g.*, images, free text) with multiple users simultaneously. Within the Workspace, users can add or upload data from Automated Targeting System holdings about subjects of interest and corresponding entities. Workspaces allow Intelligence Reporting System-Next Generation users to conduct the analysis and production portion of the CBP Intelligence Cycle. They use the results from the search to integrate, evaluate, analyze, and interpret information to be included in a finished intelligence report or informational product, as appropriate.

The Intelligence Reporting System-Next Generation Workspace function provides practical benefits for users who conduct intelligence research and analysis. The Workspace allows users to save their results and analysis in one place, even if they do not have enough information to finalize a finished intelligence report or informational product; allows them to return to their research and leads later. Intelligence Reporting System-Next Generation users can conduct link

IMPACT ASSESSMENT FOR THE PERSON CENTRIC QUERY SERVICE, DHS/USCIS/PIA-010 (2016 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

analysis[39] within the Workspace to identify other entities or individuals that are associated with the subject(s) of interest and save those linkages for later research. Users can also generate TECS Subject Records[40] directly from the Intelligence Reporting System-Next Generation based on the results of their research. Lastly, the Workspace functionality also allows multiple users to access the saved information, select an appropriate template to generate an intelligence report or an informational product, and create multiple kinds of intelligence reports and informational products from a single Workspace.

Reports Section

IPs created in the Intelligence Reporting System-Next Generation are published and then ingested into the Analytical Framework for Intelligence,[41] where authorized users with a need to know can access them. For example, intelligence reports and informational products can document encounters, provide informational bulletins, or describe situations of events or locations.

Through the Workspace in the Intelligence Reporting System-Next Generation, users can generate a variety of intelligence reports and informational products from one set of data, allowing for the publication of specific products to meet various mission and information needs. This functionality reduces the duplication of intelligence reports and informational products with various formats based on the same information. Each intelligence report or informational product is peer-reviewed to ensure completeness and quality before being approved and published. Completed, reviewed, and approved intelligence reports and informational products are published within the Intelligence Reporting System-Next Generation and can be ingested into the Analytical Framework for Intelligence. Finished intelligence reports and informational products in the Intelligence Reporting System-Next Generation are available to authorized CBP users with a valid need to know, and once ingested into the Analytical Framework for Intelligence, they can also be shared with consumers that have system access to the Analytical Framework for Intelligence's

[39] Generally, "link analysis" is a data analytics term referring to the process of looking for and establishing links between entities within a dataset as well as characterizing the weight associated with any link between two entities. Some examples include analyzing telephone call detail records to examine links established when a connection is initiated at one telephone number to a different telephone number, determining whether two individuals are connected via a social network, or the degree to which similar travelers select travel on specific flights. Not only does this form a link between a pair of entities, but other variables or attributes can be used to characterize that link.

[40] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM, DHS/CBP/PIA-009 (2010 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection. For the purposes of this Privacy Impact Assessment, "Subject Records" is a generic term that is used to describe the enforcement or inspection records located in TECS pertaining to individuals. Such records include, but are not limited to, those records related to a violation of law discovered by CBP or another authorized user agency or a CBP officer narrative concerning an interaction between CBP and a person. Subject Records encompass not only violations of laws enforced by CBP but may also include information on violations of other federal and state laws.

[41] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ANALYTICAL FRAMEWORK FOR INTELLIGENCE, DHS/CBP/PIA-010 (2012 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

finished intelligence reports and informational products, who are authorized to access and have a need to know the underlying information. Sharing outside of these uses must be pursuant to a routine use in the CBP Intelligence Reporting System (CIRS) System of Records Notice (SORN),[42] and must adhere to the handling and control requirements documented in the Analytical Framework for Intelligence Privacy Impact Assessment.[43] Additionally, the Reports section in the Intelligence Reporting System-Next Generation employs a filter function that allows users to sort reports by several criteria, including author, title, unit, and type.

Peer Review Process

Oversight is a critical part of ensuring that all finished intelligence products are aligned with current homeland security intelligence enterprise priorities and minimize inclusion of unnecessary personally identifiable information.[44] All intelligence products must have metatags limiting their distribution and ensuring alignment with current intelligence priorities. Part of the oversight process within the Intelligence Reporting System-Next Generation requires a peer review of all intelligence products prior to publication.

Once an intelligence analyst has completed a draft intelligence report or an informational product, they must submit the draft for peer review. The author of the intelligence report or an informational product must coordinate and notify the candidates who will participate in the peer review of the product. Only individuals with an "Reviewer" access level may complete a peer review of a draft product. Authors will route the draft product to the selected reviewers, who may provide comments or edits within the Intelligence Reporting System-Next Generation under the peer review function. Authors of intelligence reports and informational products may not review their products. All comments are saved within the Intelligence Reporting System-Next Generation, and authors and reviewers may exchange comments within the application to finalize the draft product. Once a reviewer is satisfied with the draft intelligence report or an informational product, they will issue a recommendation within the workspace and move the product to the status of "reviewed."

Following a peer review, the draft intelligence report or an informational product is in a "reviewed" status pending supervisory review for final approval for publication. Only individuals with a "Supervisor" access level within the Intelligence Reporting System-Next Generation may approve reviewed products for publication. Supervisors must ensure all products are coordinated appropriately, contain appropriate classification markings and warning labels, and are correctly

[42] *See* DHS/CBP-011 U.S. Customs and Border Protection Intelligence Records Systems, 82 Fed. Reg. 44198 (September 21, 2017), *available at* https://www.dhs.gov/system-records-notices-sorns.

