Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	**Open Source and Social Media Research and Development**		
Component:	Science and Technology (S&T)	**Office or Program:**	Data Analytics Technology Center
Xacta FISMA Name (if applicable):	**NA**	**Xacta FISMA Number (if applicable):**	**NA**
Type of Project or Program:	**New project**	**Project or program status:**	**Non-Operational**
Date first developed:	**November 1, 2018**	**Pilot launch date:**	N/A
Date of last PTA update	Click here to enter a date.	**Pilot end date:**	N/A
ATO Status (if applicable)	Choose an item.	**ATO expiration date (if applicable):**	Click here to enter a date.

COMPONENT PROJECT OR PROGRAM MANAGER

Name:	(b)(6)		
Office:	S&T/HSARPA/Data Analytics Technology Center (DATC)	**Title:**	Director, DATC
Phone:	(b)(6)	**Email:**	(b)(6)

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	(b)(6)		
Phone:	(b)(6)	**Email:**	(b)(6)

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: New PTA
The Science and Technology Directorate (S&T) is the lead coordinator for research and development (R&D) efforts and as such serves as a resource for DHS and its Components. The Data Analytics Technology Center (DATC) is the lead organization for this effort within S&T. S&T has contracted with the University of Alabama at Birmingham (UAB) to conduct R&D in open source and social media (OSSM), which involves the collection of publicly available information including social media. The work at UAB will be initially focused on counter-terrorism, illegal opioid supply chain, transnational crime, and understanding/characterizing/identifying the spread of disinformation by foreign entities, including the study of bot detection. However, successful methods should scale to other DHS domains. The intent is also to understand how threats evolve over time to lesser social media communities (e.g., not Facebook or Twitter) and to what extent, content can indicate location for information of interest that is not geo-tagged. UAB will be developing methods to identify information of interest for DHS missions. S&T will rely on subject matter experts within the operational Components for their input into the development process. However, the work will remain in the UAB and S&T laboratories until methods/capabilities are mature enough to transition for testing in an operational environment. At that time, PTAs will be drafted and/or updated. Beyond reports and methods/capabilities, outputs will include enduring research test sets to be kept at S&T DATC that will be used to establish baselines and measure tool capabilities for the Department.

2. Does this system employ any of the following technologies: *If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.*	☐ Closed Circuit Television (CCTV) ☒ Social Media ☐ Web portal[1] (e.g., SharePoint) ☐ Contact Lists ☐ None of these

3. From whom does the Project or Program collect, maintain, use, or	☐ This program does not collect any personally

[1] Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

disseminate information? *Please check all that apply.*	identifiable information[2] ☒ Members of the public ☐ DHS employees/contractors (list components): ☐ Contractors working on behalf of DHS ☐ Employees of other federal agencies

4. What specific information about individuals is collected, generated or retained?	
4(a) Does the project, program, or system retrieve information by personal identifier?	☐ No. Please continue to next question. ☒ Yes. If yes, please list all personal identifiers used: Social Media handles
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	☒ No. ☐ Yes.
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	Click here to enter text.
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	Click here to enter text.
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure? *For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?*	☒ No. Please continue to next question. ☐ Yes. If a log kept of communication traffic, please answer the following question.
4(f) If header or payload data[3] is stored in the communication traffic log, please detail the data elements stored.	
Click here to enter text.	

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

[3] When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?	☒ No. ☐ Yes. If yes, please list:
6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?	☐ No. ☒ Yes. If yes, please list: PII will not be from DHS systems, but if individuals in the public post their information on social media, the post may appear in the data.
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	Existing Not applicable. Please describe applicable information sharing governance in place:
7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?	☒ No. ☐ Yes. If yes, please list:
8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals/agencies who have requested access to their PII?	☒ No. What steps will be taken to develop and maintain the accounting: not applicable. ☐ Yes. In what format is the accounting maintained:
9. Is there a FIPS 199 determination?[4]	☐ Unknown. ☐ No. ☒ Yes. Please indicate the determinations for each of the following: Confidentiality:

[4] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.
[4] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

	☐ Low ☒ Moderate ☐ High ☐ Undefined Integrity: ☒ Low ☐ Moderate ☐ High ☐ Undefined Availability: ☒ Low ☐ Moderate ☐ High ☐ Undefined

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	
Date submitted to Component Privacy Office:	
Date submitted to DHS Privacy Office:	
Component Privacy Office Recommendation: *Please include recommendation below, including what new privacy compliance documentation is needed.*	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	Click here to enter text.
PCTS Workflow Number:	Click here to enter text.
Date approved by DHS Privacy Office:	Click here to enter a date.
PTA Expiration Date	Click here to enter a date.

