U.S. Department of Commerce

Privacy Impact Assessment
for the
Department-wide Use of Third-Party Websites and Social Media Applications

Reviewed by: Maria D. Dumas, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode 09/23/2021

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
Department-wide Use of Third-Party Websites and Social Media Applications

Unique Project Identifier: Social Media

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(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 Impact Assessment (PIA), 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 way the system operates to achieve the purpose(s) identified in Section 4

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 Impact Assessment (PIA) 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 PIA refer to the Department and all its operating units.

The DOC uses several social media 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 mediasites does not constitute an endorsement by the DOC or any of its employees, sponsors of thesites, 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 sitesand applications. This PIA describes the privacy considerations used by the DOC when usingthe third party's social media websites and applications that are covered by this PIA. To obtain information regard the third party's privacy policy and practices, please see the third party's privacy policy.

This PIA 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 PIA, 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, and surveying 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 the 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 PIA.

Finally, it is important to note that this PIA 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 PIAs. Likewise, this PIA does not address survey or registration tools where PII is sought or collected by the DOC.

(e) 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).

(f) 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.

(g) Any information sharing conducted by the system

The DOC does not share PII/BII that is made available through its third-party SW/W2.0 websites internally or with outside entities. Information published on third-party SM/W2.0 websites 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 of that specific website for viewing, copying, and commenting. Users are encouraged to exercise care when posting information on a public website or application.

If a website user submits PII/BII in a request or an inquiry to an agency through the agency's SM/W2.0 website, the agency may use the PII/BII provided by the user to fulfill the specific request.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

The DOC use of third-party social media websites and applications is consistent with all applicable laws, regulations, and policies. The President's Memorandum on Transparency and Open Government (January 21, 2009) and the Office of Management and Budget (OMB) Director's Open Government Directive Memorandum (December 8, 2009) direct federal departments and agencies to harness new technologies to engage the public and serve as one of the primary authorities motivating the Department's efforts to utilize social networking websites and applications.

When the DOC uses the SM/W2.0 website or applications covered under this PIA, it is not permitted to actively seek 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.

Authorities supporting the DOC's use of social networking websites and applications include:

- 5 U.S.C. § 301, the Federal Records Act
- 5 U.S.C. § 552a, the Privacy Act of 1974
- Section 208 of the E-Government Act of 2002
- The President's Memorandum on Transparency and Open Government, January 21, 2009
- The OMB Director's Open Government Directive Memorandum, December 8, 2009
- OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2015

- OMB Memorandum for the Heads of Executive Departments and Agencies, and Independent Regulatory Agencies; Social Media, Web-Based Interactive Technologies, and thePaperwork Reduction Act, April 2016

The privacy policies of the DOC do not apply to the third-party social media websites or applications that are covered by this PIA. When visiting a DOC's third-party social media website or application, the third-party's privacy policy applies.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

As outlined above, these websites, applications, and technologies involve significant participation of a nongovernment entity and are located on a location that is not part of an official government domain. As such, a FIPS 199 impact category is not applied. However, DOC limits its use of social media and third-party applications, as outlined in this PIA, to that which process information which would otherwise be classified at a "Low" impact category in accordance with FIPS 199.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

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.

____ 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).

____ 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).

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	✓	h. Date of Birth	✓	o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address		q. Military Service	
d. Gender	✓	k. Telephone Number	✓	r. Criminal Record	
e. Age		l. Email Address	✓	s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify): This PII may be requested by the third-party social media application when setting up an account on its platform. DOC does not solicit any BII/PII through these applications.					

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address		i. Business Associates	
b. Job Title		f. Salary		j. Proprietary or Business Information	
c. Work Address		g. Work History		k. Procurement/contracting records	
d. Work Telephone Number		h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording	✓	i. Height		n. Retina/Iris Scans	
e. Photographs	✓	j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify): Third-party social media application users can share/post photographs and video recordings on the applications. DOC does not solicit any of this content through these applications.					