[43] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ANALYTICAL FRAMEWORK FOR INTELLIGENCE, DHS/CBP/PIA-010 (2012 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[44] CBP Directive No. 2120-010A, *Privacy Policy, Compliance, And Implementation* (June 2022).

sourced. Once a supervisor is satisfied with the product, they will approve and publish the now finished intelligence report or an informational product.

Search Capability

As described above, authorized users can conduct queries across Automated Targeting System datasets for their research and analysis. This function is performed through the Automated Targeting System federated query search. As a part of this function, Intelligence Reporting System-Next Generation users can also utilize the Automated Targeting System facial comparison technology to augment their current search capabilities. This is done by manually uploading a photograph of a subject of interest that will run a search against the Automated Targeting System derogatory holdings.[45] In addition to a federated query search, the Intelligence Reporting System-Next Generation has search functionality that allows users to locate data within Intelligence Reporting System-Next Generation Workspaces and within the legacy Intelligence Reporting System and the Targeting Framework (TF).[46]

The search function in the Intelligence Reporting System-Next Generation differs from the Automated Targeting System federated query in that it only searches the current and historical Intelligence Reporting System and Targeting Framework systems, and not outside data sources or sources ingested or pointed to by the Automated Targeting System. The Intelligence Reporting System-Next Generation uses enhanced search functions that allow searches for structured entity data and reports, as well as unstructured data like attachments, annotations, or remarks. The ability to import existing data from the Targeting Framework eliminates the need for manual re-entry of subjects and/or associated data.

Applications Section

The Intelligence Reporting System-Next Generation contains several applications that provide ways to document information gathered via various workflows.[47] As with Workspaces, the data captured in these workflows may or may not be information linked to a particular person, information that becomes relevant over time, or information that will ever be included in intelligence reports and informational products. Appendix B of this Privacy Impact Assessment describes the applications that reside in the Intelligence Reporting System-Next Generation and

[45] This facial recognition technology and capability is described in the Automated Targeting System Privacy Impact Assessment Update Addendum 1.2.1 ATS Biometric Vetting Using Facial Recognition. *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(e), *available at*https://www.dhs.gov/sites/default/files/2022-07/privacy-pia-cbp006-ats-july2022_0.pdf.

[46] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM – ADDENDA 1.2 AND 1.2.1, DHS/CBP/PIA-006 (2007 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[47] A workflow within the Intelligence Reporting System-Next Generation is defined as the sequence or process in which the agent, officer or analyst uses the system to conduct their work within the CBP Intelligence Cycle.

will continually be updated as applications and tools are added.

User Roles

While system access can be provisioned for CBP, DHS, and other government agency personnel, access to the system is granted based on a user's role and job requirements. A user must have active TECS and Automated Targeting System accounts for access. A user's account relies on their Automated Targeting System access controls to determine what information they can search in the Automated Targeting System. This access provisioning allows the Intelligence Reporting System-Next Generation to restrict an individual's access to only the capabilities that they should have access to, based on their work and their need to know.

Additionally, system controls access to information and Workspaces by provisioning users with access to specific operating environments or areas of responsibilities, such as field offices and ports of entry for the Office of Field Operations, or, for U.S. Border Patrol, sectors/stations. There are additional units based on a job task or operating environment, and users may have access to several ports and units with a different set of roles in each:

- Consumer: This role allows authorized users to view Workspaces, intelligence reports, and informational products within the ports(s) and unit(s) to which they are provisioned.
- Author: In addition to the consumer capabilities, this role allows the authorized user to: (a) create, manage, and populate Workspaces; (b) create intelligence reports and informational products; (c) contribute to Workspaces within their provisioned unit(s); and (d) edit and delete their data within the units they are provisioned.
- Reviewer: In addition to the consumer and author capabilities, this role allows authorized users to: (a) review and provide comments for improvement to intelligence reports and informational products; and (b) recommend approval or modification within the units they are provisioned.
- Supervisor: In addition to all the preceding roles, this role allows the authorized user to: (a) approve intelligence reports and informational products; and (b) edit and delete data entered by others within the units they are provisioned.

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?

The principal legal authorities that support DHS's maintenance, use, and sharing of Intelligence Reporting System-Next Generation information to assist in identifying potential threats to the homeland include:

- Title 6 of the United States Code, Domestic Security,[48] including:
  - Functions of the Secretary of Homeland Security; and
  - Responsibilities of the Secretary of Homeland Security.
- Title 8 of the United States Code, Aliens and Nationality (powers of immigration officers and employees);[49]
- Title 19 of the United States Code, Customs Duties,[50] including:
  - Search of vehicles and persons;
  - Inspection of merchandise and baggage;
  - Examination of baggage;
  - Boarding vessels; and
  - Regulations for the search of persons and baggage.
- Title 49 of the United States Code, Transportation (passenger manifests);[51]
- Enhanced Border Security and Visa Reform Act of 2002 (Pub. L. 107-173);
- Trade Act of 2002 (Pub. L. 107-210);
- 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); and
- Security and Accountability for Every Port Act of 2006 (Pub. L. 109-347).

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

The Intelligence Reporting System-Next Generation is covered by and contains information from DHS/CBP-024 Intelligence Records System (CIRS).[52] The Intelligence Records System is the exclusive CBP System of Records Notice for finished intelligence products, raw

[48] 6 U.S.C §§ 112(b) and 202.
[49] 8 U.S.C § 1357.
[50] 19 U.S.C §§ 482, 1461, 1496, 1581, 1582.
[51] 49 U.S.C § 44909.
[52] *See* DHS/CBP-011 U.S. Customs and Border Protection Intelligence Records Systems, 82 Fed. Reg. 44198 (September 21, 2017), *available at* https://www.dhs.gov/system-records-notices-sorns.

intelligence information, public source information, or other information collected by CBP for an intelligence purpose. The underlying data used in the Intelligence Reporting System-Next Generation is housed in the Automated Targeting System and is covered by the System of Records Notice for the Automated Targeting System[53] and the System of Records Notices for the underlying source systems as noted in the Automated Targeting System Privacy Impact Assessment.

