EPIC v. DEA, No. 15-cv-00667-CRC
Plaintiff's Combined Opposition to Defendant's Motion for Summary Judgment and
Cross-Motion for Summary Judgment

Exhibit 2

PRIVACY IMPACT ASSESSMENTS

Official Guidance

Office of Privacy and Civil Liberties

United States Department of Justice

(Revised July 2015)

I. Introduction

The Department of Justice (the Department or DOJ) is committed to ensuring the appropriate protection of privacy and civil liberties in the course of fulfilling its missions. Privacy Impact Assessments (PIAs), which are required by Section 208 of the E-Government Act of 2002,[1] are an important tool to assist the Department in achieving this objective. Specifically, Section 208 of the E-Government Act of 2002 requires all federal agencies to conduct a PIA before developing or procuring information technology that collects, maintains, or disseminates information that is in identifiable form or before initiating a new collection of information that will be collected, maintained, or disseminated using information technology and that includes any information in identifiable form in certain circumstances involving the public.

This guidance is designed to assist DOJ personnel on how to effectively conduct a PIA and how to properly document this assessment. This document is solely for the purpose of setting forth internal Department policy and guidance, and does not create any rights, substantive or procedural, that are enforceable at law by any party in any matter—civil or criminal.

II. Personnel

a. *Chief Privacy and Civil Liberties Officer*

The Department's Chief Privacy and Civil Liberties Officer (CPCLO) is primarily responsible for the Department's privacy policy, including advising the Attorney General regarding "appropriate privacy protections, relating to the collection, storage, use, disclosure, and security of personally identifiable information, with respect to the Department's existing or proposed information technology and information systems."[2] Additionally, the CPCLO is responsible for advising the Attorney General concerning the "implementation of policies and procedures, including appropriate training and auditing, to ensure the Department's compliance with privacy-related laws and policies, including section 552a of title 5, United States Code [the Privacy Act of 1974], and Section 208 of the E-Government Act of 2002 (Public Law 107–347)."[3] The CPCLO's review and approval of Departmental PIAs is one mechanism through which the CPCLO fulfills the above-referenced statutory mandates.[4]

[1] E-Government Act of 2002, Pub. L. 107-347, § 208, 116 Stat. 2899, 2921-23.

[2] Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. 109-162, § 1174, 119 Stat. 2960, 3124 (2006). See also Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110-53, § 803, 121 Stat. 266, 360-1.

[3] Violence Against Women and Department of Justice Reauthorization Act of 2005 § 1174.

[4] See Attorney General Order No. 2843-2006, dated October 2, 2006 (CPCLO approval for PIAs required). See also Deputy Attorney General (DAG) Order No. 0601, Privacy and Civil Liberties (Feb. 6, 2014) (setting forth roles and responsibilities of the CPCLO).

b. *Office of Privacy and Civil Liberties*

The Office of Privacy and Civil Liberties (OPCL) supports the CPCLO through the development and implementation of the Department's privacy compliance program. With regard to PIAs, OPCL provides guidance and training to components on compliance with E-Government Act PIA requirements, reviews PIAs in preparation for signature by the CPCLO, and provides public notice of PIAs as appropriate. Accordingly, OPCL issues this PIA guidance to be followed by all Departmental offices, boards, divisions, components, and bureaus.

c. *Senior Component Official for Privacy*

The Senior Component Official for Privacy (SCOP) is responsible at the component level for managing the implementation of privacy policies and requirements, subject to, as appropriate, the CPCLO's oversight and control, in order to ensure consistency with applicable laws, regulations, and mission needs. In doing so, the Fair Information Practice Principles (FIPPs) are considered in component-level privacy policy development and implementation. This responsibility includes ensuring the proper and timely preparation and completion of required privacy compliance documentation, including PIAs.[5] The SCOP for each component is required to review and prepare a draft PIA for OPCL review and CPCLO signature.

