



## SECURITY EXECUTIVE AGENT DIRECTIVE 2

### (U) USE OF POLYGRAPH IN SUPPORT OF PERSONNEL SECURITY DETERMINATIONS FOR INITIAL OR CONTINUED ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION OR ELIGIBILITY TO HOLD A SENSITIVE POSITION

(EFFECTIVE: 14 SEPTEMBER 2014)

**A. (U) AUTHORITY:** The Intelligence Reform and Terrorism Prevention Act of 2004; Executive Order (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*; EO 10450, *Security Requirements for Government Employment*; Security Executive Agent Directive 1, *Security Executive Agent Authorities and Responsibilities*; Performance Accountability Council Memorandum, dated 6 December 2012, *Assignment of Functions Relating to Coverage of Contractor Employee Fitness in the Federal Investigative Standards*; and other applicable provisions of law.

**B. (U) PURPOSE:** This Security Executive Agent (SecEA) Directive establishes policy and assigns responsibilities governing the use of polygraph examinations conducted by agencies in support of personnel security vetting for initial or continued eligibility for access to classified information or eligibility to hold a sensitive position. Polygraph examinations conducted for any reason other than those stated above, including examinations in connection with criminal law investigations and suitability determinations, are not covered by this Directive. Nothing in this Directive alters any requirements imposed by the Employee Polygraph Protection Act (EPPA) (29 U.S.C. 2001, et seq.), the Presidential and Executive Office Accountability Act (3 U.S.C. 401, 414), the Congressional Accountability Act (2 U.S.C. 1301, 1314), the Privacy Act (5 U.S.C. 552a), executive branch agencies' System of Records Notices (SORNs) published in the Federal Register, or any other provision of law related to the use of polygraph examinations (e.g., Title 10 U.S.C. 1564a); nor may implementation of this policy conflict with the requirements of any such law or SORNs. Nothing in this Directive should be construed to limit the legal authorities of the Director of National Intelligence (DNI) or the heads of agencies, or the role of the Director of the Office of Personnel Management (OPM) under Civil Service Law and executive orders related to the use of polygraph in connection with investigations for employment in the competitive service.

**C. (U) APPLICABILITY:** This Directive applies to any executive branch agency that conducts polygraph examinations in support of personnel security vetting for initial or continued eligibility for access to classified information or eligibility to hold a sensitive position, seeks to expand an existing polygraph program for such purpose, or intends to establish a new program for such purpose.

**D. (U) DEFINITIONS:** For the purpose of this Directive, the following definitions apply:

1. (U) "Agency": Any "Executive Agency" as defined in Section 105 of Title 5, United States Code, including the "military departments," as defined in Section 102 of Title 5, United States Code, and any other entity within the executive branch that comes into possession of classified national security information or has positions designated as sensitive.

2. (U) "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.

3. (U) "Counterintelligence Scope Polygraph" (CSP): A polygraph examination that includes counterintelligence (CI) topics concerning involvement in espionage, sabotage, or terrorism; unauthorized disclosure or removal of classified information (including to the media); unauthorized or unreported foreign contacts; and deliberate damage to or malicious misuse of U.S. government information or defense systems.

4. (U) "Expanded Scope Polygraph" (ESP): A polygraph examination that includes all CI topics of the CSP, as well as the topics of criminal conduct, drug involvement, and falsification of security questionnaires and forms. (The ESP examination has also been referred to as a Full Scope Polygraph [FSP] or an Expanded Scope Screening [ESS] examination in some organizations.)

5. (U) "Personnel Security Vetting": The investigation of an individual in accordance with applicable Federal Investigative Standards, the results of which are reviewed in accordance with applicable adjudicative guidelines in order to render a determination of the individual's eligibility for initial or continued access to classified information or eligibility to occupy a sensitive position.

6. (U) "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.

7. (U) "Specific Issue Polygraph" (SIP): An examination conducted to address an individual issue of adjudicative concern such as espionage, sabotage, unauthorized disclosure of classified information, criminal conduct, etc. This examination may be used in conjunction with a CSP or ESP.

**E. (U) POLICY:**

1. (U) Agency heads are responsible for establishing and maintaining an effective program to ensure that access to classified information or placement in a sensitive position is clearly consistent with the interests of the national security. When an agency head elects to use the polygraph for personnel security vetting as defined in Section D, this policy will apply, consistent with the EPPA and other applicable laws and regulations.