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

The Intelligence Reporting System-Next Generation is part of the Automated Targeting System security authorization boundary, which has undergone the Security Authorization process in accordance with DHS and CBP policy and complies with federal statutes, policies, and guidelines.

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

CBP maintains records in the Intelligence Reporting System-Next Generation consistent with the DHS NI-563-07-016 records schedule of the DHS Office of Intelligence and Analysis for Raw Reporting Files and Finished Intelligence Case Files. The retention requirements are as follows:

- **Dissemination Files and Lists:** CBP will retain finished and current intelligence report information distributed to support the Intelligence Community, DHS Components, and federal, state, local, tribal, and foreign governments and includes contact information for the distribution of finished and current intelligence reports for two (2) years.
- **Raw Reporting Files:** CBP will retain raw, unevaluated information on threat reporting originating from operational data and supporting documentation that is not covered by another existing DHS system of records for thirty (30) years, pursuant to the System of Records Notice for the CBP Intelligence Reporting System.
- **Finished Intelligence Case Files:** CBP will retain finished intelligence and associated background material for products identifying imminent homeland security threats, assessments providing intelligence analysis on specific topics, intelligence reporting to senior leadership, intelligence summaries about current intelligence events, and periodic reports containing intelligence awareness information for specific region,

[53] *See* DHS/CBP-006 U.S. Customs and Border Protection Automated Targeting System, 77 Fed. Reg. 30297 (May 22, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.

sector, or subject areas of interest as permanent records and will transfer the records to the National Archives and Records Administration after twenty (20) years.

- **Requests for Information/Data Calls:** CBP will retain requests for information and corresponding research, responses, and supporting documentation for ten (10) years.

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 Paperwork Reduction Act does not cover the information contained in the Intelligence Reporting System-Next Generation because the system does not collect any information directly from the public. However, the Intelligence Reporting System-Next Generation collects information from other systems, which may have originally collected information using various customs, immigration, agricultural, and admissibility forms the Act covers.

Section 2.0 Characterization of the Information

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

As part of the Automated Targeting System platform, the Intelligence Reporting System-Next Generation accesses an extensive amount of travel, trade, and law enforcement information to support the development of intelligence reports and informational products. In addition to the information derived from CBP systems, Intelligence Reporting System-Next Generation users may upload information that is relevant to a Workspace, including information publicly available on the Internet including social media information related to border security, consistent with oversight and legal requirements, as well as information provided to CBP from other federal, state, local, and foreign government agencies or certain information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department. The information, generally associated with individuals, organizations, and incidents related to border security, national security, law enforcement, and immigration, customs, and agriculture issues, is used to generate intelligence reports and informational products for distribution to law enforcement and intelligence organizations through the Analytical Framework for Intelligence. There are four categories of data containing Personally Identifiable Information (PII) that are used, maintained, and disseminated by the Intelligence Reporting System-Next Generation:

1) <u>Travel Data:</u> The Intelligence Reporting System-Next Generation allows users to retrieve and use information from the Automated Targeting System, which contains

information from other CBP systems, including data about individuals who enter, exit, or transit through the United States, as well as information about individuals involved in the travel industry.

2) Trade Data: Intelligence Reporting System-Next Generation users also have access through the Automated Targeting System to information related to individuals involved in international trade, including those that import or export of merchandise across the United States border.

3) Publicly Available Information: Open-source information, including public-source data and social media information related to border security and international trade issues.

4) Threat Data: Information associated with individuals who may pose a threat to the United States, as well as persons who are alleged to be involved in, who are suspected of, or who have been arrested for violations of the laws enforced or administered by DHS.

The Intelligence Reporting System-Next Generation sources most, but not all, information from the Automated Targeting System. The Automated Targeting System maintains information about the following categories of individuals, any of which may be included in an intelligence report/informational product or Workspace, if relevant and necessary:

- Persons, including operators, crew, and passengers, who seek to, or do in fact, enter, exit, or transit through the United States or through other locations where CBP maintains an enforcement or operational presence by land, air, or sea;
- Crew members traveling on commercial aircraft that fly over the United States;
- Persons who engage in any form of trade or other commercial transaction related to the importation or exportation of merchandise, including those required to submit an Importer Security Filing;
- Persons who are employed in any capacity related to the transit of merchandise intended to cross the United States border;
- Persons who serve as booking agents, brokers, or other persons who provide information on behalf of persons seeking to enter, exit, or transit through the United States, or on behalf of persons seeking to import, export, or ship merchandise through the United States;
- Owners of vehicles that cross the border;

- Persons whose data was received by the Department as the result of memoranda of understanding or other information sharing agreement or arrangement because the information is relevant to the border security mission of the Department;
- Persons who were identified in a narrative report, prepared by an officer or agent, as being related to, or associated with other persons who are alleged to be involved in, who are suspected of, or who have been arrested for violations of the laws enforced or administered by DHS; and
- Persons who may pose a threat to the United States.

