Privacy Impact Assessment

for the

Immigration Detention Case Management System

DHS Reference No. DHS/OIDO/PIA-001

June 21, 2021

Homeland Security

Abstract

The U.S. Department of Homeland Security's (DHS) Office of the Immigration Detention Ombudsman (OIDO or Office) is an independent office responsible for objectively and impartially reviewing cases submitted by, or on behalf of, individuals affected by potential misconduct, excessive force, violations of rights of individual detainees, or violations of law, standards of professional conduct, contract terms, policy related to immigration detention, or detention standards that occurred while in immigration detention by DHS officers, or other contracted, subcontracted, or cooperating entity personnel. Thereafter OIDO seeks to resolve the matter or provide redress as appropriate. The Office also provides independent oversight of immigration detention facilities, including conducting inspections, reviewing contract terms for immigration detention facilities and services, making recommendations, and reporting to Congress on findings. To accomplish its mission, OIDO will use the Immigration Detention Case Management System (ID-CMS) to manage, process, track, and respond to complaints and conduct investigations, and to maintain contact information of OIDO stakeholders and records related to the Office's external engagements. OIDO is conducting this PIA because ID-CMS requires collection of personally identifiable information (PII) and sensitive PII (SPII).

Overview

OIDO was established by Congress in Section 106 of the Consolidated Appropriations Act 2020[1] to enhance the Department's mission of securing our nation's borders. The Act outlined OIDO's core responsibilities:

- Establish and administer an independent, neutral, and confidential process to receive, investigate, resolve, and provide redress, including referral for investigation to the Office of Inspector General (OIG), referral to U.S. Citizenship and Immigration Services (USCIS) for immigration relief, or any other action determined appropriate, for cases in which Department officers or other personnel, or contracted, subcontracted, or cooperating entity personnel, are found to have engaged in misconduct or violated the rights of individuals in immigration detention;
- Establish an accessible and standardized process regarding complaints against any officer or employee of U.S. Customs and Border Protection (CBP) or U.S. Immigration and Customs Enforcement (ICE), or any contracted, subcontracted, or cooperating entity personnel, for violations of law, standards of professional conduct, contract terms, or policy related to immigration detention;
- Conduct unannounced inspections of detention facilities holding individuals in federal immigration custody, including those owned or operated by units of State or local

[1] Consolidated Appropriations Act 2020, Pub. L. No. 116-94, December 20, 2019.

government and privately-owned or operated facilities;

- Review, examine, and make recommendations to address concerns or violations of contract terms identified in reviews, audits, investigations, or detainee interviews regarding immigration detention facilities and services;
- Provide assistance to individuals affected by potential misconduct, excessive force, or violations of law or detention standards by DHS officers or other personnel, or contracted, subcontracted, or cooperating entity personnel; and
- Ensure that the functions performed by the Ombudsman are complementary to existing functions within DHS.

In order to fulfill those responsibilities, OIDO is creating ID-CMS to assist the Office in tracking and securely maintaining complaint information as well as data gathered through the investigation process.

Collection and Use of PII

Individual Complaints

Detainees, legal or other representatives, or other persons submitting cases on a detainee's behalf (e.g., family members) can submit complaints to OIDO directly to OIDO staff in a facility or via mail, email, fax, or telephone.[2] Information collected in person may be entered onto a paper form and then entered into ID-CMS. OIDO staff will scan and electronically retain paper forms in ID-CMS. Hard copies will be destroyed. Information submitted via mail, fax, and email will also be entered by OIDO staff into ID-CMS. Information collected by telephone will be entered directly into the system. In the future, the system will be integrated with a web portal that will connect with ID-CMS.

