SECURITY EXECUTIVE AGENT DIRECTIVE 5

COLLECTION, USE, AND RETENTION OF PUBLICLY AVAILABLE SOCIAL MEDIA INFORMATION IN PERSONNEL SECURITY BACKGROUND INVESTIGATIONS AND ADJUDICATIONS

(VERSION: 5.4 – 05 MAY 2016)

(EFFECTIVE: 12 MAY 2016)

A. AUTHORITY: The National Security Act of 1947, as amended; Intelligence Reform and Terrorism Prevention Act of 2004, as amended; Executive Order (EO) 10450, *Security Requirements for Government Employment*, as amended; EO 12968, *Access to Classified Information*, as amended; EO 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*; EO 13549, *Classified National Security Information Program for State, Local, Tribal and Private Sector Entities*; Performance Accountability Council Memorandum, *Assignment of Functions Relating to Coverage of Contractor Employee Fitness in the Federal Investigative Standards*, 6 December 2012; and other applicable provisions of law.

B. PURPOSE: This Security Executive Agent (SecEA) Directive addresses the collection and use of publicly available social media information during the conduct of personnel security background investigations and adjudications for determining initial or continued eligibility for access to classified national security information or eligibility to hold a sensitive position and the retention of such information. Nothing in this Directive prohibits agencies from conducting other legally permissible investigations or inquiries.

C. APPLICABILITY: This Directive applies to "authorized investigative agencies" and "authorized adjudicative agencies" as defined below. This directive also applies to "covered individuals," as defined below, seeking initial or continued eligibility for access to classified information or eligibility to hold a sensitive position.

D. DEFINITIONS: As used in this Directive, the following terms have the meanings set forth below:

1. "Agency": Any "executive agency" as defined in 5 U.S.C. §105, the "military departments," as defined in 5 U.S.C. §102, and any other entity within the executive branch that comes into possession of classified national security information or has positions designated as sensitive.

2. "Authorized adjudicative agency": An agency authorized by law, executive order, or designation by the SecEA to determine eligibility for access to classified information in accordance with EO 12968, as amended, or eligibility to hold a sensitive position.

3. "Authorized investigative agency": An agency authorized by law or regulation to conduct a counterintelligence investigation or investigation of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information.

4. "Classified national security information" or "classified information": Information that has been determined, pursuant to EO 13526, any predecessor or successor order, or the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

5. "Covered individual":

a. A person who performs work for or on behalf of the executive branch or who seeks to perform work for or on behalf of the executive branch, but does not include the President or (except to the extent otherwise directed by the President) employees of the President under 3 U.S.C. §105 or §107, the Vice President or (except to the extent otherwise directed by the Vice President) employees of the Vice President under 3 U.S.C. §106 or annual legislative branch appropriations acts;

b. A person who performs work for or on behalf of a state, local, tribal or private sector entity, as defined in EO 13549, but does not include duly elected or appointed governors of a state or territory, or an official who has succeeded to that office under applicable law;

c. A person working in or for the legislative or judicial branches and the investigation or determination is conducted by the executive branch, but does not include Members of Congress; Justices of the Supreme Court; and Federal judges appointed by the President.

d. Employees of the U.S. Government; industrial, commercial, or personal services contractors; licensees; certificate holders; grantees; experts or consultants; and all subcontractors or any other category of person who acts for or on behalf of the U.S. Government as determined by an appropriate U.S. Government official.

6. "Investigative record": The official record of all data obtained on the covered individual from Trusted Information Providers,[1] suitability and security applications and questionnaires, and any investigative activity conducted under the Federal Investigative Standards or as approved by the executive agent.

7. "Publicly available social media information": Any electronic social media information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line to the public, is available to the public by subscription or purchase, or is otherwise lawfully accessible to the public.

---

[1] As defined in the 2012 Federal Investigative Standards.

8. "Reasonably exhaustive efforts": The appropriate level of efforts to resolve issues or corroborate discrepant information. They may include multiple attempts or techniques to satisfy the issue, attempts to corroborate the activity through references from the background investigation, and/or attempts to obtain and pursue additional leads through other aspects of the investigation.

9. "Sensitive position": Any position within or in support of an agency in which the occupant could bring about, by virtue of the nature of the position, a material adverse effect on national security regardless of whether the occupant has access to classified information and regardless of whether the occupant is an employee, military service member, or contractor.

10. "Social media": Websites, applications, and web-based tools that allow the creation and exchange of user generated content. Through social media, people or groups can engage in dialogue, interact, and create, organize, edit, comment on, combine, and share content.

