Privacy Impact Assessment
for the

Social Media Screening

DHS/USSS/PIA-026

December 6, 2019

Contact Point
Michael Mullen
Managing Chief
Security Management Division
United States Secret Service
(202) 406-5870

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The United States Secret Service (USSS or Secret Service) Security Management Division (SMD) has procured a contract to conduct social media checks in support of the background investigation (BI) process for hiring, continuous evaluation, and periodic reinvestigation. The Secret Service uses these BI processes to help mitigate the risk posed by those who potentially represent a threat to national security through proactive intervention and by identifying security-relevant information. Currently, various sources are checked for personnel security purposes, and USSS is adding a review of publicly available social media information to the existing processes that USSS security personnel use in identifying relevant information in assessing the eligibility of job applicants who have been conditionally selected for hire; reinvestigation of personnel holding clearances; and evaluation of a covered individual on an ongoing basis during the period of eligibility. The Secret Service is conducting this Privacy Impact Assessment (PIA) to discuss the collection, use, and maintenance of social media information in these processes.

Overview

The Secret Service is committed to hiring a high quality, diverse, and talented workforce. In support of the USSS BI process, SMD entered into a contract that enables referral of limited and relevant publicly available social media information to SMD. Selectees who have a conditional job offer from USSS, as well as employees and contractors who require access to USSS facilities and systems, will have these electronic records added to the current BI activities and materials already used in conjunction with continuous evaluation and periodic reinvestigation authorities.

The vendor will conduct social media checks and refer social media information on prospective employees (selectees) and contractors only after proposed employee or contractor has received a conditional job offer or contract offer, are in the process of having a personnel security background investigation conducted by USSS, and have completed Standard Form 86 (Revised November 2016) and Standard Form 85 (Revised December 2013), at a minimum. For current USSS employees and contractors, social media checks will be conducted in the course of their periodic re-investigation and in conjunction with continuous evaluation as required to maintain their security clearances.[1]

USSS's vendor will forward strictly limited and relevant publicly available social media information to USSS SMD staff for evaluation of existing and prospective personnel consistent with Security Executive Agent Directive 5 "Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications"

[1] All published Security Executive Agent Directives, including 3, 4, 5, 6, and 7, are applicable and are available at https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent/ncsc-policy.

and with DHS/ALL-023 Department of Homeland Security Personnel Security Management.[2] SMD staff and the USSS vendor will not impede a selectee's First Amendment rights, as the vendor will forward only the information detailed below to USSS SMD to consider as part of its overall requirements for mandated BI processes.[3]

USSS will review social media as an additional source of information in evaluating existing and prospective personnel as part of its overarching personnel security clearance efforts as directed by the Director of National Intelligence (DNI). The DNI serves as the Security Executive Agent, and is responsible for developing and implementing policies and procedures governing the conduct of investigations and adjudications related to personnel security clearance efforts.

The information the social media contractor will refer to the USSS SMD can be categorized into four categories: unlawful sexual deviant behavior, unlawful violent behavior, unlawful racist acts, and information depicting acts of terrorism and/or membership in an organization dedicated to terrorism. Professional investigators within SMD will include this information in furthering the mandated BI processes for evaluation of existing and prospective personnel.

The vendor will document and return to SMD the date, site(s) accessed, and information collected related to the allowable categories per the acquisition documents and signed agreements for this task and engagement. Only publicly available electronic information (PAEI) posted on social media will be viewed by the vendor. The contractor does not view any other pages other than those associated with the subject. SMD may use its investigative process and authorities to view the social media pages, corroborate the PAEI, and allow the subject to explain or refute any relevant information surfaced through the check.

The vendor will be provided via encrypted email with the individual's name, address, date of birth, and place of birth to ensure that the correct individual is identified. Mandatory social media training will be provided to SMD and vendor personnel, covering identifying and handling any issues involving all relevant laws and policies that protect civil liberties and protect activity. Unless otherwise authorized by law, USSS SMD does not store or disseminate information related to First Amendment-protected speech or activities. Neither USSS SMD personnel nor contract support will appropriate an online identity to interact with any individual whose information may be posted in the social media content. Additionally, the vendor will not review social media or collect information on individuals who are not USSS prospective employees, current employers, or contractors.