Once a complaint is entered into the system, the submitter, if permitted, will receive a unique case identification number to use as a reference for follow-up. OIDO will use the information collected to triage the complaint, reviewing for previous complaints related to the same detainee, as well as for proper consent, jurisdiction, and emergency circumstances. The information will also be used to verify information about the complaint in systems maintained by ICE, CBP, and other DHS headquarters offices. Once assigned for resolution, an analyst will review the data provided, conduct necessary background research about the complaint, and engage with DHS components (primarily ICE and CBP and their respective offices within) to come to a resolution. To facilitate this portion of the resolution process, information will be shared with DHS components and offices (and occasionally other Departments involved in the immigration process, including the Departments of State and Justice) for identification, verification, and corroboration

[2] ODIO also accepts complaints submitted anonymously. OIDO will handle anonymous complaints in the same manner it does for all other complaints; however, OIDO is unable to provide feedback in these cases.

purposes. OIDO will then communicate the result to the submitter of the complaint, to the extent appropriate. Upon resolution, the case will no longer be active in ID-CMS (though it can be reopened at any time if follow-up is required). Data in ID-CMS will be disposed of based on OIDO's Records Retention Schedule, which is currently under development. ID-CMS enables OIDO to categorize complaints into several categories, track interaction with government employees during attempts to resolve the complaint and generate internal reports.[3]

Investigations

OIDO will also conduct inspections of detention facilities based on a regular internal schedule, recommendations from leadership, trends in complaint records, or current events. In ID-CMS, the investigation team will record the triggering event(s) (e.g., complaint) and open a file. The circumstances of the event(s) will be reviewed to determine if an investigation is necessary. If so, OIDO staff will communicate with other offices (including DHS's Office of Inspector General and Office for Civil Rights and Civil Liberties and ICE's and CBP's Offices of Professional Responsibility) to ensure that no other team is already investigating the issue at the same time. Once this deconfliction is complete, OIDO will visit the facility to gather information, including, potentially, PII of individuals involved in the incident that led to the investigation. This information will be kept securely in ID-CMS and will be shared with facility staff as necessary. Any PII shared with facility staff will be information already in facility records, shared for identification purposes. Reports of OIDO's investigation findings will be shared with ICE and CBP for feedback, and updates made as necessary. When an investigation is complete, the report will be finalized, and all associated investigation records will be closed in ID-CMS. Records will be retained in accordance with the approved records retention schedule, currently under development, but will be retained indefinitely pending such approval by the National Archives and Records Administration (NARA). PII included in reports shared with ICE, CBP, or other DHS offices will be redacted from any publicly issued reports or recommendations issued by the Ombudsman.

External Relations

OIDO will also use ID-CMS to collect and maintain contact information for the Office's stakeholders, including local, state, and federal officials, non-governmental organizations and advocacy groups, and private companies that own and staff federal immigration detention facilities. ID-CMS will also keep information about events and engagements conducted and attended by OIDO staff, such as dates, locations, participants, and subject matter covered.

[3] Any complaints received by OIDO that do not fall within its purview, or that OIDO determines not to investigate, may be referred by OIDO to the appropriate DHS or outside government agency with any confidentiality protections deemed necessary, and in accordance with this PIA and applicable SORNs.

Reporting and Metrics

ID-CMS also supports the creation of charts, graphs, and customized reports based on complaint and investigation data. This information is aggregated and does not include PII. OIDO uses these products to provide feedback and recommendations to the Department, and ICE and CBP specifically. The information will also be used for policy recommendations and the Ombudsman's required annual report to Congress. ID-CMS also provides aggregated metrics and statistics to assist OIDO in understanding and improving office workflow and efficiency.

Technology and Access Controls

ID-CMS was developed in collaboration with DHS's Office of the Chief Information Officer (OCIO) Solutions Development Directorate (SDD) Business System Branch (BSB) using Microsoft Dynamics 365 in the DHS HQ Government Community Cloud (GCC) with minimal customizations.

ID-CMS is accessible only on the DHS network and uses Windows integrated authentication. The records are accessible using role-based access. ID-CMS utilizes separate modules to facilitate OIDO's responsibilities. The Complaint Module allows for intake of individual complaints. The Oversight Module is used for conducting facility inspections and reviews. Each module has tailored security roles and permissions such as ID-CMS Admin and ID-CMS Analyst to ensure only those with a need-to-know have access to certain data within modules. Future development will include a web-based portal for submitters to file complaints directly with OIDO online.