DESIGNATION

Privacy Sensitive System:	Choose an item. If "no" PTA adjudication is complete.
Category of System:	Choose an item. If "other" is selected, please describe: Click here to enter text.
Determination: ☐ PTA sufficient at this time.	

	☐ Privacy compliance documentation determination in progress. ☐ New information sharing arrangement is required. ☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. ☐ Privacy Act Statement required. ☐ Privacy Impact Assessment (PIA) required. ☐ System of Records Notice (SORN) required. ☐ Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer. ☐ A Records Schedule may be required. Contact your component Records Officer.
PIA:	Choose an item. If covered by existing PIA, please list: Click here to enter text.
SORN:	Choose an item. If covered by existing SORN, please list: Click here to enter text.
DHS Privacy Office Comments: *Please describe rationale for privacy compliance determination above.*	
Click here to enter text.	

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	**Open Source and Social Media Research and Development**		
Component:	Science and Technology (S&T)	**Office or Program:**	Data Analytics Technology Center
Xacta FISMA Name (if applicable):	**NA**	**Xacta FISMA Number (if applicable):**	**NA**
Type of Project or Program:	**New project**	**Project or program status:**	**Non-Operational**
Date first developed:	**November 1, 2018**	**Pilot launch date:**	N/A
Date of last PTA update	Click here to enter a date.	**Pilot end date:**	N/A
ATO Status (if applicable)	Choose an item.	**ATO expiration date (if applicable):**	Click here to enter a date.

COMPONENT PROJECT OR PROGRAM MANAGER

Name:	(b)(6)		
Office:	S&T/HSARPA/Data Analytics Technology Center (DATC)	**Title:**	Director, DATC
Phone:	(b)(6)	**Email:**	(b)(6)

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	(b)(6)		
Phone:	(b)(6)	**Email:**	(b)(6)

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: New PTA

The Science and Technology Directorate (S&T) is the lead coordinator of research and development (R&D) efforts for DHS. The Data Analytics Technology Center (DATC) within S&T has contracted with the University of Alabama at Birmingham (UAB), who submitted a proposal that was accepted through S&T's Long-Range Broad Agency Announcement (LRBAA). The LRBAA is a standing, open invitation to the scientific and technical communities to fund R&D projects for homeland security missions. UAB will conduct open source and social media (OSSM), which involves the collection of publicly available information including social media. Social media pages may include handles, account names, emails, pictures, phone numbers, and posted content that are accessible to anyone with an internet connection.

UAB has deep past experience in OSSM identifying online content on terrorism, transnational crime (e.g., MS-13), financial fraud, and illegal substances supply chain for both private sector and government stakeholders. S&T's UAB effort will conduct R&D to understand these methods and further develop capabilities for DHS missions.

Phase 1 (present – December 2019): While S&T may request subject matter experts' input and feedback throughout all phases, the work will remain in the UAB and S&T DATC laboratories until methods/capabilities are ready for testing/use in an operational environment. At that time, PTAs will be drafted and/or updated. S&T DATC will continue to work closely with the S&T Privacy Office, as R&D efforts have varying degrees of uncertainty and success and findings that are unpredictable.

- S&T-UAB will develop methods and tools to identify information of interest regarding terrorism, opioid supply chain, and transnational crime. S&T will work with CBP, ICE, TSA, and USCIS to provide cross-mission operational context to inform research. Phase I will produce and refine the methods for finding relevant content and show some automation of tools.
- S&T-UAB will develop methods that attempt to identify and characterize foreign influence online, such as studying bot detection. Phase I will produce a paper/brief/proof-of-concept that shows how influence might be happening to inform policy and practices or identifies gaps that require additional R&D.
- S&T-UAB will develop methods, such as key words, for identifying location absent GPS metadata. Phase I will produce a paper/brief/proof-of-concept that discusses various methods or that identifies gaps that require additional R&D.
- S&T-UAB will study possible ways to track threats that evolve over time to "lesser social media communities" (e.g., not Facebook or Twitter). Phase I will produce a paper/brief/proof-of-concept that discusses various methods for tracking evolving threats or that identifies gaps that require additional R&D.
- S&T-UAB may test the methods and tools developed under this project against live events that are unfolding in real-time, if appropriate, to evaluate performance. For example, non-GPS methods may be helpful in a hurricane scenario for help calls.

Phase 2 (January 2020 – December 2020): Phase II depends on the findings in Phase I. Phase II may include further maturing the capabilities in Phase I; increased automation and performance; testing in an operational environment; applying the methods developed in Phase I to other domains.