---

[2] *See* DHS/ALL-023 Department of Homeland Security Personnel Security Management, (February 23, 2010) 75 FR 8088.

[3] *See* 5 U.S.C. 552a (e)(7); Memorandum for All DHS Employees from Kevin K. McAleenan, Acting Secretary, "Information Regarding First Amendment Protected Activities," (May 17, 2019), *available at* https://www.dhs.gov/sites/default/files/publications/info_regarding_first_amendment_protected_activities_as1_signed_05.17.2019.pdf.

Job selectees, current employees, and contractors using Standard Form 86 (Revised November 2016) and Standard Form 85 (Revised December 2013) who require access to USSS facilities and systems are given notice during the application or reinvestigation process by signing a release for information that includes access to PAEI. The vendor verifies that the social media results relate to the correct individual by using a minimum of two points of verification out of the information provided by SMD (i.e., name, date and place of birth, home address). In addition, USSS collects and maintains photographs of individuals who are part of the BI process. Selectees are required to present valid, current government-issued identification with photographs, such as driver's license or passport, to SMD during the initial in-person security interview. In the event that social media searches result in multiple possible individuals, the vendor can use additional points of verification and photographs to identify the correct individual. Should social media checks reveal information of potential concern, USSS SMD will conduct additional in-person interviews as deemed necessary to address and/or mitigate any such concerns. Additionally, SMD will forward results of checks to law enforcement should they warrant further criminal or terrorism investigation.

All social media results will be sent electronically from the vendor to SMD via encrypted files. These results will be stored in the individual's official USSS personnel security background investigative file. Information is also stored and archived on the vendor's secure portal for no longer than 90 days, after which point the vendor's social media files will be deleted.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Under 5 U.S.C. § 1104, the Office of Personnel Management (OPM) has delegated to agencies the authority to conduct competitive examinations for positions in the competitive service, except for administrative law judge positions. USSS hiring authorities receive their delegated authority from OPM and have two fundamental responsibilities: to ensure that the agency's vacant positions are filled with the best-qualified persons from a sufficient pool of well-qualified eligible candidates; and to uphold the laws, regulations, and policies of merit selection (see 5 U.S.C. §§ 2301 and 2302). Further, the collection of information is authorized by Title 5 of the Code of Federal Regulations, (Administrative Personnel), Chapter 1, Subchapter B; parts 723. Finally, the Office of the Director of National Intelligence Security Executive Agent Directive 5[4] provides that agencies may choose to collect publicly available social media information in the

[4] *See* Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications (May 2016), available at https://www.dni.gov/files/NCSC/documents/Regulations/SEAD_5.pdf.

personnel security background investigation process as long as the information pertains to the adjudicative guidelines for making determinations of initial or continued eligibility for access to classified information or eligibility to hold a sensitive position.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The applicable SORN is DHS/ALL-023 Department of Homeland Security Personnel Security Management.[5]

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes, a system security plan has been documented for the USSS Messaging Capabilities System (MCS) by which social media checks will be transmitted, as well as for the underlying system that will be used to perform the social media checks. Additionally, USSS required the vendor to submit an IT Security Plan, which was verified by the Chief Information Security Officer.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. General Records Schedule (GRS) 5.6, Security Records, items 180/181, cover records about security clearances, and other records created to support initial favorable eligibility determinations, periodic reinvestigations, or to implement a continuous evaluation program.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

This information is not covered by the PRA.

[5] *See* DHS/ALL-023 Department of Homeland Security Personnel Security Management, (February 23, 2010) 75 FR 8088.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The categories of individuals from whom information will be collected are:

- Hiring selectees during the background investigation process;
- Staff who are undergoing periodic re-investigation or continuous evaluation; and
- Contractors who require access to USSS facilities and systems.

The PII that is collected and stored by the project will be consistent among the three categories of individuals.

SMD will provide the following information to the vendor about the individual:

- Name;
- Address;
- Date of birth;
- Place of birth; and
- Photographs, only if needed to identify a subject.