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 Office of the Immigration Detention Ombudsman was established by Congress in Section 106 of the Consolidated Appropriations Act of 2020, Pub. L. No. 116-93. The legislation states that the Ombudsman shall "establish and administer an independent, neutral, and confidential process to receive, investigate, resolve, and provide redress … for cases in which Department officers or other personnel … are found to have engaged in misconduct or violated the rights of individuals in immigration detention." ID-CMS is the mechanism that the Office will use to store and review data received in the form of complaints from the public. Efforts to resolve complaints with ICE and CBP and to provide redress to detainees (including emails, records of telephone conversations, and other outreach) will also be recorded in the system.

Further, the legislation requires that the Ombudsman "conduct unannounced inspections of detention facilities holding individuals in federal immigration custody" and "make recommendations to address concerns or violations of contract terms identified in reviews, audits,

investigations, or detainee interviews." Again, information gathered during these investigations and interviews will be maintained in ID-CMS.

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

The information collected from current or former detainees, legal or other representatives of the detainees, other persons submitting cases on a detainee's behalf (e.g., family members), or anonymous submitters, that is stored in ID-CMS, is covered on an interim basis by DHS/ALL-020 Department of Homeland Security Internal Affairs[4] and DHS/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security System of Records.[5] OIDO is also developing its own SORN to provide more fulsome transparency on the records OIDO maintains, the authority under which it collects the information, and the manner in which it shares any information externally.

The external stakeholder information collected is covered by DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System.[6] The information maintained to provision access to the system is provided by DHS/ALL-004 General Information Technology Access Account Records System (GITAARS).[7]

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

Yes. Microsoft Dynamics 365, the platform on which ID-CMS is hosted, has been granted an Authority to Operate (ATO). A system security plan (SSP) was completed as a requirement for the ATO package.

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

OIDO staff have met with NARA regarding retention schedules for OIDO records. OIDO is in the process of reviewing other department schedules to assist in the drafting of a schedule for the Office. Until a retention schedule is approved by NARA, these records are maintained indefinitely.

---

[4] *See* DHS/ALL-020 Department of Homeland Security Internal Affairs, 79 Fed. Reg. 23361 (April 28, 2014), *available at* https://www.dhs.gov/system-records-notices-sorns.
[5] *See* DHS/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security System of Records, 82 Fed. Reg. 27274 (June 14, 2017), *available at* https://www.dhs.gov/system-records-notices-sorns.
[6] *See* DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, 73 Fed. Reg. 71659 (November 25, 2008), *available at* https://www.dhs.gov/system-records-notices-sorns.
[7] *See* DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 Fed. Reg. 70792 (November 27, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.

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.

OIDO is currently working to have its intake form approved by OMB through the PRA process.

Section 2.0 Characterization of the Information

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

ID-CMS collects and maintains the following information about individuals filing a complaint – both the individual submitting it and the detainee/former detainee. In many cases, this will be the same person.

- Unique case identification number;
- Submitter's full legal name, including any aliases;
- Submitter's contact information, including mailing address, email address, phone number, and fax number;
- Law Firm/Organization if the submitter is an attorney or accredited representative;
- Detainee's full legal name, including any aliases;
- Detainee's A-Number;
- Detainee's contact information, including mailing address, email address, phone number;
- Detainee's sex;
- Detainee's transgender status;
- Detainee's date of birth;
- Detainee's Country of Birth and Country, or Countries, of Citizenship;
- Detainee's Detention History including facility name and dates detained;
- Incident Date;
- Complaint Description;

- Complaint Category (such as abuse, disability accommodation, language access, legal representation, personal property, medical concerns, or religious accommodation);
- Subject of the Inquiry (adult, family unit, or minor child, and names of other family members involved);
- Prior actions taken to remedy the problem;
- Consent of the detainee for OIDO to disclose information in the file to a designated representative, if applicable; and
- Verification statement signed and dated by the subject of the request or the authorized representative;

Submitters may offer more information than is specifically requested by OIDO. Such information may include PII such as Visa number or Passport number. Documentation provided to support complaints may also include legal and medical records or other records related to disability accommodations, personal property, and the conditions of detention.