Phase 3 (January 2021 – September 2021): Phase III is dependent on the findings of the previous phases

but may include maturing capabilities; testing in an operational environment; commercialization or hardening products for operational use.

2. Does this system employ any of the following technologies: *If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.*	☐ Closed Circuit Television (CCTV) ☒ Social Media Social media pages may include handles, account names, emails, pictures, phone numbers, and posted content that are accessible to anyone with an internet connection. ☐ Web portal[1] (e.g., SharePoint) ☐ Contact Lists ☐ None of these

3. From whom does the Project or Program collect, maintain, use, or disseminate information? *Please check all that apply.*	☐ This program does not collect any personally identifiable information[2] ☒ Members of the public ☐ DHS employees/contractors (list components): ☐ Contractors working on behalf of DHS ☐ Employees of other federal agencies

4. What specific information about individuals is collected, generated or retained?	
4(a) Does the project, program, or system	☐ No. Please continue to next question.

[1] Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

retrieve information by personal identifier?	☒ Yes. If yes, please list all personal identifiers used: Social media pages may include handles, account names, emails, pictures, phone numbers, and posted content that are accessible to anyone with an internet connection.
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	☒ No. ☐ Yes.
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	Click here to enter text.
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	Click here to enter text.
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure? *For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?*	☒ No. Please continue to next question. ☐ Yes. If a log kept of communication traffic, please answer the following question.
4(f) If header or payload data[3] is stored in the communication traffic log, please detail the data elements stored.	
Click here to enter text.	

5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?	☒ No. ☐ Yes. If yes, please list:
6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?	☐ No. ☒ Yes. If yes, please list: PII will not be from DHS systems, but if individuals

[3] When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

[4] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.

	in the public post their information on social media, the post may appear in the data.
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	Existing Not applicable. Please describe applicable information sharing governance in place:
7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?	☒ No. ☐ Yes. If yes, please list:
8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals/agencies who have requested access to their PII?	☒ No. What steps will be taken to develop and maintain the accounting: not applicable. ☐ Yes. In what format is the accounting maintained:
9. Is there a FIPS 199 determination?[4]	☐ Unknown. ☐ No. ☒ Yes. Please indicate the determinations for each of the following: Confidentiality: ☐ Low ☒ Moderate ☐ High ☐ Undefined Integrity: ☒ Low ☐ Moderate ☐ High ☐ Undefined Availability: ☒ Low ☐ Moderate ☐ High ☐ Undefined

[4] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	
Date submitted to Component Privacy Office:	
Date submitted to DHS Privacy Office:	
Component Privacy Office Recommendation: *Please include recommendation below, including what new privacy compliance documentation is needed.*	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	Click here to enter text.
PCTS Workflow Number:	Click here to enter text.
Date approved by DHS Privacy Office:	Click here to enter a date.
PTA Expiration Date	Click here to enter a date.

DESIGNATION

Privacy Sensitive System:	Choose an item. If "no" PTA adjudication is complete.
Category of System:	Choose an item. If "other" is selected, please describe: Click here to enter text.
Determination:	☐ PTA sufficient at this time. ☐ Privacy compliance documentation determination in progress. ☐ New information sharing arrangement is required. ☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. ☐ Privacy Act Statement required. ☐ Privacy Impact Assessment (PIA) required. ☐ System of Records Notice (SORN) required. ☐ Paperwork Reduction Act (PRA) Clearance may be required. Contact

	your component PRA Officer. ☐ A Records Schedule may be required. Contact your component Records Officer.
PIA:	Choose an item. If covered by existing PIA, please list: Click here to enter text.
SORN:	Choose an item. If covered by existing SORN, please list: Click here to enter text.
DHS Privacy Office Comments: *Please describe rationale for privacy compliance determination above.*	
Click here to enter text.	

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	**Open Source and Social Media Research and Development**		
Component:	Science and Technology (S&T)	**Office or Program:**	Data Analytics Technology Center
Xacta FISMA Name (if applicable):	**NA**	**Xacta FISMA Number (if applicable):**	**NA**
Type of Project or Program:	**New project**	**Project or program status:**	**Non-Operational**
Date first developed:	**November 1, 2018**	**Pilot launch date:**	N/A
Date of last PTA update	Click here to enter a date.	**Pilot end date:**	N/A
ATO Status (if applicable)	Choose an item.	**ATO expiration date (if applicable):**	Click here to enter a date.