The vendor will only collect information from PAEI when it is indicative of criminal categories (i.e., unlawful sexual deviant behavior, unlawful violent behavior, and unlawful racist acts) or terrorism activities. The USSS SMD will obtain reports on the subject gathered from PAEI, including open social media networks, through digital and cyber analysis. Reports will contain a summary of findings and at least two matching identifiers of the hiring selectees, employee, or contractor. It will include screenshots with timestamps. Reports will include social media handles or other profile information. Depending on the site displayed in the report, the following PII could also be contained in reports:

- Full name;
- Phone number;
- Email address;
- Subject photo;
- Residential address;
- Age/Date of birth;

- Employer; and
- School attended.

If the vendor does not find any information that is indicative of the activities identified above, a "no pertinent information (NPI) found" report and the methodology sources used in inquiries will be generated. The vendor will not store any additional PII about the individual.

2.2 What are the sources of the information and how is the information collected for the project?

The sources of the information USSS SMD collects for its social media checks are limited to PAEI on the prospective or current employee or contractor (e.g., internet searches, viewing publicly available social media pages, Twitter feeds). Information on associates or family members will not be searched or included. The vendor will not be creating social media accounts in order to view information. The contractor does not view any pages other than those of the subject. SMD may use its investigative process and authorities to corroborate the PAEI and allow the subject to explain or refute any relevant information surfaced through the check.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The USSS SMD uses PAEI, which includes social media sources for investigative purposes, to address potential criminal or terrorism activities. USSS will adjudicate information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, or is otherwise lawfully accessible to the public.

2.4 Discuss how accuracy of the data is ensured.

The USSS SMD sends the vendor the name and address of the individual along with the date and place of birth to ensure that the correct individual is identified for the checks. These multiple verification points enhance the accuracy of the data retrieved. Further, the USSS SMD and the vendor will attempt to corroborate any information using other publicly available sources and photographs from Government-issued identification documents obtained as part of the initial security interview. Additionally, SMD may corroborate the PAEI by interviewing the subject.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the information collected from social media will be inaccurate, resulting in a negative outcome for hiring selectees, contractors, or employees undergoing reinvestigation.

Mitigation: The risk is partially mitigated. USSS strives to obtain the most accurate data available; however, there is always a risk that the information may be inaccurate. USSS SMD will attempt to corroborate any information using other publicly available sources, as it does during the mandatory BI process that SMD currently employs for criminal activity, financial activity, and terrorist activity. Photographs from Government-issued identification documents obtained as part of the initial security interview could be used in the corroboration process. Additionally, SMD could corroborate information by interviewing the subject. Should the checks reveal information of potential concern, USSS SMD will conduct additional interviews with the subject of the investigation as deemed necessary to address and/or mitigate any such concerns.

Privacy Risk: There is a risk that USSS or the vendor on USSS's behalf will collect and retain more information from social media than is necessary to make a suitability or clearance determination, including information about the subject's relatives or associates.

Mitigation: This risk is partially mitigated. All authorized USSS SMD and vendor personnel processing social media results complete privacy awareness and operational use of social media training. Only information that has use and value to USSS for the above delineated investigative purposes will be retained.

The USSS SMD will review processes, practices, and results monthly, at a minimum, to provide direct feedback to the vendor using telephonic or electronic communications.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The social media checks seek information relevant to an individual's eligibility to access national security information, USSS facilities, or systems. Specifically, the results will be used for investigative purposes to adjudicate in accordance with the adjudicative guidelines.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

No.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that the USSS will inappropriately use information gathered from social media sites under this effort.

Mitigation: This risk is mitigated. Neither USSS SMD personnel nor contract support will appropriate an online identity to interact with any individual whose information may be posted in the social media content. USSS personnel and contract support with access to social media are required to complete training and acknowledge rules of behavior for appropriate use of social media and publicly available information. The information collected is limited and specific in scope to results indicative of criminal or terrorism activities. Further, the use limitations cited in DHS Management Directive No: 11042.1 Safeguarding Sensitive but Unclassified Information will be strictly adhered to.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Notice concerning information collected and maintained in personnel security files is provided in DHS/ALL-023 Department of Homeland Security Personnel Security Management.[6] Additionally, in the course of a personnel security investigation, selectees, current employees, and certain contractors sign either a Standard Form (SF) 86 (selectees and current employees) or an SF 85 (contractors) that authorizes the collection of publicly available electronic information and provides notice that this collection will occur.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

When an individual signs the SF 85 or SF 86, he or she consents to a background investigation that may include searching PAEI. Individuals can opt out of the hiring/reinvestigation process at any time, but USSS will not be able to complete the investigation process. This will adversely affect the individual's eligibility for access/continued access.

