The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

Privacy Compliance Review
Standard Operating Procedure
November 2016

Overview

The DHS Privacy Office (PRIV) conducts Privacy Compliance Reviews (PCR) pursuant to its responsibility under Section 222 of the Homeland Security Act to assure that technologies sustain and do not erode privacy protections, and that the fair information practice principles are followed in handling personally identifiable information (PII). Consistent with PRIV's unique position as both an advisor and oversight body for the Department's privacy sensitive programs and systems, PCRs are designed as a constructive and collaborative mechanism to ensure that a program is complying with applicable law and policy and with assurances made in existing privacy compliance documentation, including Privacy Impact Assessments (PIA) required by Section 208 of the E-Government Act of 2002 or Section 222 of the Homeland Security Act of 2002, as amended; System of Records Notices (SORN) required under the Privacy Act of 1974[1]; and in information sharing access agreements and other program documentation. Although the PCR is designed as a proactive and constructive mechanism, it is possible that potentially egregious behavior could be uncovered during the PCR. Should this occur, PRIV will either refer the matter to the DHS Office of Inspector General to investigate or convert the PCR into a formal PRIV investigation conducted under the Chief Privacy Officer's investigative authority.

This Standard Operating Procedure provides a framework to guide PRIV in the design and execution of PCRs and describes the roles of PRIV, the Component Privacy Offices, and the program being reviewed.

Initiating the PCR

PCRs are conducted at the discretion of the Chief Privacy Officer as well as when a PIA, SORN, agreement, or other program documentation specifically states that PRIV will initiate a PCR[2].

PRIV's Policy & Oversight team (P&O) leads the PCR program. P&O coordinates with the Chief Privacy Officer, Deputy Chief Privacy Officer, Deputy Chief Freedom of Information Act Officer, Senior Director for Privacy Compliance, and Senior Director for Information Sharing, Security, and Safeguarding to prioritize programs that will be subject to a PCR and forms a team

[1] Section 222(b) of the Homeland Security Act gives the Chief Privacy Officer authority to investigate Departmental programs and operations as they relate to privacy. The process by which the Chief Privacy Officer will exercise this investigative authority is distinct from the Privacy Compliance Review process.

[2] For example, PRIV reviews are part of DHS's oversight of the use of Passenger Name Records (PNR) consistent with the terms of the 2011 U.S. – European Union PNR Agreement (or any successor agreement) https://www.dhs.gov/publication/2015-report-use-and-transfer-passenger-name-records-between-european-union-and-united and compliance documents regarding the Department's use of Social Media by the Office of Operations Coordination (OPS) for situational awareness https://www.dhs.gov/publication/privacy-compliance-reviews-media-monitoring-initiative.

for each PCR that may also include relevant staff from other PRIV teams when particular knowledge or expertise is required or when resources warrant.

Review Process
The steps associated with PRIV's Privacy Compliance Reviews include:

Step 1: Collect and Review Available Background Information:
The PCR team will familiarize itself with the program/system and review the applicable PIAs, SORNs, and all other relevant program documentation. Relevant documentation may include, but is not limited to, Memoranda of Understanding, Information Sharing Access Agreements, applicable DHS Inspector General (IG) and Government Accountability Office (GAO) reports, previous PCRs, Standard Operating Procedures, and Concepts of Operation. This background information will serve as the foundation for tailoring program-specific questions. In addition, the statements in the PIA and SORN will serve as the baseline for assessing a program's compliance.

Step 2: Formulate Review Objectives
The first objective of any PCR is to assess a program's compliance with current privacy documentation and applicable DHS policies. This may ultimately be the only objective of the review. However, there may be cases when additional objectives will be included in a review. For example, if the program to be reviewed includes an MOU or some other form of agreement, PRIV may wish to add a review objective to assess compliance with the terms of such agreements. In addition, PRIV may initiate a review of a program that has been subject to recommendations from an IG or GAO report. In such cases PRIV may wish to look specifically at outstanding recommendations from relevant reports. Reviews may be designed to also include other privacy-related concerns voiced from the public or other medium (e.g., if a media outlet reports a DHS program does something to violate privacy rights, PRIV specifically reviews and assesses the claim). Depending on the type of program and concern raised, the PCR team's objective may be to review the program more holistically by way of analyzing adherence to the DHS Fair Information Practice Principles (FIPPs)[3].

Step 3: Notify Program of Review
The PCR team notifies the Component Privacy Officer/Privacy Point of Contact and Program Manager of PRIV's intent to review the program. The Component Privacy Officer and Privacy Point of Contact coordinate with the Program Manager as necessary to assist the PCR team in obtaining timely and relevant information for the review.

Step 4: Formulate Review Questions, Request Document, and Conduct Entrance Meeting
To assess compliance with current privacy documentation as well as any other objectives, the PCR team develops a set of tailored questions regarding the subject program/IT system. These questions should invoke open ended responses that show the "how" and "why" of a program's

[3] Privacy Policy Guidance Memorandum 2008-01 http://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf, Privacy Policy and Compliance Directive 047-01, July 2011 https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-directive-047-01_0.pdf, and Privacy Policy and Compliance Instruction 047-01-001, July 2011 https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-instruction-047-01-001_0.pdf.

operations and enable analysis of if and how a program complies with privacy assurances. There should be almost no "yes or no" responses. For example, if a PIA states that PII is only retained for six months, ask for records older than six months so when the query is run, there should be no PII in the response or a "no responsive records available" message from the program.