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

The Intelligence Reporting System-Next Generation, as part of the Automated Targeting System platform, does not collect information directly from individuals, but rather ingests or accesses and uses information collected, generated, and stored by and in other systems. As described in previously issued Automated Targeting System Privacy Impact Assessments, the system contains information from various other systems,[54] including DHS owned data, Other Government Agency (OGA) data, commercial data, and publicly available information, including social media information related to border security. While most of the data in the system is accessed via the Automated Targeting System and collected from other CBP data sources, there may be instances in which CBP personnel collect information directly from a member of the public, such as during an interview. The interview data may then be stored in the Intelligence Reporting System-Next Generation. Users generate informational and intelligence products and deliberative Workspace notes and projects.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Yes. Workspaces and products may include any information originally sourced from the Automated Targeting System, which includes commercial sources or publicly available data. Users may also access commercial sources and publicly available data, consistent with oversight and legal requirements, and include such information within Workspaces or intelligence or informational products. Generally, users may include information sourced from public articles, public-source data (including information from publicly available social media related to border security), and other published information on individuals and events related to CBP's mission.

[54] The specific data sources that are aggregated by Automated Targeting System and support the Intelligence Reporting System-Next Generation are outlined in the Automated Targeting System Privacy Impact Assessments, which will be updated as necessary if/when future data sets are incorporated.

This data is used to cross-check and confirm data collected and maintained by CBP from individuals and commercial entities, and broaden the scope of relevant information available to the user.

2.4 Discuss how accuracy of the data is ensured.

As with the Automated Targeting System, the data accuracy within the Intelligence Reporting System-Next Generation is mainly reliant upon accurate and complete data being maintained in the source systems. When data is added by a user into a Workspace, the information becomes a snapshot at the time of input, and there is no 'reach back' to update automatically. However, users are required to verify the accuracy of information returned in an Automated Targeting System search against the source system, and where available, other corroborating information, before it can be used in an intelligence report or an informational product. This review should identify discrepancies, if any, during the development of an intelligence report or an informational product.

If users are aware of information that has changed in the source systems, they are required to take action to correct the data, which may include creating a new intelligence report or and informational product to correct inaccurate information that may have been published previously. When incorrect information is discovered, a revised product will be published to correct the information or note the questionable fact or content, and the incorrect intelligence reports and informational products will be removed from the system. To the extent information that is obtained from another government source (for example, vehicle registration data that is obtained through National Law Enforcement Telecommunications System (NLETS)[55]) is determined to be inaccurate, it is incumbent upon the user to notify the record owner that the information is inaccurate.

In addition, Intelligence Reporting System-Next Generation products are audited and supervisor reviewed. This allows user-provided information to be reviewed for accuracy or discrepancies. If information is found to be incorrect, the product can be corrected as appropriate. All intelligence products are reviewed by a user with the supervisor role before publishing. Supervisors must ensure all products are coordinated as appropriate, contain appropriate classification markings and warning labels, and are correctly sourced. Further, once an intelligence report or an informational product is published in the Analytical Framework for Intelligence, it can be recalled from that system.

2.5 <u>Privacy Impact Analysis</u>: Related to Characterization of the Information

In addition to the privacy risks associated with the Automated Targeting System and

[55] NLETS is a private not-for-profit corporation created by the 50 state law enforcement agencies.

discussed in previous Privacy Impact Assessments, the following potential privacy risks related to the system's data collection and use have been identified.

Privacy Risk: There is a risk that Intelligence Reporting System-Next Generation users may create intelligence reports and informational products based on inaccurate or outdated information retrieved from the Automated Targeting System platform.

Mitigation: This risk is mitigated. While the Automated Targeting System platform, upon which the Intelligence Reporting System-Next Generation is built, is not the system of record for most of the source data, the Automated Targeting System receives updates with any changes to the source system databases. Continuous source system updates occur in real-time or near real-time. When corrections are made to data in source systems, the Automated Targeting System updates this information immediately, and only the latest data are used. In this way, the Automated Targeting System integrates all updated data (including accuracy updates) in as close to real-time as possible. Additionally, users are required to verify the accuracy of information returned in an Automated Targeting System search against the source system before it can be used. In cases in which information within a published intelligence report or an informational product is later found to be incorrect, there is a capability within the Intelligence Reporting System-Next Generation allows a user, with supervisory approval, to make changes or purge the product containing inaccurate information.

Privacy Risk: Because the system permits users to provide their analysis and incorporate data from commercial and publicly available sources rather than using only directly collected information, there is a risk that data from commercial and publicly available sources may be incorrect and relied upon by Intelligence Reporting System-Next Generation users.

Mitigation: This risk is mitigated. The Intelligence Reporting System-Next Generation requires that user-provided information be entirely attributable to the user who provided it. The auditing and peer review functions, including possible multiple peer reviews, further serve to ensure that user-provided information is reviewed for flaws. The auditing log documents and records the actions taken by the user across the system, including in Workspaces, intelligence reports and informational products, and its applications. To publish a product in the Intelligence Reporting System-Next Generation, the product must be reviewed and approved by a user who has been granted the supervisory role. The Intelligence Reporting System-Next Generation also can send the product to a peer for review and comment prior to sending it for supervisor approval. If information included in an intelligence report or an informational product is determined to be incorrect, the product can be corrected prior to publication. Information in intelligence reports and informational products sourced from commercial data aggregators and publicly available sources is checked for accuracy using the same review process as other information in the Intelligence Reporting System-Next Generation, including cross checking it against various other sources.

Privacy Risk: There is a privacy risk to data integrity because when data is pulled into a Workspace, it becomes a snapshot in time, and it is not automatically refreshed in the Intelligence Reporting System-Next Generation, potentially causing it to become stale or inaccurate.

Mitigation: This risk is not mitigated. CBP relies upon the source systems to ensure that data ingested by the Intelligence Reporting System-Next Generation is accurate and complete. Continuous source system updates occur in real-time or near real-time. When corrections are made to data in source systems, Intelligence the n immediately, and only the latest data is displayed in the search results. When data is pulled into a Workspace, discrepancies may be identified in the context of a user's review of the data, and users are required to take action to correct the data if they become aware of inaccurate data.