ID-CMS collects the following information during a complaint investigation or facility inspection:

- Facility Standards;
- Investigation/Inspection Date;
- Investigation/Inspection Type;
- Investigation/Inspection Notes, including photographs and written and audio/video recordings of interviews with detainees and facility staff;
- Interviewee's full legal name and contact information including mailing address, email address, and phone number;[8]
- Interviewee's position/title and current duty station if they are a facility employee or contractor; and
- Detainee biographical information if an investigation is started due to a complaint submitted to OIDO. This includes all detainee information listed in the above complaint section.

[8] An interviewee could be a DHS employee, contractor, grantee, volunteer, or other individual acting under the authority of the Department alleged to be involved in any such violations or misconduct, or a third party directly or indirectly involved in the alleged incident and identified as a relevant person to an investigation.

Further, ID-CMS may contain information about DHS employees, contractors, grantees, volunteers, or others acting under the authority of the Department alleged to be involved in any such violations or misconduct, or on third parties directly or indirectly involved in the alleged incident and identified as relevant persons to an investigation. This information is generally collected during the course of an investigation but may be initially provided by the complainant.

Additionally, ID-CMS contains a list of names and email addresses for points of contact at ICE and CBP facilities. ID-CMS will also maintain information about the Office's stakeholders:

- Name and contact information including organizational affiliation, mailing address, email address, and phone number;
- Areas of interest; and
- Notes regarding engagements with OIDO, including dates, participants, types of engagements, reminders for future actions, and materials used or distributed.

ID-CMS also contains a list of OIDO personnel who are users of the system. User profiles are created to enable staff members to gain access to the system. The user profile contains the employee's work email address and full name, as well as data related to staff schedules and trainings.

ID-CMS is used to create charts, graphs, and customized reports based on complaint and investigation data. This information is aggregated and does not include PII. OIDO uses these products to provide feedback and recommendations to the Department, and to ICE and CBP specifically. The information will also be used for policy recommendations and the Ombudsman's required annual report to Congress. ID-CMS also provides aggregated metrics and statistics to assist OIDO in understanding and improving office workflow and efficiency.

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

OIDO will collect information from current or formers detainees, their representatives, other persons submitting cases on a detainee's behalf, or others whose identity or affiliation is unknown either in person or via paper forms submitted by mail, email, or fax; and by telephone. Eventually an online form will be added as a means to submit complaints. Additional information will be added to the complaint data in ID-CMS based on investigation and communication with ICE, CBP, or others involved in the DHS immigration detention process. Stakeholder data will be gathered from publicly available resources related to organizations working in the immigration detention field or in support of detainees (such as the organizations' websites). OIDO will use organizational data, rather than individual's data, when available. Individuals and groups that affirmatively contact OIDO will also be added.

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

OIDO does not use information derived from commercial sources. Publicly available information, including news reports, may trigger a facility inspection, and related data will be stored in ID-CMS. Publicly available information related to detainees will be noted as such in ID-CMS and verified to the extent possible through the case management and investigative processes. Publicly available data will also be used to identify organizations that may be stakeholders of the Office. The Office will contact them to let them know about OIDO's existence, purpose, and work product.

2.4 Discuss how accuracy of the data is ensured.

Individual case information is collected directly from complaints and input into ID-CMS by OIDO personnel. OIDO personnel do not alter the data collected due to the need to maintain the integrity of the information as it was received but may verify it with the submitter during this process. During the investigative processes, OIDO personnel verify information in ID-CMS against information in ICE, CBP, and other DHS headquarters systems for accuracy by comparing it with data held by those components. OIDO personnel may also correspond directly with detainees, their representatives, or other persons submitting cases on a detainee's behalf (e.g., family members) to verify information and resolve complaints. If OIDO determines that information received from submitters is false or inaccurate, personnel will update the ID-CMS record appropriately. Stakeholder data is gathered from stakeholders themselves or from professional websites.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that information collected from a submitter may be inaccurate.

