Template Version Number: 01-2020

U.S. Department of Commerce

Privacy Threshold Analysis
for the
Department-wide Use of Third-Party Websites and Social Media Applications

U.S. Department of Commerce Privacy Threshold Analysis

Department-wide Use of Third-Party Websites and Social Media Applications

Unique Project Identifier: Social Media

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) Whether it is a general support system, major application, or other type of system

Social Media the term used for third-party websites and applications, which refers to 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. However, third-party applications can also be embedded or incorporated on an agency's official website.

b) System location

As noted above, Social Media are outside of or not part of an official government domain. As they are generally owned and operated by private entities, locations vary. In general, these Social Media systems are primarily operated within the United States.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

Social Media, as accounted for in this Privacy Threshold Analysis (PTA), are considered standalone systems which do not interconnect with any existing Department of Commerce (DOC or "the Department") systems which are authorized to process PII. That said, in some cases, these tools and applications may be embedded into DOC owned and operated websites. For example, https://www.commerce.gov includes embedded capabilities to "Engage" the department via its primary social media outlets: Facebook, LinkedIn, Twitter, and YouTube, or to share content via Facebook, Twitter, or Google +.

d) The purpose that the system is designed to serve

Social Media serves as a conduit of information, in which critical information regarding the Department policies, changes in business strategies, and milestones in the agency's vision, mission, and goals (short term and long term) may be shared with the public. Social Media may also be used for research or analytical purposes by any individual employed by the Department, depending on the type of social media used at any given time.

e) The way the system operates to achieve the purpose

The DOC and its operating units use various third-party social media websites and applications to engage in dialogue, share information, and collaborate with the public. This Privacy Threshold Analysis (PTA) covers all authorized third-party social media websites and applications used by the Department of Commerce and its operating units that are functionally comparable with substantially similar practices across each website and application. All references to the DOC in this PTA refer to the Department and all its operating units.

The DOC uses several third-party websites and/or applications to engage with the public. These third-party websites and applications are typically referred to as social media, Web 2.0, or Gov 2.0 (SM/W2.0). According to the Social Media Guide, Social Media can be defined as user-generated content that is shared over the Internet via technologies that promote engagement, sharing, and collaboration.

Although these sites may contain official information from the DOC, they are not the authoritative source of official Department information. Use of these third-party social media sites does not constitute an endorsement by the DOC or any of its employees, sponsors of the sites, information, or products presented on these sites. Additionally, note that the privacy protections provided on DOC websites may not be available on third-party social media sites and applications. This PTA describes the privacy considerations used by the DOC when using a third-party's social media websites and applications that are covered by this PTA. To obtain information regard a third-party's privacy policy and practices, please see that third party's privacy policy.

This PTA analyzes the DOC's potential activities on certain social networking websites and web-based applications that make up the range of social networking websites. Generally, social networking websites and applications are privately owned by third parties. These social networking websites and applications continue to grow and diversify.

In general, social media can be bucketed into one of six categories as outlined and described in Table 1 below.

TABLE 1:

Type	Description	Examples
Social Networks	A social network site is a social media site that allows users to connect and share with people who have similar interests and backgrounds. Usually, official DOC users and public users may have an account to use applicationstailored to the specific website.	Facebook, LinkedIn, Myspace, Google+

Bookmarking sites	These sites allow users to save and organize links to any number of online resources and websites. A great feature of these services is the ability for the user to "tag" links, which makes them easier to search, and invariably, share with their followers. While there any variations, the most common example of these types of capabilities are the "share" or "subscribe" buttons commonly found on websites. These capabilities do not implicate user accounts.	Add to Any, StumbleUpon, AddThis
Social News	These sites allow users to post news links and other items to outside articles. Users then vote on said items, and the items with the highest number of votes are most prominently displayed. Official DOC usersmay have an account to post or, in the case of internal use, participate,but public users may not be required to have an account to view or participate.	Reddit, IdeaScale, Disqus
Media Sharing	Media sharing websites allow users to share different types of media, suchas pictures and video. Most of these sites also offer social features, like the ability to create profiles and the option of commenting on the uploaded images. Official DOC users must have an account to post but public users may not be required to have an account to see the video or image. For public users to comment, they may need an account.	YouTube, Flicker (SmugMug), Pinterest, snip.ly, UStream.tv
Microblogs	Sites that allow the users to submit short written entries, which can include links, including links to other social media sites. These are then posted on the 'walls' of everyone who has subscribed to that user's account. Official DOC users require an account to post but public users may not be required to have an account to see the blog. For public users tocomment, they may need an account.	Twitter, Tumblr, WordPress, Storify, Medium
Blogs and Online Forum(s)	An online forum is a site that lets users engage in conversations by posting and responding to community messages. A blog comment site is the same thing except a little more focused. The comments are usually centered around the specific subject of the attached blog. As with microblogs, official DOC users have an account to post but public users may not be required to have an account to see the blog. For public users tocomment, they may need an account.	Google Blogger, WordPress

In considering the different types of social networking websites and applications, the DOC, under the auspices of the requirements and analytical understanding outlined in this PTA, focuses primarily on those where an account or similar is required and thus Personally Identifiable Information (PII) may transit and be displayed by the system during the sign-up/log-on transaction and subsequent interactions.