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		f. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify): Screen names					

Other Information (specify)
The DOC does not solicit, collect, maintain, or disseminate personally identifiable information from these third-party social media websites or applications. However, PII or BII that is voluntarily provided by a user may be used by an agency to respond to inquiries, answer questions, or fulfill a request submitted by the user. Although the DOC does not solicit, collect, maintain, or disseminate PII/BII from visitors to these third-party social media websites or applications, it is possible for individuals to voluntarily make such information available to agencies. Typical examples of the types of PII/BII that may become available to agencies include names of individuals and businesses, images from photos or videos, screen names, email addresses, etc. In addition, many third-party social media websites or applications request PII/BII at the time of registration. The process will vary across third-party social media websites or applications and often users can provide more than is required for registration. For example, users can provide such information as his or her interests, birthday, religious and political views, family members and relationship status, education, occupation and employment, photographs, contactinformation, and hometown. If the privacy setting on the third-party social media website or application is not restricted, such information may be made available to the DOC. Information provided to third-party social media websites or applications during registration is not collected or used by the DOC. The DOC does not ask individuals to post information on its Social Media/Website 2.0 (SM/W2.0) websites or applications. Information that individuals voluntarily submit as part of the registration process is not the property of the DOC and the DOC will not solicit this information.

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	✓
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			

Other (specify):

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third-Party Website or Application			✓		
Other (specify): In addition to information provided to the third-party social media website or application during registration, other sources of PII or BII may include screen names, information provided in comments, links, postings, and uploaded audio/video files, comments, or survey responses. Other activities conducted on the third-party social media website or application,such as “friend-ing”, “following”, “liking”, “joining” a “group”, becoming a “fan”, and comparable functions, can also be a source of PII/BII in the system.					

2.3 Describe how the accuracy of the information in the system is ensured.

While the DOC uses social media websites and applications as platforms for communicating their message to reach as many people as possible or to target specific audiences, the DOC does not collect, maintain, or disseminate PII/BII from individuals who interact with any DOC social media website or application, nor does it solicit such information. Therefore, risks posed by data accuracy are minimal. The DOC may use a person's screen name, email address, or other information voluntarily provided or made available by the user to respond to specific comments or questions directed to or about agency activities, or to fulfill a request. In such situations, data is provided directly by the individual and is assumed to be accurate, timely and relevant to the specific request.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
✓	No, the information is not covered by the Paperwork Reduction Act. Items collected by third-party social media websites and applications that are not collecting information on behalf of the Federal government are not subject to the Paperwork Reduction Act (PRA). The activities of the DOC on the third-party social media websites and applications covered by this PIA are carried out under the general solicitation exclusion of the PRA. Under the general solicitations exclusion, the PRA does not apply to notices published in the Federal Register or other publications that request public comments on proposed regulations, or any general solicitation for comments “regardless of the form or format thereof.” A general solicitation may have a degree of specificity. For example, a general solicitation may pose a

	series of specific questions designed to elicit relevant public feedback; but the solicitation may not be a survey and the responses should be unstructured. Unstructured solicitations, such as those found in the preambles of proposed rules published in the Federal Register, give members of the public the option of replying to some or all the questions in the manner they prefer (e.g., open-ended questions rather than selections from a list of choices). Similarly, agencies may offer the public opportunities to provide general comments on discussion topics through other means, including but not limited to social media websites; blogs; microblogs; audio, photo, or video sharing websites; or online message boards (whether hosted on a .gov domain or by a third-party provider).

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

✓	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

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

✓	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online	✓	For employee or customer satisfaction	✓

For web measurement and customization technologies (single session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The DOC uses third-party social media websites and applications to collaborate and share information online by facilitating public dialogue, providing information about or from the DOC, make information and services more widely available, and to improve customer service. Our use of these third-party social media websites and applications offer important opportunities for promoting the goals of transparency, public participation, and collaboration. Through these services, people or groups can create, organize, edit, comment on, combine, and share content of mutual interest.

As outlined above, the DOC does not solicit, collect, maintain, or disseminate PII/BII from visitors to these third-party social media websites or applications, although it is possible for individuals to voluntarily make such information available to agencies. Any PII or BII that is voluntarily provided by a user may be used by the Department to respondto inquiries, answer questions, or fulfill a request submitted by the user.