Mitigation: This risk is partially mitigated. The risk of inaccurate information is reduced because OIDO personnel collect as much information as possible directly from the detainee or their representative. Notwithstanding efforts by OIDO personnel, this risk is inherent to any Government collection of complaints; therefore, OIDO does not use complaint information to ascertain whether the complaint is accurate as submitted. Rather, the collection is intended to provide submitters with an opportunity to share with OIDO as much information as they have based on their own observations or experiences of the potential violation or misconduct. OIDO does not make determinations or recommendations based on complaint information alone; it uses

that information to conduct its own investigation into the issue. If during the investigative process OIDO makes the determination that information received through a complaint is inaccurate, personnel will update the ID-CMS record appropriately.

Privacy Risk: There is a risk that information provided by an individual in person, via paper form, or over the telephone could be inaccurately entered into ID-CMS during the manual data entry process.

Mitigation: This risk is partially mitigated. There is always a risk of making manual mistakes during data entry, but OIDO personnel perform the same process of verifying accuracy whether information is submitted in person, or via mail, email, fax, telephone. Personnel will contact the submitter, as required, to resolve any inconsistences or typing errors both during the data entry phase and the investigation process. In the future, OIDO plans to integrate ID-CMS with a web portal that will allow submitters to submit complaints electronically and eliminate the potential for OIDO personnel to inaccurately transcribe information during the manual data entry process.

Privacy Risk: There is a risk of over-collection during the OIDO investigation process.

Mitigation: This risk is partially mitigated. OIDO requires information to identify individuals associated with both sides of a complaint, and their respective accounts of any incidents. OIDO also solicits a large amount of information through its intake form and process that may eventually be determined not to be germane to a complaint and subsequent investigation.

To mitigate this risk of over-collection, OIDO worked with the DHS Privacy Office and Office of General Counsel to determine the information needed to intake and process complaints. The information solicited on the intake form represents this collaboration. Additionally, the instructions on the intake form inform submitters that not all fields are required to be completed. Notwithstanding, complainants may provide more information that is necessary, in supplemental documents, for OIDO to conduct an investigation. Information collected is only used by OIDO personnel with a need-to-know and personnel only share the information necessary to conduct investigations.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

OIDO collects biographical data and complaint information to assist current or former detainees who are experiencing difficulty resolving a detention-related matter with ICE or CBP. Complaint information is used to identify detainees and the details about the conditions of their federal immigration detention. Information is also collected during the investigation process to determine the nature of submitted complaints and provide assistance or redress to those individuals as necessary.

Data provided and collected during investigations is also used to identify comprehensive challenges or trends in the DHS immigration detention process that need to be investigated. Additionally, OIDO collects information on specific facilities during investigations to determine if those facilities are meeting their required standards of care.

Information collected on and provided by OIDO's stakeholders will be used to communicate with appropriate individuals and groups to plan and conduct outreach and to share news and information about the Office.

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 specific technology is used to conduct electronic searches to determine predictive patterns beyond OIDO's own analysis of data from complaints and from materials supplied or collected during the investigation process.

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

ID-CMS is completely controlled and exclusively used by OIDO. No other components or directorates have access to its information, except for DHS OCIO admin and technical support. Information from the system will be shared via email and in person with ICE and CBP (as well as other DHS headquarters offices) in the form of inquiries as part of the investigation of individual complaints or broader facility inspection.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information in ID-CMS will be used in a manner beyond what is described in this PIA or beyond OIDO's mission and authorities.

Mitigation: This risk is mitigated. All OIDO personnel receive annual privacy and security control training, as well as training specific to ID-CMS providing necessary awareness of the functionality of the system as it pertains to the secure processing, storage, and retrieval of information. Access to ID-CMS is permitted only through a DHS HQ network account. Access is controlled through a strict access provisioning process on to those with a need-to-know within OIDO and all records are restricted as necessary using role-based access. Tailored security roles and permissions include those such as ID-CMS Administrator and ID-CMS Analyst.

Further, ID-CMS allows for the auditing and tracking of every user action taken within the system. All actions taken regarding complaints and investigations are tracked and logged for security control and continuity of operations. All correspondence back to a detainee,

representative, or facility point-of-contact is tracked and logged.

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.

