Privacy Impact Assessment

for the

TeamMate Application

DHS Reference No. DHS/OIG/PIA-004

May 9, 2024

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) Office of Inspector General (OIG) is responsible for conducting and supervising independent and objective audits, inspections, evaluations, and investigations to prevent and detect fraud, waste, and abuse and promote economy, effectiveness, and efficiency within DHS programs and activities. The OIG carries out these functions via the strategic programs of the Office of Audits and the Office of Inspections and Evaluations. TeamMate is a Windows based audit management application installed on OIG servers located at OIG's primary data center. TeamMate provides an internal common platform for documenting, sharing, reviewing, and tracking work throughout the lifecycle of an audit, inspection, and/or evaluation of a DHS program or activity (not individuals). Auditors and Inspectors collect and process information in the form of work papers, interviews, and on-site visits during audits, and/or inspections/evaluations. Information collected during an audit or inspection/evaluation is scanned or uploaded into OIG's TeamMate. Auditors and Inspectors may request and receive personally identifiable information (PII) and sensitive PII (SPII) during an audit, inspection, and/or evaluation, when needed and relevant to the review. This personally identifiable information and sensitive PII may be included, for example, in supporting documents provided to OIG or obtained through OIG's factfinding.

Overview

DHS OIG conducts audits, inspections, and/or evaluations on DHS programs and activities, not on individuals. To support the audit, inspection, and/or evaluation, DHS Components provide data such as files, records, and reports in response to, among other things, OIG on-site visits and interviews. This information is provided to OIG auditors, inspectors, and data specialists. And while the audit, inspection, or evaluation is not directed at an individual, the information shared with OIG may contain PII.[1]

TeamMate is a Commercial Off the Shelf (COTS) application designed to provide a centralized location to collect, prepare, and maintain documentation related to audits, inspections, and evaluations pursuant to the Inspector General Act of 19785 U.S.C. §§ 401-424. All information located in TeamMate is stored within the application on the OIG network. Audits, inspections, and evaluations are stored as "projects" in TeamMate. Projects use the audit or inspection/evaluation project code as a unique identifier within TeamMate.[2] Access to the TeamMate system must be granted by TeamMate administrators. Access to the projects within

[1] For more information on DHS OIG, see Department of Homeland Security Management Directive System, MD Number 0810.1 (June 10, 2004), *available at* https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_0810_1_the_office_of_inspector_general.pdf.

[2] Project code is the unique identifier used to search for a project in TeamMate; the project title and report number may also be used.

TeamMate may be granted to and only by individuals on the project team. Data and documents associated with a project can only be viewed and shared by team members assigned to that project. No one outside of OIG is granted access to TeamMate.[3] Once a project is complete, its status is changed to "read only" as part of the finalization process. The finalized project is maintained within TeamMate according to established records management schedules.

The below types of information may be provided by DHS Components as part of an audit and/or inspection/evaluation. Additional information as part of an auditor's or inspector's research can be obtained from publicly available sources, such as public websites, news sources, Congress, and through interviews of DHS personnel and on-site visits conducted by the auditors or inspectors.

- Full Name (including aliases);
- Physical Address;
- Visa Number;
- Passport Information;
- Driver's License Number;
- A-Number;
- State ID number;
- Social Security Number;
- Bank Account Information;
- Credit Card and other Financial Information; and
- Tax Identification Number
- Any other information or PII/SPII necessary and relevant to an OIG audit or inspection/evaluation may be collected.

OIG may request PII/SPII, if it is relevant to an audit, inspection, or evaluation of a DHS program or activity. Also, PII/SPII may also be included in information provided by DHS in support of the OIG audit, inspection, or evaluation, e.g., supporting documentation or data.[4] PII/SPII is not included in the reports OIG issues to DHS or its Components, and OIG does not collect PII/SPII directly from the public as part of its audit or inspection/evaluation function. OIG disseminates

[3] Peer reviewers outside of OIG are granted Read-Only access to TeamMate project files as part of the External Peer Review Process for Audits. *See* further discussion on page 3 below.