Workspaces are dynamic in that the user can update the information; however, the information does not automatically change as new information is discovered and displayed in the source system. If users are aware of information that has changed in source systems, they can recall intelligence reports and informational products to correct inaccurate information that may have been published previously. To the extent information is obtained from another government source and determined to be inaccurate, CBP would communicate with the agency that maintains the record to notify them of the need for remedial action. Users should verify the accuracy of information prior to the publication of any product.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

the Intelligence Reporting System-Next Generation allows users to enhance the data CBP already collects through its advanced search technology and collaborative Workspaces. The Intelligence Reporting System-Next Generation consolidates query results across multiple source systems into an integrated view, eliminating the need for users to log into separate systems as they conduct research for the development of intelligence reports and informational products. This reduces the time spent searching each system and reduces the load placed on those systems through repeated queries. User-provided information and data obtained from publicly available and commercial sources are used to complement, clarify, and/or provide context to the source data that is used.

The Intelligence Reporting System-Next Generation maintains this information to:

- Author intelligence reports and informational products to reflect and generally support CBP's collection, analysis, reporting, and distribution of law enforcement, immigration administration, terrorism, intelligence, and homeland security information in support of CBP's law enforcement and facilitation of legitimate travel and trade missions;

- Produce law-enforcement intelligence reports and informational products that provide actionable information to CBP's law enforcement personnel and other appropriate government agencies;
- Enhance the efficiency and effectiveness of the research and analysis process for DHS law enforcement, immigration, and intelligence personnel through information technology tools that provide for the advanced search and analysis of various datasets;
- Facilitate multi-jurisdictional information exchange between CBP, other law enforcement agencies, and intelligence organizations regarding known and suspected terrorists and associates; and
- Identify potential criminal activity, terrorism, trafficking of illicit narcotics, immigration violations, trade violations, and threats to homeland security to uphold and enforce the law and to ensure public safety.

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. While the Intelligence Reporting System-Next Generation sits on the Automated Targeting System platform where risk assessments for persons, cargo, and conveyances are applied to criteria and rules, it does not perform data mining activities. While the Intelligence Reporting System-Next Generation uses link analysis and can make visual links and associations between two or more data sets, there is no technology that performs predictive patterns or anomalies.

3.3 Are there other components with assigned roles and responsibilities within the system?

The Intelligence Reporting System-Next Generation is available to CBP as well as authorized DHS components and other government agency users who demonstrate a mission need. the system is specifically limited to users in DHS components and other government agency users who analyze information and intelligence and author intelligence reports and informational products. Users from components outside of CBP, and other government agencies, only have access through the Intelligence Reporting System-Next Generation to the data maintained in the Automated Targeting System, which they have been authorized to view and use. Access to the Automated Targeting System and the Intelligence Reporting System-Next Generation by personnel from other government agencies requires the establishment of access agreements and the regular completion of security and privacy awareness training.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that authorized users of the Intelligence Reporting System-Next Generation could utilize their access for unapproved or inappropriate purposes, such as performing searches on themselves, friends, relatives, or neighbors.

Mitigation: This risk is mitigated. CBP has developed training, support materials, and enhanced auditing features to address permissible queries specifically.

1.) Training

Users are required to complete annual security and data privacy training that outlines the legal and policy restrictions that govern the use and dissemination of data. Additionally, CBP developed and implemented training specific to intelligence research and reporting activities, focusing on law enforcement authorities, the First and Fourth Amendments, the Privacy Act, and civil rights and civil liberties considerations. This training is delivered on an ad-hoc basis.

2.) Support Materials

CBP issued a memorandum and guidance on permissible queries and research, identifying limits to queries and information sharing with law enforcement partners. Specifically, these memoranda address:

- permissibility/appropriateness of running queries on individuals who have not engaged in criminal conduct or do not pose an articulable threat to border security, national security, officer safety, or public safety.
- appropriate limits to conducting research on individuals who are not a subject of interest but who may be associated with such a subject and what does and does not warrant research in CBP systems.
- limits on research engagement with non-governmental entities and individuals (media or otherwise).

3.) Auditing

The Intelligence Reporting System-Next Generation has an auditing function that monitors each user’s access and use of the system to ensure compliance with all privacy and data security requirements, as described in Section 8. The detection of inappropriate use results in suspending the user’s access to the system until the issue can be investigated and resolved.

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.

Most of the information used in the Intelligence Reporting System-Next Generation is pulled from the Automated Targeting System and is not collected directly from the public, so there is no opportunity to provide notice for this specific collection. However, notice is generally made when information provided by members of the public is collected for maintenance in the source systems. In some instances, intelligence reports and informational products built in the Intelligence Reporting System-Next Generation may include interview notes collected directly from an individual. In those cases, general notice of collection is provided during the interview. Additional public notice of the existence, contents, and uses of the Intelligence Reporting System-Next Generation is provided through the publication of this Privacy Impact Assessment and the System of Records Notice for the CBP Intelligence Reporting System, as well as through the individual Privacy Impact Assessments and System of Records Notices for the source systems in which information is maintained. The source system documents outline how the information may be used and the circumstances under which information can be shared. Providing direct notice to individuals prior to the use of information in the Intelligence Reporting System-Next Generation could impede CBP's law enforcement and investigative activities.

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

In most cases, CBP does not provide opportunities for individuals to decline the collection or use of their information. Additionally, all persons attempting to enter or depart the United States are subject to data collection requirements and processes, including interviews that may provide an officer or agent information pertaining to an alleged violation.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not know that their information is being used beyond its original collection or to develop intelligence products.