2. (U) CSP examinations represent the baseline for the application of polygraph in support of personnel security vetting. Heads of agencies may authorize the use of the CSP for the purposes stated above in Section B when deemed to be in the interest of national security. CSPs may be used in support of determinations of initial eligibility for access to classified information and initial eligibility to hold a sensitive position, thereafter in support of reinvestigations or continuous evaluation, and administered at periodic or aperiodic intervals.

3. (U) SecEA and National Center for Credibility Assessment (NCCA) notification is required prior to an agency initiating a program using CSP or ESP examinations in support of personnel security vetting.

4. (U//~~FOUO~~) Nothing in this Directive prohibits agencies currently conducting ESP examinations in support of personnel security vetting (Central Intelligence Agency, National Security Agency, Federal Bureau of Investigation, the United States Secret Service, and Naval Criminal Investigative Service) from continuing to conduct ESP examinations, nor does this Directive alter an agency head's authority to continue an existing CSP program or institute a new CSP or ESP program, consistent with guidance in Section E.3.

5. (U) SIP examinations may be conducted to attempt to resolve known or developed information of adjudicative significance.

6. (U) An ESP or CSP examination conducted in accordance with this Directive—which is an element of a favorable national security adjudication *and is current and consistent with the type and age of examination required by the receiving agency*—shall be reciprocally accepted.

7. (U) Heads of agencies shall adhere to the following principles in administering their personnel security polygraph programs:

a. (U) Polygraph examination types and their completion dates shall be recorded in Scattered Castles, the Joint Personnel Adjudication System within the Department of Defense, or the Central Verification System database within the U.S. Office of Personnel Management, or successor databases, unless authorized by the SecEA to withhold information from the database for national security purposes.

b. (U) A signed consent form explaining the purpose and uses of any information disclosed as part of the examination shall be obtained from the examinee prior to each polygraph session.

c. (U) Refusal, without reasonable cause (as determined by the agency), to undergo or failure to cooperate during a polygraph examination or purposeful non-cooperation, including confirmed polygraph countermeasures, may result in an additional review and a potential adverse security determination regarding the individual's eligibility for access to classified information or eligibility to hold a sensitive position.

d. (U) Questions used in polygraph examinations, except for technical and diagnostic questions, shall cover the topic areas for the specific type of polygraph as defined in Section D and shall be limited to adjudicatively relevant national security matters.

e. (U) Agencies conducting polygraph examinations shall act upon and share relevant reported information of law enforcement, security, or CI concern with appropriate law enforcement, security, and CI officials consistent with informed consent pursuant to Section E.7 (b).

f. (U) All polygraph programs shall include standardized training and educational certification of polygraph examiners to ensure consistency, reciprocity, and a fair process. All examiners shall receive initial training from the NCCA and undergo educational certification processes as well as advanced or refresher polygraph training as defined by their agency consistent with NCCA standards.

8. (U) Polygraph programs shall undergo NCCA quality assurance audits on a biennial basis.

**F. (U) RESPONSIBILITIES:**

1. (U) The DNI as the SecEA is responsible for:

a. Establishing guidelines and minimum standards for personnel security polygraph programs.

b. Establishing the notification and NCCA review process for agencies seeking to initiate a polygraph program utilizing the CSP or ESP.

c. Establishing the notification process for agencies incorporating an ESP examination into an existing CSP program.

d. Maintaining a Polygraph Expert Working Group to review and address issues relating to the polygraph as they arise.

2. (U) NCCA is the office of primary responsibility for polygraph examiner education and training, continuing education certification, audits of agencies' quality assurance programs against federal standards, and credibility research.

3. (U) Heads of agencies shall:

a. Notify SecEA and NCCA of their intention to implement a CSP or ESP program, and ensure consistency with NCCA certification, education and training requirements. (Notification of program expansion is not required.)

b. Implement the provisions of this Directive within their respective organization as applicable, ensuring compliance with EPPA.

c. Ensure policies and procedures governing the collection and use of polygraph-derived information are in accordance with all applicable laws and executive orders and include appropriate protections for privacy and civil liberties.

d. Ensure compliance with the standards of polygraph program supervision and quality control consistent with NCCA guidelines.

e. Coordinate polygraph-related research with NCCA to enhance the effectiveness of the polygraph and other credibility assessment programs.

f. Maintain agreements with NCCA, as needed, to ensure reimbursement to NCCA consistent with existing appropriations laws.

**G. (U) EFFECTIVE DATE:** This Directive is effective on the date of signature.

  
James R. Clapper

14 September 2014  
Date