[4] For instance, OIG may conduct an audit on a DHS program that provides support to individuals. Therefore, OIG would request information related to the program, not the individuals who receive support. In providing OIG with responsive information, however, the Component may provide PII/SPII that is relevant to the audit.

unclassified final reports on its public website and provides the report to DHS, relevant Components, and Congressional committees. However, working papers, data extracts, and other internal documentation obtained through the audit, inspection, or evaluation is not shared publicly and remains in TeamMate.[5]

OIG does not routinely share any information it collects and stores within TeamMate. One exception is during peer reviews,[6] which are completed to ensure OIG audits, inspections, and evaluations follow Government and internal OIG standards. Information that may be shared with the peer review team members include workpapers, meeting notes, and draft and final reports for completed audits, inspections, and evaluations. Additionally, Congressional requests for information and Freedom of Information Act (FOIA) requests may require OIG to provide information related to OIG audits, inspections, and evaluations, subject to applicable statutory exemptions. This information may include PII/SPII, which is handled in accordance with law and policy. The information and documents shared or provided varies based on the request.

Access to the OIG TeamMate application is only granted through the OIG Network. All DHS OIG TeamMate users must have an OIG network account to use TeamMate.

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 Inspector General Act of 1978, as amended, and the Homeland Security Act of 2002, as amended, permit the OIG to collect information necessary for the OIG to perform audits, inspections, investigations, and legal analysis on programs and operations within the Department. DHS Management Directive System MD Number 0810.14 states the roles and responsibilities of the Heads of U.S. Department of Homeland Security Organizational Elements (OE), Department

[5] For large data sets, the OIG Data Analytics Cloud System (DACS) is used to maintain the data. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF THE INSPECTOR GENERAL, PRIVACY IMPACT ASSESSMENT FOR THE OIG DATA ANALYTICS CLOUD SYSTEM, DHS/OIG/PIA-003 (2021), *available at* https://www.dhs.gov/privacy-documents-office-inspector-general-oig.

[6] External peer reviews for audits are required of an OIG that performs audits using generally accepted government auditing standards. The objective is to determine whether "the reviewed OIG's system of quality controls for the audit function was suitably designed[,] and whether the OIG is complying with its system of quality control to provide it with reasonable assurance of conforming with applicable professional standards and legal and regulatory requirements in all material respects." *See* https://www.ignet.gov/content/ig-peer-reviews. External peer reviews for Inspections and Evaluations are "required of (OIGs that issue reports in accordance with the Council of the Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation during the appropriate 3-year period. The objective is to assess whether an OIG's Integrity and Efficiency organization's internal policies and procedures are consistent with the standards and whether its reports and associated or supporting project documentation comply with those standards and the Integrity and Efficiency organization's associated internal policies and procedures." *See* https://www.ignet.gov/sites/default/files/files/FinalIEEPeerReviewGuideDec2021.pdf.

of Homeland Security employees, and the OIG in collecting and providing any files, records, reports, or other information that may be requested either orally or in writing.

As the Department's oversight component for preventing fraud, waste, and mismanagement, the OIG and divisions within OIG's Office of Audits and Office of Inspections and Evaluations are tasked with auditing, inspecting, and evaluating DHS programs. Through this authority, OIG audit, inspection, and evaluation teams collect information from DHS specific to the audit or inspection/evaluation being performed.

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

A significant portion of the information that TeamMate uses and maintains is provided by DHS or its Components. The DHS or Components' source systems perform the original collection and, thus, are covered by the individual System of Records Notices for those systems. DHS and Component data remains covered by these source systems' System of Records Notices until it is processed or incorporated into an OIG audit, inspection, or evaluation report.

The DHS/OIG-002 Investigative Records System of Records Notice[7] covers the information and records the OIG processes during its audits, inspections, and evaluations and incorporates into its reports. This System of Records Notice also covers the collection of information from other government agencies, and publicly available sources, which may include commercially available information and social media information, relevant to OIG audits, inspections, and evaluations.

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

TeamMate is an application maintained on the Homeland Security Inspector General Network (HSIGN) General Support System (GSS), and uses the Security Plan from HSIGN which has been in Ongoing Authorization status since September 2014.

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

The project files created and maintained in TeamMate, both for the Office of Audits and the Office of Inspections and Evaluations, are governed by OIG retention schedule N1-563-09-10.[8] In accordance with NARA regulations and the retention schedule, OIG Audit, Inspection, and Evaluation reports are transferred to NARA five years after the audit, inspection, or evaluation has

[7] *See* DHS/OIG-002 Investigative Records System of Records, 86 Fed. Reg. 58292 (October 21, 2021).
[8] *See* DHS OIG NARA Retention Schedule #N1-563-09-10, *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/n1-563-09-010_sf115.pdf.

been closed out. Supporting documentation and workpapers are eligible for destruction or deletion after 15 years; however, prior to deletion, a review is completed to determine if OIG will retain a specific audit, inspection, or evaluation report and supporting documentation as reference material.