III. What is a PIA?

A PIA is an analysis required by the E-Government Act of 2002 of how information in identifiable form[6] is handled to ensure compliance with applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of collecting, maintaining, and disseminating such information in an electronic information system; and to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[7] The PIA demonstrates that the Department considers privacy from the beginning stages of a system's development and throughout the system's life cycle (i.e., collection, use, retention, processing, disclosure, and destruction). This ensures that privacy protections are built into the system from the start – not after the fact – when they can be far more costly or could affect the viability of the project.

[5] DAG Order No. 0601, Privacy and Civil Liberties (setting forth roles and responsibilities of the SCOP).

[6] The E-Government Act of 2002 applies to "information in identifiable form." We note that the National Institute of Standards and Technology (NIST) has stated that the term "information in identifiable form" is "[o]ften considered to have been replaced by the term PII [personally identifiable information]." NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Appendix C (April 2010). However, NIST also notes that terms such as "information in identifiable form" are similar to NIST's definition of PII and "organizations should not use the term PII (as defined in this document) interchangeably with these terms and definitions because they are specific to their particular context." Id.

[7] See OMB Memorandum, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Attachment A, Section II.A.6 (Sept. 26, 2003).

Additionally, the PIA demonstrates that the system developers and owners have made technology choices that reflect the incorporation of privacy into the fundamental system architecture. The PIA also gives the public notice of this analysis and helps promote trust between the public and the Department by increasing transparency of the Department's systems and missions.

IV. What is the Department's PIA Process?

a. *When Should a PIA be Completed?*

A PIA should be conducted before developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form; or initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for ten or more persons (excluding agencies, instrumentalities or employees of the federal government).[8]

OPCL assists components by assessing the need to conduct a PIA through the Initial Privacy Assessment (IPA) process.[9] First, components provide a recommendation to OPCL, as part of the completed IPA template, of whether a PIA is required. If OPCL determines that a component must complete a PIA, the component drafts a PIA using the current PIA template. However, if deemed appropriate by OPCL, components may draft an "Admin PIA," which is shorter in length, but still meets the minimum requirements of a PIA for purposes of Section 208 compliance. The use of the Admin PIA template is explained further in this guidance. See Appendix A. Whichever PIA template is used, the PIA should be drafted and issued during system development, with sufficient lead time to permit final Departmental approval and public website posting on or before the commencement of any system operation (including before any testing or piloting).

Further, although Section 208 of the E-Government Act does not apply to national security systems,[10] it is the Department's policy that PIAs must also be conducted for national security systems and submitted to OPCL for review and approval by the CPCLO.

b. *Who Should Prepare the PIA?*

The PIA process requires that candid and forthcoming communications occur among the system manager/owner, SCOP and other senior component privacy officials, and OPCL, to make the PIA comprehensive and meaningful and to ensure appropriate and timely handling of privacy concerns. With this in mind, the PIA should be written and reviewed by a combination of the component's privacy officials, IT security staff, and the program personnel responsible for the system.

[8] See id. at Section II.B.1.

[9] More information about the IPA process can be found in the DOJ's IPA Instructions and Template at http://www.justice.gov/opcl/privacy-compliance-process.

[10] See E-Government Act of 2002, § 202(i) (stating that most provisions of Title II (including Section 208) do not apply to national security systems).

c. *Preparing a PIA*

The E-Government Act requires, where practicable, that agencies make PIAs publicly available. Therefore, PIAs should be clear, unambiguous, and understandable to the general public. The length and breadth of a PIA will vary according to the size and complexity of the system.

To ensure consistency within the Department in the preparation of PIAs, all components must utilize and fully complete the most recent Department PIA template, as posted on the OPCL website at http://www.justice.gov/opcl/privacy-compliance-process, or on DOJNet. However, as above, there may be times when components may utilize the Department's "Admin PIA" template, which is shorter in length, but still meets the minimum requirements of a PIA for purposes of Section 208 compliance. This Admin PIA template is explained further in Appendix A of this guidance.

First, when using either template, please provide an executive summary of the PIA. The executive summary is a short paragraph describing the system and the PIA. The paragraph should consist of three or four sentences and should include the following information:

- Name of the component and system, technology, program, or pilot (hereinafter referred to as "system") and a brief description of the system and its function;
- The purpose of the system; and
- An explanation of why a PIA was completed. This sentence should explain the information in identifiable form that is collected, maintained, or disseminated by the system; and the context for why the system may be privacy sensitive.