A Privacy Act Statement will be available to submitters at the point of collection on the paper intake form and, on the form that in the future will be made available for submission via the DHS webpage. Call operators will also provide the Privacy Act Statement to those individuals who submit information via phone. The Privacy Act Statement addresses OIDO's authority to collect information, purpose of collection, routine uses of the information, and potential effects on the detainee of the collection. OIDO also provides general notice to individuals through the publication of this PIA, the associated SORNs outlined above, and the forthcoming OIDO-specific SORN. Additional information about the Ombudsman and its mission is available on the agency website.

In third-party complaint situations, the individual about whom the information is collected may only be notified about collection after OIDO contacts them to obtain more information regarding the complaint. Individuals who are interviewed by OIDO personnel but are not submitters of or detainees related to a complaint receive notification during the investigation process.

Because of the nature of ODIO's mission and the process by which the Office collects information, it is not always feasible to provide notice to individuals at the time their information is input into the system. When OIDO personnel interact with individuals in connection with a complaint, however, those individuals are generally aware that their information will be recorded and stored. Personnel also directly inform individuals, when appropriate, that the information they provide will be recorded and stored.

Stakeholders whose information is gathered from publicly available sources may not be notified before being entered into ID-CMS. That information will be used only for initial contact.

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

OIDO assists individuals who are unable to resolve problems directly with ICE or CBP regarding some aspect of their immigration detention. To receive assistance with a complaint, individuals may submit information to OIDO. Prior to providing their information, detainees and their representatives or other persons submitting cases on a detainee's behalf (e.g., family members) will be made aware via a Privacy Act Statement that providing their information is

voluntary; however, not providing it may prevent the individual from receiving assistance from OIDO. The intake form specifically asks submitters to provide consent for OIDO to conduct any investigation and share information as necessary.

During the course of its investigations, OIDO collects information from CBP, ICE, and other entities involved in the immigration detention process. Those agencies may be required to provide notice by statutory mandate at the time of collection. As such, individuals may not have an opportunity to decline to provide the required information, opt out, or consent to uses. During interviews with those associated with a complaint, individuals may have the opportunity to consent or decline depending on the nature of the investigation. OIDO personnel undergo training on interviewees' rights and obligations in the context of responding to complaints.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not know their information is maintained in ID-CMS.

Mitigation: This risk is partially mitigated. This PIA, in conjunction with the applicable SORNs, provides some notice about the information OIDO maintains and uses. OIDO also provides detainees, their legal representatives, and/or other persons submitting cases on a detainee's behalf (e.g., family members) with a Privacy Act Statement before they submit any information to OIDO. All actions taken are with the individual's knowledge and consent that the information provided will be shared with other DHS offices. Stakeholders whose contact information is added to ID-CMS without their knowledge are companies and organizations in the immigration detention field whose publicly available information is gathered from their own websites. Stakeholder information will be removed from OIDO's database upon request or when indicated that the stakeholder or their organization does not want further correspondence with DHS.

The nature of the OIDO's mission, however, may make it infeasible or inappropriate to provide notice to individuals at the time their information is input into the system. For example, a submitted complaint may contain information about individual CBP or ICE personnel. OIDO is unable to provide notice to that employee at the time of collection, but they would likely become aware when OIDO begins investigating and interviewing those associated with the complaint.

Privacy Risk: There is a risk that submitters may not know their information will be shared with CBP, ICE, or other DHS offices.

Mitigation: This risk is mitigated. The OIDO intake form asks for specific consent from individuals for OIDO to conduct an investigation on the detainee's behalf and share information as necessary to conduct that investigation. Consent will also be required during other intake processes, such as by phone.

Section 5.0 Data Retention by the Project

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

OIDO staff have met with NARA regarding retention schedules for OIDO records. OIDO is in the process of reviewing other department schedules to assist in the drafting of a schedule for the Office. Until a schedule is developed, no records will be destroyed.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information submitted via mail, email, or fax could be retained after the data has been entered into ID-CMS.

Mitigation: This risk is mitigated. Standard procedures have been implemented to destroy submissions after data entry. Staff will receive regular training on these procedures and the ID-CMS Product Owner will ensure adherence to this requirement.