Mitigation: This risk is partially mitigated. CBP partially mitigates this risk through the publication of this Privacy Impact Assessment and the System of Records Notice for the CBP Intelligence Reporting System. Both publications serve as public notice of the system's existence, contents, and uses, and help to increase the transparency of its operations. In addition, notice of collection by the source systems performing the original collection is described in the individual Privacy Impact Assessments and System of Records Notices for those systems.

Section 5.0 Data Retention by the Project

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

CBP will abide by the safeguards, retention schedules, and dissemination requirements of DHS source system System of Records Notices to the extent those systems are applicable, and the information is not incorporated into a finished intelligence report or an informational product. A published intelligence or informational product's retention schedule will fall under the DHS/CBP-024 Intelligence Records System.[56] Records maintained in the Intelligence Reporting System-Next Generation will be retained consistent with the DHS NI 563-07-016 records schedule of the DHS Office of Intelligence and Analysis for Raw Reporting Files and Finished Intelligence Case Files, which is described in more detail in Section 1.4 of this Privacy Impact Assessment.

When a user searches, the user must manually add and save only the relevant, responsive data into an Intelligence Reporting System-Next Generation Workspace. All other data that populated as a result of the search that was not manually entered into a Workspace will immediately be purged when the user closes the search function. While the Intelligence Reporting System-Next Generation does not retain search results, there is a function that allows for the saving of search parameter sets. This makes it possible for a user to quickly conduct the same search later to return updated or additional information based on the same search criteria.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information maintained in the Intelligence Reporting System-Next Generation may be maintained for longer than is required or beyond its established retention period.

Mitigation: This risk is partially mitigated but will be fully mitigated in the future. CBP is in the process of developing a technical solution that will ensure that information maintained in the Intelligence Reporting System-Next Generation will not be retained for longer than the timeframes outlined in Section 1.4, in accordance with established record retention schedules. The technical solution will delete information that has reached its retention limit through the implementation of an automated roll-off process. When a record reaches its retention limit, either 30 years for Raw Intelligence products (including items that have remained in an unpublished/draft status) or 20 years for Finished Intelligence products, the system will automatically identify and delete them. At the time this Privacy Impact Assessment was developed, none of the records maintained in the Intelligence Reporting System-Next Generation are near their retention limit.

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

[56] *See* DHS/CBP-011 U.S. Customs and Border Protection Intelligence Records Systems, 82 Fed. Reg. 44198 (September 21, 2017), *available at* https://www.dhs.gov/system-records-notices-sorns.

information is accessed and how it is to be used.

No, intelligence products that are published in the Intelligence Reporting System-Next Generation and distributed within the Analytical Framework for Intelligence are only accessible to DHS users. The only exception is access to other agencies working on behalf of the CBP mission. CBP considers requests from users outside of DHS to access the system on a case-by-case basis. External users are generally co-located with CBP, working closely on joint programs. These joint programs facilitate and improve CBP's information sharing capabilities. Other government agency employees must have a valid Tier 5 Background Investigation required for all CBP system access, justify their need for access, and agree to CBP's terms as outlined in the MOU/MOA regarding the proper use, handling, and dissemination of data. Designated Points of Contact are responsible for updating CBP on their employees' status regarding a continued need for access. CBP also conducts regular audits on the continued need for system access and Tier 5 Background Investigation expiration dates; and access is removed as necessary.

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

Consistent with DHS's information sharing mission, information stored in DHS/CBP-024 CBP Intelligence Reporting System may be shared with other DHS Components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS/CBP may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in the System of Records Notice for the CBP Intelligence Reporting System.

6.3 Does the project place limitations on re-dissemination?

Information from the Intelligence Reporting System-Next Generation may be provided outside of DHS, consistent with law, DHS/CBP policy, and the routine uses in the System of Records Notice for the CBP Intelligence Reporting System. Users of the Intelligence Reporting System-Next Generation will utilize the processes and procedures already established within DHS and CBP regarding the dissemination of data and information. Intelligence reports and informational products contain warning banners that address re-dissemination; specifically, it requires recipients of CBP products to obtain CBP consent before sharing such products or information contained therein with other entities.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

CBP personnel who disclose information outside of DHS must account for the disclosure via a DHS Form 191 or other approved method per DHS Directive 047-01 Privacy Policy and

Compliance,[57] and DHS Instruction 047-01-001 Privacy Policy and Compliance.[58]

6.5 Privacy Impact Analysis: Related to Information Sharing

<u>Privacy Risk</u>: There is a risk that authorized users may make unauthorized disclosures of this information.

<u>Mitigation</u>: This risk is mitigated. As part of the periodic recertification process, all users are required to complete annual privacy awareness training, which includes instruction on appropriate and inappropriate uses and disclosures of the information they receive as part of their official duties. The use of the system and access to data is monitored and audited, as described in Section 8 below. Should users inappropriately disclose information, they may lose access to the system and information, and the disclosure will be referred to the appropriate internal investigation entity. Additionally, CBP distributed a Research Guidance document where information sharing is specifically discussed to ensure disclosures are reasonable, necessary, appropriate, and in compliance with all relevant laws and policies.