COMPONENT PROJECT OR PROGRAM MANAGER

Name:	(b)(6)		
Office:	S&T/HSARPA/Data Analytics Technology Center (DATC)	**Title:**	Director, DATC
Phone:	(b)(6)	**Email:**	(b)(6)

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	(b)(6)		
Phone:	(b)(6)	**Email:**	(b)(6)

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: New PTA
The Science and Technology Directorate (S&T) is the lead coordinator for research and development (R&D) efforts and as such serves as a resource for DHS and its Components. The Data Analytics Technology Center (DATC) is the lead organization for this effort within S&T. S&T has contracted with the University of Alabama at Birmingham (UAB) to conduct R&D in open source and social media (OSSM), which involves the collection of publicly available information including social media. The award was made on September 21, 2018. The contract has a base of 1 year with two option periods. The work at UAB will be initially focused on counter-terrorism, illegal opioid supply chain, and understanding/characterizing/identifying the spread of disinformation by foreign entities, including the study of bot detection. However, successful methods should scale to other DHS domains. The intent is also to understand how threats evolve over time to lesser social media communities (e.g., not Facebook or Twitter) and to what extent, content can indicate location for information of interest that is not geo-tagged. UAB will be developing methods to identify information of interest for DHS missions. S&T will rely on subject matter experts within the operational Components for their input into the development process. However, the work will remain in the UAB and S&T laboratories until methods/capabilities are mature enough to transition for testing in an operational environment. At that time, PTAs will be drafted and/or updated. Beyond reports and methods/capabilities, outputs will include enduring research test sets to be kept at S&T DATC that will be used to establish baselines and measure tool capabilities for the Department.

2. Does this system employ any of the following technologies: *If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.*	☐ Closed Circuit Television (CCTV) ☒ Social Media ☐ Web portal[1] (e.g., SharePoint) ☐ Contact Lists ☐ None of these

3. From whom does the Project or Program collect, maintain, use, or	☐ This program does not collect any personally

[1] Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

disseminate information? *Please check all that apply.*	identifiable information[2] ☒ Members of the public ☐ DHS employees/contractors (list components): ☐ Contractors working on behalf of DHS ☐ Employees of other federal agencies

4. What specific information about individuals is collected, generated or retained?	
4(a) Does the project, program, or system retrieve information by personal identifier?	☐ No. Please continue to next question. ☒ Yes. If yes, please list all personal identifiers used: Social Media handles
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	☒ No. ☐ Yes.
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	Click here to enter text.
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	Click here to enter text.
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure? *For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?*	☒ No. Please continue to next question. ☐ Yes. If a log kept of communication traffic, please answer the following question.
4(f) If header or payload data[3] is stored in the communication traffic log, please detail the data elements stored.	
Click here to enter text.	

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

[3] When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?	☒ No. ☐ Yes. If yes, please list:
6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?	☐ No. ☒ Yes. If yes, please list: PII will not be from DHS systems, but if individuals in the public post their information on social media, the post may appear in the data.
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	Existing Not applicable. Please describe applicable information sharing governance in place:
7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?	☒ No. ☐ Yes. If yes, please list:
8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals/agencies who have requested access to their PII?	☒ No. What steps will be taken to develop and maintain the accounting: not applicable. ☐ Yes. In what format is the accounting maintained:
9. Is there a FIPS 199 determination?[4]	☐ Unknown. ☐ No. ☒ Yes. Please indicate the determinations for each of the following: Confidentiality:

[4] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.
[4] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

	☐ Low ☒ Moderate ☐ High ☐ Undefined Integrity: ☒ Low ☐ Moderate ☐ High ☐ Undefined Availability: ☒ Low ☐ Moderate ☐ High ☐ Undefined

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	
Date submitted to Component Privacy Office:	
Date submitted to DHS Privacy Office:	
Component Privacy Office Recommendation: *Please include recommendation below, including what new privacy compliance documentation is needed.*	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	Click here to enter text.
PCTS Workflow Number:	Click here to enter text.
Date approved by DHS Privacy Office:	Click here to enter a date.
PTA Expiration Date	Click here to enter a date.

DESIGNATION

Privacy Sensitive System:	Choose an item. If "no" PTA adjudication is complete.
Category of System:	Choose an item. If "other" is selected, please describe: Click here to enter text.
Determination: ☐ PTA sufficient at this time.	

	☐ Privacy compliance documentation determination in progress. ☐ New information sharing arrangement is required. ☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. ☐ Privacy Act Statement required. ☐ Privacy Impact Assessment (PIA) required. ☐ System of Records Notice (SORN) required. ☐ Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer. ☐ A Records Schedule may be required. Contact your component Records Officer.
PIA:	Choose an item. If covered by existing PIA, please list: Click here to enter text.
SORN:	Choose an item. If covered by existing SORN, please list: Click here to enter text.
DHS Privacy Office Comments: *Please describe rationale for privacy compliance determination above.*	
Click here to enter text.	