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

The information in TeamMate is not covered by the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

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

Information collected by OIG and maintained in TeamMate pertains to DHS and generally is provided by the Component being audited, inspected, or evaluated. The information is used for audits, inspections, or evaluations to ensure there is no fraud, waste, abuse, and/or mismanagement of the program under review. As part of these audits, inspections, and evaluations, the below information may be collected from DHS and/or its Components and used for the audit/inspection/evaluation. Additional information as part of an auditor's or inspector's research can be obtained from publicly available sources, such as public websites, news sources, Congress, and through interviews of DHS personnel and on-site visits conducted by the auditors or inspectors.

- Full Name (including aliases);
- Physical Address;
- Visa Number;
- Passport Information;
- Driver's License Number;
- A-Number;
- State ID number;
- Social Security Number;
- Bank Account Information;
- Credit Card and other Financial Information;

- Tax Identification Number; and
- Any other information or PII/SPII necessary and relevant to an OIG audit, inspection, or evaluation may be collected.

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

Information is collected from DHS and the Component(s) being audited, inspected, or evaluated. Additional information as part of an auditor's or inspector's research can be obtained from publicly available sources, such as public websites, news sources, Congress, and through interviews of DHS personnel and on-site visits conducted by the auditors or inspectors.

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. Information may be obtained from publicly available sources, if needed and relevant to the audit, inspection, or evaluation being conducted by OIG. This information is used to assist OIG with the audit, inspection, or evaluation. As noted, however, audits, inspections, and evaluations are focused on DHS programs or activities, not individuals; though, PII about individuals may be collected if directly relevant to the audit, inspection, or evaluation.

2.4 Discuss how accuracy of the data is ensured.

While the data collected by OIG is only as accurate as DHS and its Components records are, auditors and inspectors must assess and validate the reliability of the data.[9] The individual audit programs document the steps that are planned and ultimately taken to conduct the validation assessment. Auditors and inspectors may validate the data collected through corroboration with other evidence or conducting interviews of DHS personnel, for example. Additionally, validation may include tracing back the data from a sample of records to the source documentation to ensure they match.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the audit, inspection, or evaluation team will collect and maintain in TeamMate more information from DHS and/or its Components than is necessary for conducting the audit, inspection, or evaluation.

Mitigation: This risk is partially mitigated. OIG limits the data collected by scoping its

[9] *See* Government Auditing Standards: 2018 Revision Technical Update (April 2021), *available at* https://www.gao.gov/products/gao-21-368g.

information requests to only that data which is necessary and relevant to the audit, inspection, or evaluation being conducted. Prior to the start of an audit, inspection, or evaluation, an entrance conference is held between OIG auditors/inspectors and the DHS Component being audited, inspected, or evaluated. During the entrance conference, the Rules of Engagement are discussed with DHS and/or Component representatives.

Generally, to assist with narrowing the risk of non-relevant PII/SPII being provided to OIG, prior to the start of OIG's work, OIG may request specific documents from DHS in support of the audit, inspection, or evaluation. If specific documents are unknown prior to starting the review and assessment, OIG may explain to DHS and/or the Components represented what the audit, inspection, or evaluation is trying to accomplish. Thereafter, DHS and/or the Components will provide documents or data that is relevant and necessary to the audit, inspection, or evaluation, which could include PII/SPII if the Component determines that the PII/SPII is necessary and relevant information.

If certain documents are withheld from OIG because purported unnecessary and irrelevant PII/SPII is included therein, or for other reasons, OIG may meet with DHS and/or the Component personnel s to assess the need for the PII/SPII and/or the other information being withheld. If the PII/SPII or the other information is neither relevant nor necessary to OIG's audit, inspection, or evaluation, the PII/SPII and/or other information may be redacted by DHS and/or the Component prior to sharing the document or data with OIG. DHS and/or the Component will then provide an accounting or a list summarizing data elements that were redacted. This is an important mitigation measure to prevent the over-collection of PII/SPII by OIG.

The initial scope of information to be provided by DHS and Components will be defined according to the audits, inspections, and/or evaluations that are planned by OIG. This scope may expand depending on OIG's findings or if the audit, inspection, or evaluation results in a referral for investigation. Notwithstanding, only information that OIG or the Components determined is relevant and necessary to the inquiry is requested by OIG and maintained in TeamMate.

Privacy Risk: There is a risk that inaccurate data may be provided by DHS and/or the Component and maintained in TeamMate.