Examples of how the DOC may use PII/BII from a user includes:

a. After reading a Census Bureau posting on the Census Bureau's Facebook page, John Doe uses the email function provided on Facebook to submit a question directly to the Census Bureau's Facebook email account. Upon receipt of the question, a Census Bureau employee may use John Doe's email address to reply directly to his question. No PII/BII is maintained by the agency.

b. Jane Doe submits a question on Twitter in response to a Tweet posted by the National Institute of Standards and Technology (NIST). A NIST representative may direct their response to Jane by addressing her by her screen name.

c. An internal Office of the Secretary employee participates in an internal (DOC) conference where participants are asked to respond to a series of polls and surveys about leadership and strategy-related issues. Employees may respond, real time, by texting their responses to a provided number which is connected to a specific survey administered

by a DOC employee. The responses are captured and displayed, in real time on the screen, but the PII (telephone number) isnot collected by or made available to the DOC.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

There is a risk of unnecessary collection of or access to PII by DOC employees and contractors. There may be a potential for insider threat if the social media application is used in a manner that is not intended, and of any individual potentially divulging information that is sensitive. However, annual Cyber Security and Privacy Awareness Training is mandated across the Department for annual completion. As previously stated, DOC does not collect, maintain,or disseminate PII/BII from individuals who interact with any of its SM/W2.0 websites or applications that are in a request or an inquiry to an agency through the agency's SM/W2.0 website, or otherwise makes such information available, the agency may use the PII/BII provided by the user to fulfill the specific request. Although the PII/BII may be maintained by the third-party SM/W2.0 website or application, it is not maintained by the agency.

To further mitigate the risks of access to or collection of sensitive PII/BII, the agency may, to the extent possible, and in accordance with internal policies and federal rules and regulations, choose to delete or hide comments or other user interactions when a user's sensitive information is included.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

✓	The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
✓	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
✓	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	✓
Contractors	✓		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at:_____.	
✓	Yes, notice is provided by other means.	Specify how: Notice is provided via this Privacy Impact Assessment and by the individual privacy policies available on individual social media and third-party

		applications and capabilities used by the public to engage with DOC. As previously noted, the privacy policies of the DOC do not apply to the third-party social media websites or applications that are covered by this PIA. When visiting a DOC's third-party social media website or application, the third-party's privacy policy applies.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

✓	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: PII/BII is voluntarily provided by users. DOC does not solicit, collect, or disseminate this information.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

✓	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: DOC may use the screen name, email address, or other information provided by application users to respond to inquiries, answer questions, or to fulfill requests submitted by the user. Users voluntarily submit communication with DOC through third party social media applications and are consenting PII/BII by electing to do so.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

✓	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: The information that is generally provided by an individual can be modified, as it is contact user log in information for setting up an account, etc.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
✓	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
✓	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
✓	Access to the PII/BII is restricted to authorized personnel only.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): _____ ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
✓	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
✓	Other (specify): 1) Requests for creation of new accounts or new platforms are subject to review by the Office of Public Affairs, in conjunction with information security and privacy representatives. 2) All sites/tools must meet requirements outlined in OMB 10-23 and this PIA as outlined below.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

The DOC's privacy and security officials have established that no PII/BII from the DOC's SM/W2.0 websites or applications covered by this PIA will be collected, maintained, or disseminated by the DOC. Likewise, for websites or applications covered by this PIA, no PII is solicited. Additionally, DOC has implemented the following administrative and governance controls to reduce the risk that websites or applications, or any PII made available through them, are misused:

- Only approved staff members from the DOC have access to manage DOC's SM/W2.0 websites and applications.
- The DOC has established the SM/W2.0 rules of behavior as described in this PIA. Each staff member with access must comply with the internal rules of behavior for account management to maintain account administration.
- DOC's use of third-party websites and applications have an intended purpose directly related to an agency function that supports its mission.
- Third-party website and application terms and conditions, or terms of service,

which governs access to and use of such products and services are reviewed for compatibility with Federal law and regulations, or for a federal-compatible Terms of Service agreement, in accordance with Federal Acquisition Regulation Clause 48 CFR 52.212- 4(u) and OMB M-13-10, Anti-deficiency Act Implications of Certain Online Terms of Service Agreements.