Second, in general, please adhere to the following guidelines when drafting responses to the questions posed in either PIA template:

- Use plain language and take into account the perspective of a member of the public who is unfamiliar with the system or technology.
- Spell out each acronym the first instance it is used it in the document (e.g., Office of Management and Budget (OMB)).
- Use words, phrases, or names in the PIA that are readily known to the public.
- Define technical terms or references.
- Clearly reference projects and systems and provide explanations, if needed, to aid the general public.
- Include the complete name of the reference when first referencing National Institute of Science and Technology (NIST) publications and other documents (e.g., NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)). The abbreviated format may be used for subsequent references. Full names for NIST documents can be found at NIST's website http://csrc.nist.gov/publications/nistpubs.

It is imperative that in preparing a PIA, the component also review other privacy and security documentation relevant to the system, such as any Privacy Act System of Records Notice (SORN) and/or System Security Plan (SSP), to ensure consistency among all privacy/security documentation and the PIA.

A component privacy office with concerns regarding the sufficiency of a proposed answer, or with questions about the PIA template, is welcome to consult informally with OPCL before submitting the response or PIA for final review and approval. Similarly, component IT security staff with concerns or questions regarding the sufficiency of a proposed response to questions concerning the technical or security aspects of the system, should feel free to consult with the Department's Office of the Chief Information Officer (OCIO).

The component is responsible for preparing the PIA, including the completion of all internal component reviews, and obtaining the signature of the appropriate component Security Review Official. For Department components with an appointed Chief Information Officer (CIO), the Security Review Official shall be the Component CIO. For offices within JMD, the Security Review Official shall be the JMD Staff Director. For Offices, Boards and Divisions (OBDs) without an appointed CIO, the Security Review Official shall be the OBD Executive Officer if the system is owned by the OBD, or the OCIO Staff Director if the system is owned by the OCIO. In each case, the appropriate Security Review Official shall review all PIAs, assessing whether the system controls meet the security requirements, and shall indicate his/her approval of the system's technical description and security by signing the PIA.

The Senior Component Official for Privacy should then sign the PIA, indicating official issuance by the component, and then forward the PIA to OPCL for Departmental review and final approval. [11] (Please email the PIA to OPCL at privacy@usdoj.gov; if a PIA is classified, please contact OPCL to coordinate delivery.) PIAs should not be sent to OPCL until all required component signatures have been obtained.

d. PIA Review and Publication Process

Upon receipt of the PIA, OPCL will review the PIA for legal sufficiency and compliance with the E-Government Act of 2002, as well as further advise the CPCLO on any privacy policy issues. Part of that review will include ensuring that there is consistency with related materials (such as SORNs and SSPs). If warranted, OPCL and/or the CPCLO may return the PIA to the component for revision, or may disapprove it in accordance with the CPCLO's authority.[12] The CPCLO will approve and sign the PIA once the CPCLO determines that the PIA satisfies the applicable requirements. An approved PIA will then be returned to the component for information and publication.

[11] If a PIA contains information that the component wishes to redact prior to publication due to its sensitive or protected nature, the PIA should be appropriately marked to indicate the proposed redactions and the component must provide an explanation, as discussed below, under "PIA Review and Publication Process."

[12] See Violence Against Women and Department of Justice Reauthorization Act of 2005 § 1174.

The PIA should not be published until the PIA has been approved and signed by the CPCLO, and OPCL has so advised the component. Approved PIAs will be available to the general public. However, the Department, in its discretion, is not required to make a PIA (or portions thereof) publicly available if such publication would raise security concerns, or would reveal classified, sensitive, or otherwise protected information (e.g., potentially damaging to a national interest, law enforcement effort, or competitive business interest) that is contained in the assessment. If a component submits a PIA to OPCL that contains information that the component wishes to redact prior to publication due to its sensitive nature, the PIA should be appropriately marked to indicate the portions that the component proposes to redact, and the component must attach a separate explanation for the proposed redaction(s).