Privacy Risk: There is a risk that information maintained in ID-CMS will be retained longer than necessary.

Mitigation: This risk is currently unmitigated. Until a records retention schedule is developed and approved, ID-CMS records will be retained indefinitely. Once that retention scheduled is approved, ID-CMS will be able to automatically archive and remove records based on the records retention rules that are established.

Section 6.0 Information Sharing

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

OIDO may share complaint information with the Department of Justice or Department of State if components of those departments may be able to assist with a detainee's immigration-related concerns. Information may be shared if it is relevant to litigation. Information may also be shared with the Department of Health and Human Services' Office of Refugee Resettlement (HHS-ORR) and the United States Marshals Service, as those entities are also involved in the detention of immigrants in the United States. Similarly, data sharing may occur with state and local law enforcement entities (primarily state detention facilities) and private sector facilities that the Federal Government contracts with for immigration detention.

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

OIDO is currently developing its own SORN. In the interim, coverage is provided by the DHS/ALL-020 Department of Homeland Security Internal Affairs SORN, which allows for the collection and maintenance of records concerning internal affairs matters, specifically internal integrity or disciplinary inquiries, as well as internal reviews, inspections, or investigations. This SORN is intended to cover records required to support and protect the integrity of Departmental operations; to ensure compliance with applicable laws, regulations, and policies; and to ensure the integrity of DHS employees' conduct and those acting on behalf of DHS. Interim SORN coverage is also provided by DHS/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security System of Records, which covers the collection and maintenance of records used "to pursue criminal prosecution or civil penalty action against individuals or entities suspected of offenses that may have been committed against property owned, occupied, or secured by DHS or persons on the property."

For example, during the course of an investigation, OIDO may need to share information with another federal, state, or local agency involved with an individual complaint. In this situation, the OIDO would share the minimal amount of information necessary to the outside entity to further the investigation. The information sharing is this example would be compatible with Routine Use G of the DHS/ALL-020 Internal Affairs SORN.

6.3 Does the project place limitations on re-dissemination?

Beyond DHS, information will only be shared with other offices dealing with immigration issues, such as those within the Departments of Justice, State, and Health and Human Services. Those agencies handle any information shared in accordance with their own SORN(s).

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

ID-CMS itself does not share information outside the Department directly. Any external sharing is typically done through email, orally during briefings, interviews, official requests, and by telephone with other entities, chiefly other federal agencies and third parties with a need-to-know. OIDO supervisors approve all external sharing prior to any external dissemination. An accounting of external disclosures is documented within the ID-CMS records for the associated complaint.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information in ID-CMS will be inappropriately shared

with external recipients.

Mitigation: This risk is mitigated. Information may be shared with recipients outside DHS when sharing is aligned with the purpose for which the information was collected. ID-CMS users receive annual training addressing the safeguarding of information through IT security and integrity awareness, as well as privacy awareness. OIDO supervisors must approve all sharing prior to any external dissemination and ID-CMS will retain an accounting of all external sharing for auditing purposes.

Section 7.0 Redress

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

Individuals may seek notification of and access to any OIDO record contained in ID-CMS, pursuant to procedures provided by the Freedom of Information Act (FOIA) and access provisions of the Privacy Act of 1974 at https://www.dhs.gov/freedom-information-act-foia, or by mailing a request to:

Office of the Immigration Detention Ombudsman
Privacy Act/FOIA
U.S. Department of Homeland Security
Mail Stop 0134
Washington, D.C. 20593

Requests for information are evaluated to ensure that the release of information is lawful; will not impede an investigation of an actual or potential criminal, civil, or regulatory violation; and will not improperly reveal the existence of an investigation or investigative interest on the part of DHS or another agency.

Further information about how to contact OIDO is available at https://www.dhs.gov/office-immigration-detention-ombudsman.

