



**Adapted PRIVACY IMPACT ASSESSMENT (Adp-PIA)**

**Third-Party Website or Application Name:**

**DoD Component Name:**

This Adapted PIA (Adp-PIA) Form 2930A is intended to support the management of risk to privacy. If it is likely that personally identifiable information (PII) will become available via a third-party website or application (such as Facebook and YouTube), complete this form. Complete PIA Form 2930 for all instances of electronic collection and maintenance of PII, in accordance with DoDI 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance." Refer to the Appendix for the definition of third-party websites or applications.

This Adapted PIA (Adp-PIA) Form 2930A is intended to support the management of risk to privacy. If it is likely that personally identifiable information (PII) will become available via a third-party website or application, complete this form.

**(1) Describe the specific purpose of the DoD Component's use of the third-party website or application.**

**(2) Describe any personally identifiable information (PII) that is likely to become available to the DoD Component through public use of the third-party website or application.**

**(3) Describe the circumstances under which PII will likely become available on the third-party website or application.**

**(4) With whom will the DoD Component share PII?**

**(5) Will the DoD Component maintain PII? If yes, for how long, and under what circumstances?**

**(6) Describe the means and steps by which the DoD Component will secure PII that it uses or maintains.**

**(7) Describe other privacy risks that exist and how the DoD Component will mitigate those risks.**

**(8) Will the DoD Component's activities create or modify a "system of records" under the Privacy Act? If yes, describe.**

**REVIEW AND APPROVAL SIGNATURES**

**Public Affairs or other Point of Contact**

Signature: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Organization: \_\_\_\_\_

Work Telephone Number: \_\_\_\_\_

DSN: \_\_\_\_\_

Email Address: \_\_\_\_\_

Date of Review: \_\_\_\_\_

**Other (Optional)**

Signature: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Organization: \_\_\_\_\_

Work Telephone Number: \_\_\_\_\_

DSN: \_\_\_\_\_

Email Address: \_\_\_\_\_

Date of Review: \_\_\_\_\_

**Other (Optional)**

Signature: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Organization: \_\_\_\_\_

Work Telephone Number: \_\_\_\_\_

DSN: \_\_\_\_\_

Email Address: \_\_\_\_\_

Date of Review: \_\_\_\_\_

**Component Senior Official for Privacy (CSOP), or designee**

Signature: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Organization: \_\_\_\_\_

Work Telephone Number: \_\_\_\_\_

DSN: \_\_\_\_\_

Email Address: \_\_\_\_\_

Date of Review: \_\_\_\_\_

**Component CIO, or designee (i.e., Department of the Navy CIO, Department of the Air Force, etc)**

Signature: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Organization: \_\_\_\_\_

Work Telephone Number: \_\_\_\_\_

DSN: \_\_\_\_\_

Email Address: \_\_\_\_\_

Date of Review: \_\_\_\_\_

## APPENDIX

### Definitions

**Make PII Available** - The term “make PII available” includes any agency action that causes PII to become available or accessible to the agency, whether or not the agency solicits or collects it. In general, an individual can make PII available to an agency when he or she provides, submits, communicates, links, posts, or associates PII while using the website or application. The term “Associate” can include activities commonly referred to as “friend-ing,” “following,” “liking,” joining a “group,” becoming a “fan,” and comparable functions.

**Personally Identifiable Information (PII)** - The term “PII,” as defined in OMB Memorandum M-07-16<sup>1</sup> refers to information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual.

**Privacy Impact Assessment (PIA)** - The term “PIA,” which is now subject to the modifications in this Memorandum, was defined in OMB Memorandum M-03-22<sup>2</sup> as:

[A]n analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

**Third-party websites or applications.** The term “third-party websites or applications” refers to web-based technologies that are not exclusively operated or controlled by a government entity, or web-based technologies that involve significant participation of a nongovernment entity. Often these technologies are located on a “.com” website or other location that is not part of an official government domain.<sup>3</sup> However, third-party applications can also be embedded or incorporated on an agency’s official website.

<sup>1</sup> OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007), available at <http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf>

<sup>2</sup> OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Sept. 26, 2003), available at [http://www.whitehouse.gov/omb/memoranda\\_m03-22/](http://www.whitehouse.gov/omb/memoranda_m03-22/)

<sup>3</sup> See OMB Memorandum M-05-04, *Policies for Federal Agency Public Websites* (Dec. 17, 2004) (identifying “.gov,” “.mil,” and “.Fed.us” as appropriate government domains), available at <http://www.whitehouse.gov/OMB/memoranda/fy2005/m05-04.pdf>