Mitigation: This risk is partially mitigated. To ensure accuracy of the information provided to OIG, OIG validates the data not only through testing and interviews with DHS personnel during the course of the audit, inspection, or evaluation, but also through tracing the data from a sample of records back to the source documentation to ensure they match. Finally, if OIG determines that data is inaccurate during the course of its audits, inspections, and/or evaluations, DHS and/or the Component are informed of those inaccuracies and OIG may not rely on the data in its audit, inspection, or evaluation.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

TeamMate maintains information collected by OIG in an audit, inspection, or evaluation from DHS. TeamMate is used internally by OIG auditors and inspectors as a collaboration tool to centrally store related workpapers.

The information obtained during the audits, inspections, and evaluations is used to ensure Component programs are being managed properly; there is no misuse or waste of Department resources or funds; and there is no fraudulent activity occurring.

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.

TeamMate is the Office of Audits' and the Office of Inspections and Evaluations' primary management application used when conducting audits, inspections, and evaluations of DHS programs or activities. This application does not connect to any internal or external database. Searches for project information within TeamMate are limited to an OIG TeamMate user searching for the audit, inspection, or evaluation project using the project code, project title, or report number assigned to it.

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

OIG's TeamMate application is not used or accessed by any other DHS Components. With the exception of external peer reviews, TeamMate is only used by OIG personnel with access to the OIG network and the TeamMate application.

3.4 <u>Privacy Impact Analysis</u>: Related to the Uses of Information

<u>Privacy Risk</u>: There is a risk of improper use of or access to information within TeamMate.

<u>Mitigation</u>: This risk is mitigated. Access to the TeamMate application leverages Least Privileged and role-based access controls, which is based on assignments to an ongoing OIG audit, inspection, or evaluation. Least Privileged and role-based controls are used to manage who has access to the application and the projects within TeamMate. Except for external peer reviewers, OIG users that are not part of the Office of Audits or the Office of Inspections and Evaluations do not have access to TeamMate. The Inspector General, OIG Audit Managers, the Assistant and Deputy Inspector General for Audits, the OIG Inspections Managers, and the Assistant and Deputy Inspector General for Inspections are granted access to TeamMate to review, approve, and sign final audit, and inspection/evaluation reports.

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.

OIG provides notice to the public through this Privacy Impact Assessment and the OIG Investigative System of Records Notice. However, because TeamMate maintains potentially sensitive information related to audits and inspections/evaluations, it is not always feasible or advisable to provide notice to individuals at the time their information is collected.

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

Information within TeamMate is primarily obtained directly from DHS to support OIG audit and inspections/evaluations. OIG auditors and inspectors do not request PII/SPII from the public. Therefore, it is not possible for OIG to notify individuals and provide them with the opportunity to decline/opt out of their PII/SPII being shared with OIG.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not know that their information is shared with OIG and maintained in TeamMate.

Mitigation: The risk is partially mitigated. This Privacy Impact Assessment and the very nature of OIG's responsibilities (outlined in publicly available information about the OIG[10]), provide notice of TeamMate and the collection and maintenance of this type of information. The DHS/OIG-002 Investigative Records System of Records Notice also provides notice of the information and records the OIG processes during its audits, inspections/evaluations. Additionally, source system collections require notice provisions such as Privacy Act Statements and Privacy Notices, as applicable, when collecting information. However, because OIG relies on notice provisions of the source systems, individuals may not know that their information is shared with OIG and maintained in TeamMate.

Section 5.0 Data Retention by the Project

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

Retention of records within TeamMate is governed by OIG records retention schedule N1-563-09-10. The National Archives and Records Administration approved records retention schedule covers records related to OIG Audit and Inspection reports, supporting documentation

[10] *See* https://www.oig.dhs.gov/.

and workpapers, OIG correspondence, policy and procedural guidance, and other records maintained by various OIG components. Excluded are OIG Investigative case files and the Enforcement Data System, which are covered under N1-563-07-5.

In accordance with NARA regulations and the retention schedule, OIG Audit, Inspection, and Evaluation reports are transferred to NARA five years after the audit, inspection, or evaluation has been closed out. Supporting documentation and workpapers are eligible for destruction or deletion after 15 years; however, prior to deletion, a review is completed to determine if OIG will retain a specific audit, inspection, or evaluation report and supporting documentation as reference material.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information in TeamMate will be retained longer than the retention schedule.