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

Individuals are able to correct inaccurate or erroneous information provided to OIDO throughout the intake and investigation process. Individuals can inform OIDO of inaccurate information when a complaint is submitted and any time thereafter. A person who believes that OIDO's actions are the result of incorrect or inaccurate information may request information about his or her records pursuant to procedures provided by FOIA. U.S. citizens, lawful permanent residents, and individuals who have records covered under the JRA who believe that OIDO's actions are the result of incorrect or inaccurate information may request correction of that data

under the amendment provisions of the Privacy Act of 1974 through the procedures outlined above. OIDO will review all requests for correction and amendment on an individual basis.

Individuals may also correct erroneous information in their record by contacting OIDO by telephone, email, fax, or mail.

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

OIDO will send a confirmation notification to submitters indicating receipt of their information and providing the office's contact information. Currently this is done via email or mail. Future development may include notification through text messages or mobile application. Submitters may contact to OIDO at any time to update or correct information related to a case. Other individuals such as stakeholders, component points of contact, and staff members will have the contact information for their associates at OIDO to update their information at any time. Additionally, notification is provided through this PIA, the forthcoming OIDO SORN, Privacy Act Statement on the intake form, and the OIDO portion of the DHS website.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that detainees or their representative will not know how to gain access to their information, how to correct it, and where redress is provided.

Mitigation: This risk is mitigated. Information about how to reach the Office is easily available on the OIDO website, as well as on the complaint intake form, the notification confirming OIDO's receipt of the complaint, and through this PIA. In addition, OIDO is publishing its own SORN that will further outline notification, access, and redress provisions.

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?

OIDO ensures that the practices stated in this PIA comply with federal, DHS, and OIDO policies and procedures through various measures including standard operating procedures, orientation and training, rules of behavior, and auditing and accountability procedures.

ID-CMS allows for the auditing and tracking of every user action taken within the system. Additionally, all actions taken regarding complaints and investigations are tracked and logged for security control and continuity of operations. All correspondence back to a detainee, representative, or facility point-of-contact is tracked and logged.

ID-CMS access is restricted to OIDO personnel with a valid DHS HQ network account and need-to-know. ID-CMS will have different user roles based on the user's assigned duties.

Administrative staff will be assigned to answer phone calls and other correspondence and review form submissions. They will complete the initial intake of the data into ID-CMS. These users will only have access to create complaints. Case Managers and Analysts will review and process complaints and have access to edit and review all complaints. The ID-CMS Product Owner administers and provides oversight for ID-CMS.

Junior Auditors will be responsible for the initial intake of investigations. They, and the Investigators and Subject Matter Experts, will have access to edit any investigation assigned to them. Managers will have access to all investigations.

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

All federal employees and contractors, including OIDO staff, are required to complete annual privacy and security awareness training. DHS's Privacy Awareness training addresses appropriate privacy concerns including Privacy Act obligations. The Information Security Awareness training also examines appropriate technical, physical, personnel, and administrative controls to safeguard information. In addition, OIDO conducts internal training specifically focusing on the use of ID-CMS, providing necessary awareness of the functionality of the system as it pertains to the secure processing, storage, and retrieval of information.

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

Access to information contained in ID-CMS is provided on a need-to-know basis, which is determined by the users' respective responsibilities and granted by ID-CMS Administrator or OIDO supervisors. OIDO personnel with a valid need-to-know will be granted access to ID-CMS to assist with complaints or investigations, consistent with the office's statutory mission. Once it is determined that personnel no longer have a need-to-know (e.g., separation from the office, change of role), their access is immediately revoked.

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?

Any Memoranda of Understanding (MOU), Memoranda of Agreement (MOA), and similar agreements are reviewed by the ID-CMS Product Owner and senior OIDO personnel, as appropriate, before being forwarded as needed to other DHS headquarters offices (e.g., Privacy Office, Office of General Counsel) for a formal review.

OIDO is currently developing agreements with the other stakeholders involved in this

process. These agreements will discuss the deconfliction process for complaints as well as the necessary confidentiality provisions when sharing data.

Contact Official

Carla Fall
Chief of Case Management
Office of the Immigration Detention Ombudsman
carla.fall@hq.dhs.gov

Responsible Official

David Gersten
Ombudsman (Acting)
Office of the Immigration Detention Ombudsman
david.gersten@hq.dhs.gov

Approval Signature

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

_____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717