Section 7.0 Redress

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

Because the system contains sensitive information related to intelligence, counterterrorism, homeland security, and law enforcement programs, activities, and investigations, DHS has exempted the Intelligence Reporting System-Next Generation from certain access and amendment provisions of the Privacy Act of 1974 through a final rule in the Federal Register.[59]

Notwithstanding the applicable exemptions outlined in the System of Records Notice for the CBP Intelligence Reporting System, CBP reviews all requests on a case-by-case basis. When such a request is made, and access would not appear to interfere with or adversely affect the national security of the United States or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of CBP and in accordance with procedures published in the applicable System of Records Notice. Individuals seeking notification of and access to any record contained in this system of records or seeking to

[57] *See* DHS DIRECTIVE 047-01 PRIVACY POLICY AND COMPLIANCE, *available at* https://www.dhs.gov/publication/privacy-policy-and-compliance-directive-047-01.

[58] *See* DHS INSTRUCTION 047-01-001 PRIVACY POLICY, AND COMPLIANCE, available at https://www.dhs.gov/publication/privacy-policy-and-compliance-instruction-047-01-001.

[59] *See* Privacy Act of 1974: Implementation of Exemptions; DHS/CBP-024 CBP Intelligence Records System (CIRS) System of Records, 82 Fed. Reg. 44124 (September 21, 2017), *available at* https://www.dhs.gov/system-records-notices-sorns.

contest its content may submit a Freedom of Information Act (FOIA) or Privacy Act request in writing.

If an individual requests information that may be maintained in the Intelligence Reporting System-Next Generation, a search will be conducted of the system. When seeking records about oneself from this system of records or any other CBP system of records, the request must conform to the Privacy Act regulations set forth in 6 CFR Part 5. An individual must first verify their identity, meaning they must provide full name, current address, and date and place of birth. The request must include a notarized signature or be submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, forms for this purpose may be obtained from the Director, Disclosure and the Freedom of Information Act, https://www.cbp.gov/site-policy-notices/foia, or 1-866-431-0486.

In addition, the following should be provided:

- An explanation of why the individual believes the Department would have information on them;
- Details outlining when they believe the records would have been created; and
- If the request seeks records pertaining to another living individual, it must include a statement from that individual certifying their agreement for access to their records.

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

Because portions of this system are exempt from the Privacy Act's individual access and amendment provisions, individuals have limited opportunities to correct inaccurate or erroneous information. Access to the records contained in this system of records could inform the subject of an investigation of the existence of that investigation or reveal investigative or law enforcement interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede law enforcement, the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

However, the data accessed by the Intelligence Reporting System-Next Generation from source systems may be corrected by means of the processes described in the Privacy Impact Assessments for those systems. Intelligence Reporting System-Next Generation users are required to take action to correct the data if they become aware of inaccurate data. Workspaces are dynamic, and information can change as new information is discovered and investigations or projects expand. In some cases, the Intelligence Reporting System-Next Generation receives updates from source system databases, but these updates are often not in near real-time. If users are aware of information that has changed in source systems, they should recall previously issued intelligence reports and informational products and create new intelligence reports and informational products to correct inaccurate information. For any intelligence reports and informational products that were externally disseminated and need recall or correction, a recall message or revised product will be disseminated to the recipients of the original product(s) with appropriate instructions.

As noted in Section 7.1 above, any requests from the public for information in the Intelligence Reporting System-Next Generation will be reviewed on a case-by-case basis.

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

Notification of the procedures for individuals to request access to and amendment of records contained in the system is provided through the publication of this Privacy Impact Assessment, as well as through the System of Records Notice for the CBP Intelligence Reporting System and each System of Records Notice published for the source systems from which the Intelligence Reporting System-Next Generation accesses information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that the Intelligence Reporting System-Next Generation does not provide individuals with an opportunity to access, review, and correct intelligence reports and informational products (finished or in-progress) that contain information about them.

Mitigation: This risk is partially mitigated. Given the heightened sensitivity of the intelligence reports and informational products generated in the Intelligence Reporting System-Next Generation and the potential harm to government activities that providing such access may cause, this risk cannot be completely mitigated. While individuals will not have a formal mechanism for access or redress within the system, individuals may correct inaccuracies in the source systems, the processes for which have been made public in the source systems' Privacy Impact Assessments and System of Records Notices. If information is changed in a source system that impacts information in the Intelligence Reporting System-Next Generation or any intelligence product that has been published via the Intelligence Reporting System-Next Generation or the Analytical Framework for Intelligence, CBP will pull that published report and correct the information.

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?

Intelligence Reporting System-Next Generation records the search activities of all users and performs extensive auditing to mitigate any risk of authorized users conducting searches for inappropriate purposes. Intelligence Reporting System-Next Generation controls account access by passing individual user credentials to the originating system or through a previously approved certification process in another system to minimize the risk of unauthorized access. When a user conducts a search, the Intelligence Reporting System-Next Generation will only display those results that an individual user has permission to view in the source system. In addition, each intelligence report or an informational product created in the Intelligence Reporting System-Next Generation is reviewed by a peer and a supervisor to ensure completeness and quality.

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

CBP and all Intelligence Reporting System-Next Generation users are required to complete annual training in privacy awareness to understand how to handle Personally Identifiable Information. All authorized CBP personnel undergo additional privacy training required of all CBP employees with access to CBP's law enforcement systems. This training is regularly updated. Users who do not complete all required training will lose access to all computer systems, which are integral to their duties. Additionally, CBP issued training specific to intelligence research and reporting activities, focusing on law enforcement authorities, the First and Fourth Amendments, the Privacy Act, and civil rights and civil liberties considerations. This training is delivered on an ad-hoc basis.

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

Through CBP's entitlement system, users are provisioned with different Ports, Units, and roles in accordance with their access needs. For example, a user may only be provisioned to workspaces within their Port and, therefore, not be able to access other workspaces generated at other Ports. Access is granted through a two-tier process through which the user's supervisor approves the access request. Then a second-level approver also reviews and approves (or denies) the access request. A user must provide a valid justification for the access request. Access is reassessed every six months, during which a supervisor can choose to renew or revoke such access.