Hiring selectees and current employees/contractors freely and voluntarily post publicly available information on social media sites or otherwise make information publicly available online. Individuals retain the right and the ability to refrain from making information public or, in

[6] *See* DHS/ALL-023 Department of Homeland Security Personnel Security Management, (February 23, 2010) 75 FR 8088.

most cases, to remove previously posted information from their respective social media accounts. In addition, individual users of social media may choose to keep private the information they share through their respective accounts.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not be on notice that information is being collected from social media sites.

Mitigation: This risk is mitigated in that all hiring selectees, current employees, and those contractors subject to the checks are provided notice during the application and reinvestigation process by signing a release for information that includes access to PAEI (SF86, SF85). Further, notice is provided by the publication of this PIA.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

After the results of the social media checks have been obtained by the vendor, the vendor will transmit the information to USSS SMD. The vendor will retain data for 90 days in encrypted form. After 90 days the vendor will destroy data and send confirmation to USSS regarding the destruction of data.

Consistent with GRS 5.6, items 180/181, USSS records relating to hiring selectees not issued clearances will be destroyed upon notification of death; or no later than five years after termination/expiration of the hiring selectee relationship or contract relationship, whichever is applicable. Records related to active employees will be managed by SMD in hard copy files, with GRS 5.6 retention prescribing records to be destroyed one year after the employee relationship ends; however, records may be retained longer if required for business use, and approved by both the USSS Chief of SMD and the USSS Records Officer.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that USSS SMD will retain social media information that is not applicable to eligibility and background investigation/reinvestigation determinations.

Mitigation: All authorized USSS SMD and vendor personnel processing social media results complete privacy and operational use of social media training. Only information that has use and value to USSS for above delineated investigative and adjudicated purposes will be retained.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

The previously listed identifiers are shared with the contractor to facilitate the checks. Once the results are received at USSS SMD, they will not be shared outside of DHS, unless the subject of the check seeks external review of a clearance action by an Inspector General panel or the results of the check are indicative of criminal or terrorism activity warranting further law enforcement investigation.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Identifiers will be provided to a third party (the contractor) so that they may be used in conducting checks relevant to determining eligibility for access to national security information. This sharing is consistent with routine uses as stated in the purpose for the collection of records in DHS/ALL-023 Department of Homeland Security Personnel Security Management February 23, 2010, 75 FR 8088, "processing of personnel security-related clearance actions, to record suitability determinations, to record whether security clearances are issued or denied, and to verify eligibility for access to classified information or assignment to a sensitive position."

6.3 Does the project place limitations on re-dissemination?

Results of the social media checks, once received from the vendor, are not re-disseminated to external agencies. Further, DHS Management Directive No: 11042.1 Safeguarding Sensitive But Unclassified Information will be strictly adhered to regarding re-dissemination.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

The USSS does not anticipate any disclosures outside of DHS. Once the results are received at USSS SMD, they will not be shared outside of DHS, unless the subject of the check seeks external review of a clearance action after having exhausted the internal review procedures.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the identifying information provided to the contractor and the results of the social media checks could be erroneously disclosed.

Mitigation: PII that will be shared with the contractor is restricted to the four items outlined above (name, address, date of birth, and place of birth). The information sharing restrictions and obligations are enforced through non-disclosure documents. In the event that searches result in multiple possible individuals, the vendor can use additional points of verification and photographs to identify the correct individual.

To mitigate the risk of social media check results being erroneously disclosed, the results of checks will be transmitted from the vendor to USSS using encrypted password protected electronic communications.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Information contained in the personnel security file is covered by the Privacy Act. Individuals may file a Privacy Act request to access their personnel security records. Access requests may be submitted in writing to the following address, as specified in the applicable SORNs:

USSS Freedom of Information Act/Privacy Act (FOIA/PA) Officer,
Communications Center (FOIA/PA),
245 Murray Lane,
Building T-5,
Washington, D.C. 20223,.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The procedures are the same as those outlined in 7.1.