Publication normally should be accomplished by placing the PIA on the Justice.gov/opcl website. OPCL has a dedicated webpage where Department PIAs are posted. Components may also post their PIAs on a component-specific PIA webpage.

For PIAs that are completed for systems in development, the PIA does not need to be published until the design and construction of the system have been completed, and the PIA reflects the system as it will operate. However, a component may exercise its discretion and publish a PIA for a system still in development, if it so chooses.

e. Updating PIAs

Recognizing that information systems may undergo changes throughout their life cycle, it is important that any changes to the system be evaluated with regard to their effect on individuals' privacy. Components must update their PIAs to reflect significant changes to information collection authorities, business processes, or other factors affecting the collection and handling of information in identifiable form.[13] Components should use the IPA process to ascertain whether or not such changes would require a modification to an existing PIA or would require a new PIA, and may also consult OPCL for further guidance.

V. Contact the Office of Privacy and Civil Liberties

If one has any questions, please feel free to reach out to OPCL at the following:

Email: privacy@usdoj.gov; Phone: 202-514-0208
Website Link: www.justice.gov/opcl

[13] See OMB Memorandum, M-03-22, Attachment A, Section II.B.2.

VI. Definitions

- Individual – for purposes of conducting PIAs, it is the Department's policy to define "individual" in this context as any natural person regardless of citizenship status.

- Information in Identifiable Form – refers to information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements (i.e., indirect identification). These data elements may include a combination of gender, race, birth date, geographic indicators, and other descriptors. OMB Memorandum, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Attachment A, Section II.A.2. (Sept. 26, 2003).

- Information Technology – means, as defined in the Clinger-Cohen Act, any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Id. at Section II.A.3.

- National Security System – means, as defined in the Clinger-Cohen Act, any telecommunications or information system operated by the United States Government, the function, operation or use of which: (1) involves intelligence activities, (2) involves cryptologic activities related to national security, (3) involves command and control of military forces, (4) involves equipment that is an integral part of a weapon or weapons systems, or (5) is critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics and personnel management. Id. at Section II.A.5.

- Personally Identifiable Information – is any information that can be used to distinguish or trace an individual's identity such as name, social security number, biometric records, etc., alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. DOJ Order 0601, "Privacy and Civil Liberties" (Feb. 6, 2014).

APPENDIX A:

USE OF ADMIN PIA TEMPLATE

I. Background

Department components submit initial privacy assessments (IPAs) to the Office of Privacy and Civil Liberties (OPCL) in order for OPCL to determine whether a privacy impact assessment (PIA) and/or system of records notice (SORN) is required for a new or modified information system pursuant to the E-Government Act of 2002 and Privacy Act of 1974. Components recommend to OPCL, as part of the IPA template, whether a PIA or SORN is required. Once completed, components must submit a copy of each IPA to OPCL in order to make a final determination of whether a PIA and/or SORN is required.

If OPCL determines that a component must complete a PIA, the component must either draft a PIA using the traditional DOJ PIA template, or utilize a shorter template called the "Admin PIA," short for Administrative PIA. The Admin PIA template is designed primarily for those systems used for administrative purposes, rather than for law enforcement purposes or for any other duties or responsibilities related to the component's mission. Thus, use of this template should only be used for those very limited situations. Further, guidance below will help determine whether use of this template is appropriate.

This Admin PIA contains fewer questions than the traditional PIA template. The contents of the Admin PIA template will document, however, at a minimum, the requirements set forth by Section 208(b)(2) of the E-Government Act of 2002 and OMB M-03-022, Attachment A, II, (C)(1). However, there are additional questions from the traditional PIA template in the Admin PIA template.