- Third-party website or application privacy policies are evaluated for risks and to determine whether the website or application is appropriate for the agency's use (initially and periodically thereafter).
- Embedded third-party application on DOC websites or any other official DOC domain are accounted for in the relevant Privacy Policy for that website or domain.
- Appropriate branding is used to distinguish DOC's activities from those of non-government actors – generally the use of a DOC or Bureau seal or emblem to indicate that it is an official agency presence.
- Privacy Notices and Privacy Policies are linked or posted on the third-party website or application (where feasible).

Additional governance controls in place include a process by which both platforms (third-party applications, websites, etc.) and new user accounts must be requested and approved.

Finally, the internal DOC list of approved online platforms and social media services, which is available to DOC employees via the DOC's intranet, contains the following warning banner:

*"**WARNING:** The free platforms and tools below have been approved for DOC use by the DOC Office of Digital Engagement and have signed Terms of Service that allow Commerce employees to use them for official work purposes. A platform or tool's inclusion on this list **does not mean** that it has been reviewed and approved by your operating unit's Public Affairs and CIO teams, particularly in regard to cybersecurity and privacy. It is **your responsibility** as a future or current account owner to verify that your operating unit's CIO has completed the necessary cybersecurity and privacy risk assessments and has authorized the use of a given platform for your operating unit in general and your use case in particular. For more information on the bureau CIOs' responsibilities regarding these platforms, see page 12 of the DOC Policy on the Approval and Use of Social Media and Web 2.0."*

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g., name or Social Security number)?

____ Yes, the PII/BII is searchable by a personal identifier.

✓* No, the PII/BII is not searchable by a personal identifier.

**DOC does not collect PII/BII, however it may be collected by a third-party web application.*

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered*

by an existing SORN).
As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(List all that apply)*:
	Yes, a SORN has been submitted to the Department for approval on (date).
✓	No, this system is not a system of records and a SORN is not applicable. A Privacy Act system of records will not be created or altered as a result of the DOC's use of the SM/W2.0 websites or applications covered by this PIA because no PII/BII is retrieved by the DOC from these third-party services.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

✓	There is an approved record control schedule. Provide the name of the record control schedule: General Records Schedule (GRS) 4.2, General Records Schedule (GRS) 6.4 Please note, records consist of general information request(s) and response(s) as well as routine public affairs records that are of temporary value – for example: - Routine, day-to-day operational records - Correspondence and communications from the public which do not require formal action - Certain records related to the development of public affairs projects - Routine media relations records - Non-Mission related photographs and other similar audiovisual records. As previously stated, the DOC does not collect, maintain, or disseminate PII/BII from individuals who interact with any of its SM/W2.0 websites or applications that are covered by this PIA. If a user submits PII/BII in a request or an inquiry to an agency through the agency's SM/W2.0 website, the agency may use the PII/BII provided by the user to fulfill the specific request. Although the PII/BII may be maintainedby the third-party SM/W2.0 website or application, it is not maintained by the agency.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
✓	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	
Degaussing		Deleting	
Other (specify): N/A. No DOC IT systems have any control over the PII/BII voluntarily collected, nor does DOC have control over information that is maintained or disseminated, as provided by individuals who interact with Social Media websites or applications that are covered by this PIA.			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

✓	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

✓	Identifiability	Provide explanation: PII which is made available or voluntarily provided contains quasi-identifiers which, in combination with other available data could uniquely identify an individual.
✓	Quantity of PII	Provide explanation: Includes a large volume of records across multiple applications and websites.
✓	Data Field Sensitivity	Provide explanation: PII which is made available or voluntarily provided is generally widely known, publicly available, or otherwise not inherently "private" or "sensitive" in and of itself, and where the compromiseor unauthorize disclosure of such information would not lend itselfto substantial harm or inconvenience to the subject individual.
✓	Context of Use	Provide explanation: Information is not collected for the purposes of making determinations about specific individuals rights, benefits, or privileges, or in the administration of such, or would not otherwisebe reasonably considered "sensitive" in and of itself.