E. POLICY: Agencies may choose to collect publicly available social media information in the personnel security background investigation process, which pertains to the covered individual's associations, behavior and conduct, 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. Authorized investigative agencies may collect, use, and retain publicly available social media information as part of a covered individual's background investigation and, if collected, shall incorporate the relevant results in the investigative record. The period of coverage for publicly available electronic information will be consistent with the scope of the investigation.

2. Authorized adjudicative agencies may use and retain publicly available social media information when determining initial or continued eligibility of a covered individual for access to classified information or eligibility to hold a sensitive position.

3. Collection of publicly available social media information shall only be conducted after obtaining the signed *Authorization for Release of Information* form of the Standard Form 86, *Questionnaire for National Security Positions*, which includes notice of the collection of such information.

4. Only publicly available social media information pertaining to the covered individual under investigation shall intentionally be collected. Absent a national security concern, or criminal reporting requirement, information pertaining to individuals other than the covered individual will not be investigated or pursued. Information inadvertently collected relating to other individuals will not be retained unless that information is relevant to a security determination of the covered individual.

5. Covered individuals shall not be requested or required to:

   a. Provide passwords;

   b. Log into a private account; or

c. Take any action that would disclose non-publicly available social media information.

6. Agencies shall not create accounts or use existing accounts on social media for the purpose of connecting (e.g., "friend", "follow") to a covered individual or enlist the assistance of a third party in order to bypass privacy controls and/or access otherwise non-publicly available social media information. Agencies shall not request that a covered individual connect to an agency account or access their account from an agency system in order to provide access to information which would otherwise be protected from public view.

7. Authorized investigative agencies shall make reasonably exhaustive efforts to verify that any information collected that is discrepant or potentially disqualifying pertains to the covered individual. When publicly available social media information pertaining to the covered individual identifies discrepant information or potentially disqualifying issues relevant to one or more of the adjudicative guidelines, the investigation shall be expanded to fully resolve all issues.

8. Any potentially disqualifying issue(s) shall be adjudicated using the National Security Adjudicative Guidelines, reference 3. No unfavorable personnel security actions shall be taken solely on uncorroborated or unverified discrepant information collected pursuant to this Directive. When an adjudicative determination is made to deny or revoke eligibility for access to classified information or eligibility to hold a sensitive position, the covered individual shall be afforded the review proceedings in EO 12968, as amended, Part 5.

9. Agencies that use publicly available social media information pursuant to this policy shall reciprocally accept existing investigations or adjudications, that otherwise meet requirements for reciprocity, performed by an agency that does not collect or use publicly available social media information. The gaining agency may collect social media information on the covered individual pursuant to this policy.

F. RESPONSIBILITIES:

1. The SecEA is responsible for:

a. Development of standard requirements for the collection, use, and retention of information obtained from social media sources.

b. Ensuring policies and procedures governing the collection, use, and retention of publicly available social media information are in accordance with this Directive.

c. Issuing guidelines and instructions to ensure appropriate uniformity, efficiency, effectiveness, and timeliness in processes and procedures relating to the collection and use of publicly available social media information.

d. Overseeing policies and procedures governing uniform investigator and adjudicator training in the collection, use, and retention of publicly available social media information.

2. Heads of Agencies shall:

a. Inform the SecEA of their intent to collect, use, and retain publicly available social media information in determinations for persons requiring initial or continued eligibility for access to classified information or eligibility to hold a sensitive position.

b. Ensure that agency policies and procedures governing the collection, use, and retention of publicly available social media information are in accordance with all applicable laws, executive orders, and implementing guidance, and include appropriate protections for privacy and civil liberties, including any necessary changes to documentation required by applicable law (e.g., Privacy Impact Assessments required by the E-government Act or System of Records Notices required by the Privacy Act).

c. Ensure that the collection, analysis, reporting, and retrieval of publicly available social media information are automated to the greatest extent practicable.

d. Promptly advise the SecEA of any challenges or impediments to the implementation of this policy.

e. Ensure that authorized investigative and adjudicative personnel are provided training on the collection, use, and retention of publicly available social media information governed by this policy.

f. Act upon and share relevant information of a security, counterintelligence (CI), or law enforcement concern with appropriate security, CI, insider threat, or law enforcement officials.

g. Share best practices for more secure, effective, and efficient methods for the collection and use of publicly available social media information.

G. EFFECTIVE DATE: This Directive becomes effective on the date of signature.

James R. Clapper

12 MAY 2016
Date

REFERENCES

1. Security Policy Board, *Investigative Standards for Background Investigations for Access to Classified Information,* 24 March 1997, or its successor.
2. *Federal Investigative Standards,* December 2012, or its successor.
3. National Security Council, *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information,* 29 December 2005, or its successor (the "National Security Adjudicative Guidelines").
4. 2012 *National Training Standards*, or its successor.