Mitigation: This risk is mitigated. As indicated, final reports are transferred to NARA five years after the audit, inspection, or evaluation has been closed out, and supporting documentation/workpapers are eligible for destruction or deletion after 15 years. Prior to any destruction of documentation, however, there may be a determination to keep supporting documentation as reference material. To ensure any information maintained in TeamMate is protected, not only such information kept as reference material but all documentation associated with a project, OIG implements controls restricting access to the information in TeamMate related to a completed audit, inspection, or evaluation. A TeamMate application administrator may grant an OIG TeamMate user access to a closed project only if the OIG user has a need to access and review the information. Thus, any documentation maintained, either for the duration of the retention period or after if being used for reference material, can only be accessed by those individuals with a valid need-to-know.

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.

Information collected by OIG and stored in TeamMate is used internally for team collaboration during audits and inspections/evaluations. Audit and inspection/evaluation teams use this information, such as workpapers, for the creation of audit and inspection/evaluation reports. Reports are generated in Microsoft Word and imported into TeamMate. The final reports are created using Microsoft Word, converted to an Adobe PDF for digital signature, then saved as a PDF in TeamMate. Final reports are provided by email to DHS and/or the Component being audited, inspected, or evaluated. In addition, OIG may share final audit and inspection/evaluation reports with Congress when requested and as needed, and may publicly post unclassified, non-sensitive reports. These reports do not contain PII/SPII.

Additionally, peer reviews are periodically conducted on the Office of Audits' and Office of Inspections and Evaluations' policies, procedures, and final reports to ensure compliance with governing standards. During the peer review, members of the review team may request information from OIG that is maintained in TeamMate. This information is provided as requested. This information is only used as part of the peer review process and is not kept by the peer review team. If the peer review team does not have TeamMate or does not have the version of TeamMate OIG uses, OIG will provide the peer review team with software, known as a TeamEWP Reader, which allows the team to access the project. TeamEWP Reader is a part of the TeamMate products. OIG provides the installation for this software via email. Once the team has the reader software, OIG provides them with a copy of the relevant OIG project via email. OIG password protects the copy and separately sends the password to the team to access the project. The team then saves the copy to their laptops and uses the TeamEWP Reader to open and view the project. If the projects are too large to email, OIG uses Kiteworks, a secure and encrypted data transmission tool to transmit the files. Once the peer review is complete, the peer review team disposes of the provided information in accordance with appropriate Memoranda of Understanding (MOU).

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

Consistent with the OIG Investigative Records System of Records Notice, records maintained in TeamMate 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," and with peer review team members, as needed. As an example, information is shared in accordance with the following routine use:

> To the Council of the Inspectors General on Integrity and Efficiency (CIGIE) and other Federal agencies, as necessary, if the records respond to an audit, investigation, or review conducted pursuant to an authorizing law, rule, or regulation, and those conducted at the request of the CIGIE's Integrity Committee pursuant to statute.

6.3 Does the project place limitations on re-dissemination?

TeamMate does not place limitations on re-dissemination; however, auditees are provided with a copy of the draft report for technical comments and responses. Auditees are asked not to disseminate the draft copy of the report. This process is the same when the Office of Audits and/or the Office of Inspections and Evaluations are in a peer review.

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

For peer reviews that are conducted, which necessarily requires the sharing of information outside of the Department, a Memorandum of Understanding (MOU) is entered into between DHS OIG and the agency reviewing OIG's work. Copies of the MOUs are retained by DHS OIG. Such agreements detail the scope of the review which permits DHS OIG to account for the information that is required and shared.

Privacy Impact Analysis: Related to Information Sharing

<u>Privacy Risk</u>: There is a risk that information maintained in TeamMate may be shared improperly.

<u>Mitigation</u>: This risk is mitigated. Only authorized OIG personnel in the Office of Audits and the Office of Inspections and Evaluations have access to data maintained in TeamMate. Moreover, any sharing of information maintained in TeamMate is done on a need-to-know basis or when required for peer review purposes. The peer review process procedures are documented so that they are followed and do not risk improper access.

Section 7.0 Redress

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

Individuals may request access to information maintained in TeamMate through the Freedom of Information Act (FOIA)[11] and provisions of the Privacy Act of 1974 at https://www.oig.dhs.gov/foia. Requests can also be made by email, fax, or mail:

OIG Office of Counsel
Phone: 202-254-4001
Fax: 202-254-4398
Email: FOIA.OIG@OIG.DHS.GOV

Mailing Address:
245 Murray Lane SW
Mail Stop – 0305
Washington, D.C. 20528-0305
DHS OIG FOIA Request Form[12]

OIG maintains ownership of its own data. Therefore, OIG will refer FOIA and Privacy Act requestors seeking non-OIG data to the appropriate DHS Component(s). Individuals who would

[11] 5 U.S.C. § 552.