In addition, users can add workspace restrictions that could disallow access to users at the discretion of the workspace's owner. Access to data in the Intelligence Reporting System-Next Generation is controlled via the user's access to source systems such as TECS and the Automated

Targeting System. Users who do not have access to data in source systems would not see data in the Intelligence Reporting System-Next Generation.

Access to the Intelligence Reporting System-Next Generation is controlled through user roles. The system has many ports and units. By provisioning a user to a specific port(s) and unit(s), management can limit the Workspaces to which the user has access. Users may have access to several ports and units with different sets of roles in each.

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?

CBP considers requests from users outside of DHS to access the Intelligence Reporting System-Next Generation on a case-by-case basis. If an initial decision is made that access is appropriate, a written document will be prepared that outlines the restrictions and conditions of such access and is sent to the relevant CBP offices for review, including the CBP Office of Chief Counsel and the Privacy and Diversity Office.

Contact Official

Executive Director
National Targeting Center
Office of Field Operations

Responsible Official

Debra L. Danisek
CBP Privacy Officer
Office of the Commissioner
U.S. Customs and Border Protection

Approval Signature

Original, signed version on file with the DHS Privacy Office.

____

Roman Jankowski
Chief Privacy Officer
U.S. Department of Homeland Security
Privacy@hq.dhs.gov

Appendix: Applications

The Intelligence Reporting System-Next Generation contains a suite of applications for Intelligence gathering and dissemination. These applications streamline the analysis of gathered information regarding specific workflows such as apprehension interviews, identifying threat networks, collaboration with foreign partners, tracking hidden transnational tunnels, and reporting field leads.

Seizure and Apprehension Workflow (SaAW)

The SaAW application is an intelligence aggregator intended to promote collaboration, data augmentation, and information sharing as it relates to CBP Seizures and Apprehensions. SaAW is integrated with the Enforcement Integrated Database (EID)[60] and Unified Secondary[61] through which the application pulls into SaAW those events on a continual basis. Pulling the CBP EID and USEC data into SaAW allows a user to enrich and augment apprehension data by analyzing the entity data with other source system data that is used for analysis, investigation, and interviews.

Unlike a Workspace in the Intelligence Reporting System-Next Generation, SaAW is a transactional system with activities that are short lived. Extensive analysis on subjects, seizures, and events requires importing to a Workspace and continuing the analysis.

TNET

To streamline data collection and maintain data integrity and accuracy, TNET is established as the single source to populate and visualize CBP threat networks. The TNET application is not a data entry system. It is a threat network analysis and visualization tool. Threat network data entry and associations are done in the source targeting application, such as the Intelligence Reporting System-Next Generation, Unified Secondary, or Unified Passenger

[60] The Enforcement Integrated Database is a DHS shared common database repository used by several DHS law enforcement and homeland security applications. EID stores and maintains information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations and operations conducted by ICE, USCIS, and CBP. *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 (2019 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-ice.

[61] As part of this mission, CBP conducts inspections of travelers and their belongings at the border. While some travelers are processed during what is referred to as “primary” inspection, others are referred for additional scrutiny, which is a continuation of the border inspection known as “secondary” inspection. This approach enables CBP to facilitate traveler processing. CBP developed Unified Secondary, a module under the Automated Targeting System, as a consolidated secondary processing system that handles the secondary inspection process from referral to resolution. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR UNIFIED SECONDARY, DHS/CBP/PIA-067 (2020 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

(UPAX),[62] and that data is brought into TNET via a TNET interface to those systems. TNET is a visualization tool that can organize and categorize criminal methods, techniques, illicit routes, and criminal operational information provided by source systems available in the Intelligence Reporting System-Next Generation to speed up the response to national threats. This gives analysts the ability to expand and view all possible affiliations across all networks. A dashboard can display a series of metrics, trends, maps, and timeline of activities for broad analysis.

Grupo Conjunto Inteligencia Fronteriza (GCIF)

GCIF is a multinational border intelligence group that includes a growing number of countries including Salvadoran, Guatemalan, Honduran, Mexican, and United States government personnel. The main purpose of GCIF is for CBP, sometimes in coordination with other government or state and local agencies, to gather information from participating countries to help identify suspected members of Transnational Organized Crimes.

When a CBP agent or officer has a subject of interest on which they need additional information, they will use the GCIF platform to send a Request for Information if they believe a GCIF country has information on the individual. If the information received back h is relevant to the case or potential product, the information collected on the individual will be added to an Intelligence Reporting System-Next Generation Workspace and the foreign data will be tagged accordingly.

Tunnel Entry

As efforts to strengthen security on our borders increase, criminals are forced underground to avoid detection and disruption. All transnational tunnels create viable means for smugglers to enter the U.S. and pose a potential threat to national security. CBP developed the Tunnel Entry Application within the Intelligence Reporting System-Next Generation to record the location and remediation of subterranean tunnels used to smuggle illicit contraband and humans into and out of the United States.

Field Leads and Observations (FLOW)

Field Leads and Observations (FLOW) is primarily used by CBP Air and Marine Operations and is intended to report and memorialize leads and observations derived from encounters, surveillance, or other activities conducted in furtherance of the CBP mission. Field Leads and Observations serves as a platform for officers and agents in the field to document and memorialize leads and observations in a structured, centralized, and searchable form. After the

[62] *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(e) (2017, Addendum 1.1), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

event is reviewed and approved by a supervisor, it may go into an Intelligence Reporting System-Next Generation Workspace for further analysis and reporting.