Depending on the extent of the review, an entrance meeting should be held. During the entrance meeting, the PCR team sets the tone for the review, stressing that it is designed to be a proactive and constructive mechanism and not an adversarial process. The questions should be sent in advance of the meeting with the program or IT system owners to allow time for initial analysis and to ensure the appropriate people are present at the meeting to address any concerns from either PRIV or the program office. Further, to the extent any other documentation needs can be identified up front, these should be included with the tailored questions sent to the program. Documents requested may include Standard Operating Procedures, policies, and system audit logs and will vary depending on the scope of the review.

Step 5: Conduct Interview(s) and Obtain Additional Supporting Documents
The two primary mechanisms for PCRs will involve interviews with program personnel and document reviews. The number of interviews conducted will depend on the scope of the review and follow-up needed by the PCR team. Once PRIV receives responses to the initial questionnaire and reviews supporting documents, arrange for an in-person interview with subject matter experts (any follow-up or additional discussions may be conducted via teleconference or via e-mail). During the interview, if the PCR team finds that references are made to a policy, procedure, or other written artifact that demonstrate how the program operates and/or complies with privacy requirements, the PCR team should request a copy of the document for analysis.

Step 6: Analyze Documentation and Interviews and Draft Preliminary Conclusions
As documents are provided by the program, the PCR team should review them and evaluate them against statements made in privacy compliance documentation and against the FIPPs. Note that Steps 5 and 6 may be concurrent, iterative steps, depending on the level of back and forth between the PCR team and the program. If compliance gaps are found (e.g., PIA references a retention schedule that has not yet been finalized), this should be noted and documented in the record of analysis. The PCR team will review the totality of information received through interviews and document reviews and identify its preliminary conclusions in a written record of analysis. The record of analysis will serve as the first step toward preparing the final report. The record of analysis should be cleared by the Senior Director for Privacy Policy & Oversight.

Step 7: Review and Confirm Findings
Once the preliminary analysis has been documented, the PCR team, and other PRIV staff as appropriate, will discuss the appropriate format and content for documenting the results of the PCR including any recommendations that should be communicated to the program. Subsequent to this discussion, the PCR team will notify the program of preliminary findings and recommendations from the record of analysis and confirm key facts contained within. This will often be achieved through sharing a draft product with program staff for their review and comment. These findings may include recommendations to mitigate issues not previously addressed in existing privacy compliance documentation. Depending on the issue, a PTA or PIA update may be needed. The PCR team may choose to communicate some of its findings more

informally to the program with suggestions for short-term and long-term solutions for any identified privacy gaps.

Step 8: Prepare and Issue Final Product
PCRs may result in recommendations to a program, updates to privacy documentation, informal discussions on lessons learned, or a formal internal or publicly available report. In order to further the impact of the review as a tool to enhance privacy compliance rather than as a mechanism to highlight weaknesses, any written results of PCRs will consist of a high-level summary of findings and recommendations, if applicable, delivered in a report signed by the Chief Privacy Officer to the program principal. To the extent practicable, the DHS Privacy Office will make results of PCRs publicly available. Given that the primary goal of a PCR is to improve program/system practices, a publicly available report may not always be the appropriate vehicle for achieving this goal. Nevertheless, PRIV at a minimum makes information about PCRs and their results publicly available through Congressionally-mandated reports including the Privacy Office Annual Report and Section 803 of the 9/11 Commission Act Semiannual reports.

Public reports will include general language about the PRIV review function, background information on the program, a summary of the key findings of the review, associated recommendations, and any additional conclusions. Public reports should be written at such a level that is transparent about findings but is sensitive to the overall goal of improving program practices. To the extent that any non-compliance was remedied through the conduct of the PCR, this should be identified. Regardless of the form PCR results take, PRIV will provide the program and the affected Component Privacy Officer or Privacy Point of Contact the opportunity to review and comment on a draft product and will make revisions as appropriate. PCR products will be reviewed internally by the Deputy Chief Privacy Officer and/or Deputy Chief Freedom of Information Act Officer and when appropriate, the Senior Director for Privacy Compliance, Senior Director for Information Sharing, Security, and Safeguarding and, at the discretion of the Chief Privacy Officer, the Office of General Counsel.[4]

PCR Management

Privacy Compliance Tracking System
The Privacy Compliance Tracking System (PCTS) is a workflow management system that tracks the full-lifecycle of privacy compliance processes and associated documentation including Privacy Threshold Analyses, PIAs, SORNs, Notices of Proposed Rulemaking, Final Rules, Computer Matching Agreements, Social Media Operational Use Templates, and PCRs. For PCRs, the PCTS provides users the ability to track the status of an active PCR, view the recommendations made, and track their implementation.

Follow Up
Once the PCR report is finalized, the Component Privacy Officer or Privacy Point of Contact is responsible for working with the Program Manager to track the implementation of the recommendations. The Component Privacy Office is required to report the status of the

[4] The Policy and Oversight team will consult with these reviewers to determine the appropriate timing for their reviews. In most cases the review will occur prior to sharing a draft product with the program for review.

recommendations to the PCR team on whatever schedule is agreed to and documented in the PCR report. The PCR team is responsible for keeping the PCTS up-to-date based on information provided from the Component Privacy Office.

The PRIV Compliance team should ensure that any subsequent updates to relevant PIAs and SORNs reflect the implementation, or pending implementation, of the PCR recommendations, when appropriate.