✓	Obligation to Protect Confidentiality	Provide explanation: Data is otherwise publicly available, or social norms, context, andexpectations are such that a reasonable person would assume no assurance of confidentiality or that information provided may be disclosed or otherwise be made publicly available.
✓	Access to and Location of PII	Provide explanation: PII is maintained and stored non-locally by a non-DOC affiliated entity. DOC employees' access is limited to approved staff members who may access and manage DOC accounts on third-party websites and applications, and access to PII is limited to that which is readily made available by end users of the website or application or is voluntarily provided to fulfill a specific request.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

There is a risk of disclosure of PII/BII by users: When interacting on a social media website (e.g. posting comments), PII/BII that users share or disclose will ordinarily become available to other users or anyone else with access to the site. Most users will likely avoid disclosing particularly sensitive or confidential PII/BII (e.g., Social Security or credit card number), which could be used by itself; or with other available information, to commit fraud or identity theft, or for other harmful or unlawful purposes. However, to help reduce those risks, the DOC will monitor postings to its authorized social media websites and applications to the extent practicable and will delete such posts of which the DOC becomes aware. Despite such efforts, the information may remain available elsewhere on the website, and others may have already viewed or copied the information. Additionally, the DOC does not request or collect any sensitive personal information, nor does it conduct any official business transactions on social media applications. Where possible, the DOC will also provide appropriate notice to users on the third-party social media website itself; warning them to avoid sharing or disclosing any sensitive PII/BII when interacting with the agency on the website. Users should also review the privacy policies of any third-party social media providers to determine if they wish to utilize that social media.

There is a risk that users may be subject to third-party advertising and tracking: A

third-party website operator may display advertising or other special communications on behalf of other businesses, organizations, or itself when a user interacts with the Department on the website. If the user clicks on the advertisement or reads the communication to learn about the advertised product or service, the user'sPII/BII may be shared by the website operator with the advertiser. The user's actions may also initiate tracking technology (e.g., "cookies," "web bugs," "beacons"), enabling the website operator or advertiser to create or develop a history or profile of the user's activities. The tracking data can be used to target specific types of advertisements to the user, i.e., behavioral advertising, or it can be used or shared for other marketing or non-marketing purposes. Users can avoid or minimize these risks by regularly deleting "cookies" through their browser settings, not clicking on advertisements, or not visiting advertisers' sites. Users may also opt-out of some tracking technologies all together. See http://www.usa.gov/optout-instructions.html for more information on how to do this.

There is a risk that users may be subject to SPAM, unsolicited communications, spyware, and other threats: Users may also receive spam or other unsolicited or fraudulent communications as a result of their interactions with the Department on third-party social media websites. To avoid harm, users should be wary of responding to such communications, particularly those that may solicit the user's personal information, which can be used for fraudulent or other undesirable purposes. Users should also avoid accepting or viewing unknown or unsolicited links, applications, or other content that may be sent or forwarded in such communications. These unsolicited links and applications can contain unwanted tracking technology as well as computer viruses or other malicious payloads that can pose a variety of risks to the user. Where possible, the DOC will also provide warnings about these risks in a notice(s) to users on the Department's data posted on the third-party social media website.

External links and embedded third-party applications: If the DOC posts a link that leads to a third-party social media website or any other location that is not part of an official government domain, where possible, the DOC will provide notice to the visitor, explaining that visitors are being directed to a non-government website that may have different privacy policies (and risks) from those of the DOC's official website. Likewise, if the DOC incorporates or embeds a third-party social media application, separate from any applications that may be incorporated or embedded by the website operator itself, the DOC will disclose and explain the nature or extent, if any, of the third-party's involvement in the DOC's use of the social media application(s). The DOC will also describe the use of these social media application(s) its own privacy policy.

Monitoring future requirements and future technology: In addition to the measures described above, the DOC will establish and/or maintain procedures to identify, evaluate, and address any new additional privacy requirements that may result from new statutes, regulations, or policies. Second, the DOC will evaluate the privacy risks of any new technologies before deciding whether to adopt it. Third, the DOC will monitor research or trends in privacy protection technologies or policies that may

facilitate new approaches to avoiding or mitigating privacy risks and better protecting PII/BII.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
✓	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
✓	No, the conduct of this PIA does not result in any required technology changes.