



Adapted PRIVACY IMPACT ASSESSMENT (Adp-PIA)

Third-Party Website or Application Name:

DoD Use of Third-Party Websites and Applications

DoD Component Name:

Department of Defense (DoD)

This Adapted PIA (Adp-PIA) Form 2930A is to be used when personally identifiable information (PII) is likely to become available via a third-party website or application (such as Facebook and YouTube). Refer to the Appendix for the definition of third-party websites or applications.

This Adapted PIA (Adp-PIA) 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.

This is a blanket Adapted Privacy Impact Assessment (Adp-PIA) for authorized use of third-party websites and applications by DoD Components. This Adp-PIA will be reviewed periodically and updated as necessary for changes in the way third-party websites and applications are used across DoD. Any DoD Component whose use of third-party websites and applications deviates from the circumstance below, shall complete a separate PIA enumerating the deviations and submit it to the Office of the DoD Chief Information Officer (DoD CIO).

The Department has demonstrated its commitment to improve transparency, participation, innovation and collaboration. Improved transparency enables the public to better understand goals and activities of the Department; lowers barriers between the Department and the public; and encourages greater exchange of ideas among the public, DoD employees, public interest groups and the interagency community to maximize creation of best practices and new initiatives. Embracing Open Government at the Department will generate new ideas benefiting both warfighters and U.S. citizens.

Third-party websites and 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. This includes a sphere of websites and Internet-based tools that focus on connecting users to engage in dialogue, share information and media, and collaborate. The Department may also use third-party websites and applications to make information widely available, while promoting transparency and accountability as a service for those seeking information about or services from the DoD.

One of the most common uses of third-party websites and applications is by warfighters communicating with their families. Third-party websites and applications are also used for outreach by Public Affairs and for collaboration and information sharing in numerous other mission areas.

Assumption:

The accounts that the DoD will open on third-party websites and applications are not a part of the DoD internal information systems. Third-party websites and applications are non-Federally operated and controlled. As such, the DoD cannot control the security measures the third-party websites and applications have to protect users' personally identifiable information (PII).

(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.

Third-party websites and applications may require individuals to register to access various accounts. However, the Department does not collect, maintain, use or share such information collected by the third-party websites and application providers. Any information that users provide to register for a third-party website or application is voluntarily contributed and is not maintained by the DoD.

The Department will not collect, maintain, use or share PII that may become available. This Adp-PIA provides transparency to the public regarding the Department's policy on the use of third-party websites and applications.

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

PII could become available from users' input. The Department will not collect, maintain, use or share PII that may become available. If PII inadvertently becomes available from user input, the PII will be removed to safeguard the individual's privacy per DoD policy.

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

The Department will not collect, maintain, use or share PII that may become available.

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

The Department will not collect, maintain, use or share PII that may become available.

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

Third-party websites and applications are not owned, operated or controlled by the Department. Users should consult the security and privacy policies of the third-party websites and applications they subscribe to for more information.

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

There are privacy risks that are not within the control of the Department and that the Department has limited ability to mitigate. Third party advertisements for example may pose privacy risks in the form of cookies or malware to those individuals who click on them.

The information available via third-party websites and applications is largely user-generated which means that the individual chooses the amount of information available about himself/herself as well as the ease with which it can be accessed by other users. Thus, the primary account holder should seek to redress any concerns through the third-party website or application provider. Individuals should consult the privacy policies of the third-party website or application they subscribe to for more information.

The Department does not own or control access to any of the third-party websites and applications on which it maintains accounts. If an individual desires to seek information regarding the controls in place over the confidentiality, privacy, integrity, and availability of information maintained by the third-party website or application provider, the individual should direct those inquiries to them. The Department will take steps to remove any material deemed to be privacy and/or operations security sensitive.

One of the most effective forms of mitigating these risks is education and training users of third-party websites and applications. The Department has many useful resources that explain how to use them safely, such as:

The DoD Social Media Hub site has an Education and Training section containing a wide array of resources on operations security and social media awareness at <http://www.defense.gov/socialmedia/education-and-training.aspx/>

Defense Information Systems Agency (DISA) has a training video on Social Networking which can be viewed online by government personnel and members of the public at the following link: http://iase.disa.mil/eta/sns_v1/sn/launchPage.htm

The Department has a Social Media User Agreement which contains Terms of Participation of users accessing DoD third-party websites. Use of any aspect of the websites will constitute user agreement to comply with the rules. The Social Media User Agreement can be obtained from the link: <http://www.defense.gov/socialmedia/user-agreement.aspx>

For Official Use Only (FOUO), classified, pre-decisional, proprietary or business-sensitive information should never be discussed or posted on third-party websites and applications. Similarly, personnel lists, rosters, organization charts or directories should not be discussed or posted.

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

Because DoD use of third-party websites and applications does not meet the criteria for a System of Records under the Privacy Act, a System of Records Notice is not required.