[12] DHS OIG FOIA Request Form FOIA Request Form, *available at* https://www.oig.dhs.gov/sites/default/files/assets/PDFs/OIG_Cert_Ident_Form.pdf.

like to make a FOIA request outside of OIG should contact the corresponding DHS Component. All requests must conform to the Privacy Act regulations[13] set forth in federal regulations and are evaluated to ensure that the release of information is lawful, will not impede an investigation, and will not reveal the existence of an investigation or investigative interest on the part of DHS or another agency.

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

Covered individuals may submit a Privacy Act Amendment request in accordance with the procedures for correcting inaccurate or erroneous information referenced in Section 7.1 above.

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

The audits, inspections, and evaluations conducted by OIG are completed on a DHS program or activity, not on an individual. As part of the audits, inspections, or evaluations process, findings related to program issues are identified and potential corrective actions are provided to DHS and the relevant Component(s). Nonetheless, this Privacy Impact Assessment and the OIG Investigative Records System of Records Notice provide notice and information to individuals on redress procedures.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not know what procedures exist to access or correct their information maintained in TeamMate.

Mitigation: This risk is partially mitigated. This Privacy Impact Assessment and the relevant System of Records Notice provide information on the redress provisions available to individuals. Due to the nature of OIG’s mission, however, it may not be readily apparent to individuals that OIG maintains their data. Further, because OIG’s Investigative Records System of Records Notice has been exempted from certain provisions of the Privacy Act through issuance of its corresponding Final Rule, not all records may be accessed or amended.

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?

The TeamMate application is accessed through Single Sign On (SSO) Personal Identity Verification (PIV). Auditors and inspectors must be logged into the OIG network to access

[13] 6 CFR Part 5.

TeamMate. The audit and inspection/evaluation managers are responsible for assigning team members within TeamMate to specific projects. Only those auditors or inspectors assigned to that project may view the documents/data in the project file. As an audit or inspection/evaluation project is closed out and completed, any audit or inspection/evaluation member who had access to that project is automatically removed. OIG employees who are not part of the Office of Audit or Office of Inspections and Evaluations do not have access to the TeamMate application. Further, logs are sent to the OIG's Splunk applications through which IT security personnel monitor for anomalous activity daily.

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

OIG employees are required to take annual security awareness training and role-based training (e.g., training for ISSOs, Authorizing Officials (AO), network and system administrators, and managers). All OIG users are required to participate in mandatory annual privacy training. Furthermore, OIG personnel responsible for conducting audits, inspections, and evaluations are trained on the risks associated with improper use of information and the OIG's responsibilities.

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 the TeamMate application is through Single Sign-On Personal Identity Verification. When a network account is created, the auditor or inspector is placed into an organizational unit (OU) which allows them access to the TeamMate application. Further access restrictions are in place within the application. Auditors and inspectors are assigned to a TeamMate project based on assigned audits, inspections, or evaluations. Within TeamMate there are roles for each project which include but are not limited to Audit/Inspections Deputy Inspector General, Audit/Inspections Supervisors, Audit/Inspections Reviewers, and Audit/Inspections Team Member. Each role has a defined access level to the projects which allows access based on a need to know.

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

All project reviews, approved information sharing, Interconnection Systems Agreement (ISA), Memoranda of Understanding (MOU), Memoranda of Agreement (MOA), and other uses of information maintained in TeamMate must comply with DHS Sensitive Systems Handbook and

Policy Directive 4300A.[14] All appropriate documentation and requirements must be approved by all authorizing officials of each system such as:

- System Owner (SO);
- Chief Information System Security Officer (CISO);
- Information System Security Manager (ISSM);
- Information System Security Officer (ISSO); and
- Program Manager (PM).

System Owner

Bridget Glazier
Deputy Chief Information Officer
Office of Chief Information Officer/OIG

Responsible Official

Darcia Rufus
Acting Chief, Information Law and Disclosure Division
Office of Counsel/OIG

Approval Signature

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

____

Mason C. Clutter
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

[14] DHS 4300A Sensitive System Handbook is a series of information security policies, which are the official documents that create and publish Departmental security standards in accordance with DHS Management Directive 140-01, Information Technology System Security. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, DHS 4300A SENSITIVE SYSTEMS HANDBOOK, *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.