7.3 How does the project notify individuals about the procedures for correcting their information?

The procedures for requesting the correction of information are specified in the applicable SORN[7] and on the Secret Service's public webpage.[8]

[7] *See* DHS/ALL-023 Department of Homeland Security Personnel Security Management February 23, 2010, 75 FR 8088.
[8] http://www.secretservice.gov/press/foia/request/.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that job selectee will not know how to access, correct, or amend his or her personnel security records.

Mitigation: All personnel security records are covered by the Privacy Act and fall under the DHS/ALL-023 Department of Homeland Security Personnel Security Management SORN. There are Privacy Act notices on all OPM applications to alert job selectees that their records are afforded Privacy Act protections.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

The USSS maintains files within the SMD in locked facilities. These files are secured by physical intrusion detection platforms. USSS compiles audit records from information system components in sufficient detail to facilitate the reconstruction of relevant events. IT managers identify critical functions to be audited and review audit findings. They also ensure that audit trails on all network devices (for example, routers, switches and servers) are regularly reviewed to ensure that only authorized activity is occurring on the networks. The USSS collects and compiles event logs from the email servers. Additionally, the USSS uses appropriate electronic tools and procedures to provide individual accountability, reconstruction of events, intrusion detection, and problem identification.

The vendor has signed a detailed Memorandum of Understanding (MOU) with USSS as well as nondisclosure agreements and rules of behavior, outlining its requirement to maintain the confidentiality of the results of information obtained on a job selectees, employee, or contractor. The vendor system has met the NIST 800-53 Appendix J privacy controls regarding "Use of External Information Systems." The vendor obligation is enforced in the MOU. The USSS will verify the implementation of the required security controls on this external system. Additionally, the vendor manually audits all of its reports to confirm matching identifier, scope of searches, and source(s) viewed before delivery of a final report.

The USSS SMD will review processes, practices, and results monthly, at a minimum, to provide direct feedback to the vendor using telephonic or electronic communications. The USSS SMD will consult with the USSS Privacy Office to mitigate any perceived or confirmed misuses of PII by the contractor or SMD. The MOU and contract provide SMD the ability to conduct its standard, in-person facility checks of vendor sites, as necessary.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

SMD provides security awareness training to information system users. The appropriate content of security awareness training and security awareness techniques is based on the SMD organizational requirements, and the information systems to which federal employee and contractors have authorized access. Privacy and IT Security Awareness Training required for all DHS personnel is included as a requirement in the signed MOU.

The vendor shall ensure that its employees performing under this contract and accessing USSS-supplied PII shall complete a USSS-delivered Privacy Training Course on Operational Social Media Use at the beginning of the contract and each option year thereafter as well as the required DHS Protecting Personal Information course. The vendor shall maintain documentation of employee training completions and shall provide it to USSS prior to receiving subject information and annually thereafter.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

The USSS has strict access agreement policies in place to include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized. Employees and contractors must sign the USSS Non-Disclosure Agreement (NDA) prior to initiating work on the contract.

The vendor has signed a detailed MOU with USSS outlining its ability to maintain the confidentiality of the results of information obtained on a hiring selectee, employee, or contractor. The vendor agrees to provide a signed copy of a NDA to SMD to indicate that the confidentiality of the search results is to be maintained.

USSS SMD will review processes, practices, and results monthly, at a minimum, to provide direct feedback to the vendor using telephonic or electronic communications. The MOU and contract provide SMD the ability to conduct its standard, in-person facility checks of vendor sites, as necessary.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

The governing MOU with the contractor was reviewed by the program manager and other staff within SMD, as well as the USSS Deputy CISO, Privacy Officer, and Counsel staff. Further, the contractor must abide by DHS policy and USSS procedures for information sharing as described above in Section 6 whereby USSS will verify the implementation of the required controls.

Responsible Officials

Michael Mullen
Managing Chief
Security Management Division
U.S. Secret Service

Approval Signature

[Original signed and on file with the DHS Privacy Office]

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security