Additionally, the DOC and its operating units leverage a variety of web-based tools for engaging members of the public, as well as DOC and other Federal employees. In general, a web-based tool is something that runs from a browser, on an outside server using the Internet. Many web applications fall under this category. DOC's use of web-based tools is generally

limited to those used for internal collaboration and productivity, data sharing, andsurveying participants in DOC-sponsored events. Examples include but are not limited to: Trello; Socrata; Survey Monkey; Asana; and Poll Everywhere. DOC's use of these web-based tools distinguishes them from third-party social media websites and applications discussed in this PIA. For that reason, these third-party web-based tools are discussed under a separate PTA.

Finally, it is important to note that this PTA does not cover or contemplate DOC-managed websites and applications. Departmental and Bureau website(s), and any DOC-managed applications (including mobile) are covered by separate PTAs. Likewise, this PTA does not address survey or registration tools where PII is sought or collected by the DOC. Such tools are covered by a separate Department-wide PTA.

The DOC does not share PII/BII that is made available through its third-party SW/W2.0 websites internally with outside entities. Information published on third-party's SM/W2.0 web sites that are covered under this PIA are open for public viewing and/or commenting. Whenever someone publicly posts to an agency's SM/W2.0 website, the entire contents of the posting will be publicly displayed on the agency's SM/W2.0 website and available to all visitors that specific web site for viewing, copying, and commenting. Users are encouraged to exercise care when posting information on a publica web site or application.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

When the DOC uses the SM/W2.0 website or applications, it does not solicit or collect PII or Business Identifiable Information (BII) and may only use the minimum amount of PII/BII, which it receives from a user, to fulfill a user's request.

g) Identify individuals who have access to information on the system

DOC Federal employees and DOC contract employees with operating unit access to interact with the public through third-party social media websites and applications.

h) How information in the system is retrieved by the user

When the DOC uses the SM/W2.0 website or applications covered under this PIA, it does not solicit or collect PII or Business Identifiable Information (BII).

i) How information is transmitted to and from the system

The Social Media used in the form of websites, applications, and technologies may be obtained by the end user to either input general information for log in purposes or to analyze statistical data, pending the type of Social Media in use. Such social media involve significant participation of a non-government entity and are in a location that is not part of an official government domain.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

✓ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017). *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

✓ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

☑ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII.

☑ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

☑ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- ☑ DOC employees
- ☑ Contractors working on behalf of DOC
- ☑ Other Federal Government personnel
- ☑ Members of the public *DOC does not solicit PII, but it may be provided voluntarily.

_____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

____ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

☑ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

☑ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

☑ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

✓ I certify the criteria implied by one or more of the questions above **apply** to Social Media and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the Social Media and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Kenyetta Haywood Office: DOC OPOG Phone: 202.482.6473 Email: khaywood1@doc.gov Signature: KENYETTA HAYWOOD Digitally signed by KENYETTA HAYWOOD Date: 2021.08.31 12:35:29 -04'00' Date signed:	**Information Technology Security Officer** Name: Jerome Nash Office: DOC OCIO Phone: 202.482.5929 Email: jnash@doc.gov Signature: JEROME NASH Digitally signed by JEROME NASH Date: 2021.08.31 12:32:06 -04'00' Date signed:
Privacy Act Officer Name: Tahira Murphy Office: DOC OPOG Phone: 202.482.8075 Email: tmurphy2@doc.gov Signature: TAHIRA MURPHY Digitally signed by TAHIRA MURPHY Date: 2021.09.13 11:41:01 -04'00' Date signed:	**Authorizing Official** Name: Lawrence Anderson Office: OS, OCIO Phone: 202.482.2626 Email: landerson@doc.gov Signature: LAWRENCE ANDERSON Digitally signed by LAWRENCE ANDERSON Date: 2021.09.01 14:33:14 -04'00' Date signed:
Bureau Chief Privacy Officer Name: Maria Dumas Office: DOC OPOG Phone: 202.482.5153 Email: mdumas@doc.gov Signature: MARIA STANTON-DUMAS Digitally signed by MARIA STANTON-DUMAS Date: 2021.09.17 00:45:55 -04'00' Date signed:	