II. Assessment

As stated above, the Admin PIA template is designed primarily for those systems used for administrative purposes, rather than for law enforcement purposes or for any other duties or responsibilities related to the component's mission. When considering whether use of the Admin PIA is appropriate, components and OPCL should take into account other factors as well. As required by Section 208, such other factors include: (1) the size of the information system being assessed; (2) the sensitivity of information that is in an identifiable form in that system; and (3) the risk of harm from unauthorized release of that information. It is important to note, that in addition to these three factors, there may be additional issues that arise from use of the system that will determine whether an Admin PIA or traditional PIA is required. See below though for more information on the three factors stated above:

1. *Data Volume and Size of System*

Volume is defined as the number and type of affected individuals. For instance, if the system only pertains to government employees, then it would be considered a low risk. If the system pertains to members of the general public, but only a subset of the general public, it would be considered either a high, moderate, or low risk. Similarly, if the component identifies the system as a major system, it may be considered a moderate or high risk. However, if a component requires assessment for a small subset or child of a parent system, then it may be considered a low risk.

2. *Data Sensitivity*

Data sensitivity is dependent on the type of the data, specifically the kind of PII. For instance, the following elements in many generic contexts can be considered a low risk, alone or in aggregate: full names, organizational information (e.g., office, job title), and physical addresses (e.g., work and/or personal). The following elements in most contexts can be considered a moderate risk, alone or in aggregate, due to the increased risk of fraudulent activity, or otherwise increased risk of harm associated with disclosure: SSNs, other sensitive ID numbers, authentication credentials, and limited credit information. The following elements in most contexts can be considered a high risk, alone or in aggregate: biometric data, federally protected data (e.g., medical/HIPAA), and financial data (e.g., personal banking, credit card). Thus, components and OPCL can make a subjective determination to increase the risk rating if the context is explained.[14]

3. *Risk of Harm from Unauthorized Disclosures*

The degree of risk of harm from potential unauthorized disclosures and releases of PII depends on the data sensitivity, the degree of security applied to the information in identifiable form, and the types of individuals and parties with whom the information is shared originally. For instance, if information is not considered to be sensitive, the security applied to the system containing such information is high, and information is initially restricted to a small subset of Department employees, then the risk of harm from unauthorized disclosures is a

[14] It is sometimes difficult to analyze the “data sensitivity” of PII in a system. Although some elements may be considered low sensitivity, such as date and place of birth, when considered in isolation, they may be considered moderately or highly sensitive when linked to additional information (e.g., such information may be used as an authentication factor for password recovery at many websites). Thus, categorizing the type of PII as low, moderate, or high sensitivity is a subjective assessment based on context. Therefore, components should use their best judgment and discretion in assessing the sensitivity rating of the PII included in the information system.

low risk. Although subjective, the following actions would lower the risk of harm of potential disclosures:

- If information in identifiable form is protected with Department-standard encryption.
- If a Certification and Accreditation and a security assessment has been completed.
- If appropriate security controls have been identified and implemented to protect against risks identified in a security risk assessment (e.g., physical access is controlled via a physical access control system (PACS), authentication to workstations requires the use of unique user IDs and passwords, data is encrypted in storage).
- If monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse (e.g., documentation is audited upon peer review and program review, access to certain sensitive information requires specific authorization and is limited to select personnel).
- If auditing procedures are in place to ensure compliance with security standards.
- If training on how to access, handle, and protect information specific to the system for authorized users, or general training that can be applied to this system, within the Department has been completed.
- If any sharing or dissemination has been limited to internal component or Department employees.

Based on the factors described above, as well as any other issues that may arise from use of the system, OPCL will make a final determination, with component input, whether an Admin PIA is appropriate in order to meet legal requirements as well as provide sufficient information to the public on the Department's collection of information and use of the system. As stated above, the Admin PIA template will be used primarily for those systems used for administrative purposes (e.g., setting up a voicemail system with contact information; utilizing a system that collects names and contact information for a list serve), rather than for law enforcement purposes, or any other purpose that is related to the component's mission.

The Admin PIA template can also be used by components when required to complete a PIA for use of third-party websites pursuant to OMB M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications", *available at*: http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf.[15]

[15] The admin PIA template may be used to fulfill the adapted PIA requirements pursuant to OMB M-10-23, Section 4(a); however, please review the Department-wide PIA for Third-Party Social Web Services to determine whether that PIA may cover the component's use of a system. That PIA is available here: http://www.justice.gov/opcl/docs/opa-webservices-pia.pdf.