INTELLIGENCE COMMUNITY POLICY GUIDANCE

704.6

04 February 2015

Conduct of Polygraph Examinations for Personnel Security Vetting

A. AUTHORITY: The National Security Act of 1947, as amended; Executive Order (EO) 12333, as amended; EO 12968, as amended; EO 13467; EO 13526; Security Executive Agent Directive 2; and other applicable provisions of law.

B. PURPOSE: This Intelligence Community (IC) Policy Guidance establishes policy for the conduct of polygraph examinations supporting personnel security vetting within the IC and implements Security Executive Agent Directive 2, *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.*

C. APPLICABILITY

1. This Guidance applies to the IC, as defined by the National Security Act of 1947, as amended, and to such elements of any other department or agency as may be designated an element of the IC by the President, or jointly by the Director of National Intelligence (DNI) and the head of the department or agency concerned.

2. This Guidance establishes policy and assigns responsibilities governing the use of polygraph examinations conducted by IC elements in support of personnel security vetting. Polygraph examinations conducted for any reason other than personnel security vetting, including examinations in connection with criminal law investigations or suitability determinations, are not covered by this Guidance.

D. GUIDANCE

1. When deemed to be in the interest of national security, heads of IC elements may authorize the use of the polygraph examination as a component of their personnel security vetting programs.

2. There are three types of polygraph examinations which may be used as a component of personnel security vetting programs: Counterintelligence (CI) Scope Polygraph (CSP) examinations, Expanded Scope Polygraph (ESP) examinations, and Specific Issue Polygraph (SIP) examinations.

3. CSP examinations may be conducted as part of initial personnel security vetting and may be administered at periodic or aperiodic intervals in support of reinvestigations or continuous evaluation. CSP examinations shall cover the topics of espionage, sabotage, 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 systems or defense systems.

4. ESP examinations may be conducted as part of initial personnel security vetting and may be administered at periodic or aperiodic intervals in support of reinvestigations or continuous evaluation. ESP examinations shall cover the CSP topics plus 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 IC organizations.

5. SIP examinations may be conducted to resolve an individual issue of adjudicative concern such as espionage, sabotage, unauthorized disclosure of classified information, or criminal conduct or to aid in CI investigations. The SIP examination may be used in conjunction with CSP or ESP examinations.

6. Any possible violations of law shall be reported responsibly and expeditiously, in accordance with DNI Executive Correspondence E/S 2014-00402, *Reporting Possible Violations of Federal and State Criminal Law* (see Appendix A).

7. CSP and ESP examinations for the IC shall specifically include the issue of unauthorized disclosures of classified information during pre-examination explanations by incorporating a definition that explicitly states that an unauthorized disclosure means unauthorized communication or physical transfer of classified information to an unauthorized recipient. Further, pre-examination explanations will define "protected disclosure" as defined in ICD 120, *Intelligence Community Whistleblower Protection*. The polygraph examiner shall thoroughly explain this issue to the examinee and include the following details:

a. "Unauthorized recipient" includes any U.S. person or foreign national without a need to know or not cleared at the appropriate level for the information, including any member of the media.

b. "Unauthorized disclosure" means a communication, confirmation, acknowledgement, or physical transfer of classified information, including the facilitation of, or actual giving, passing, selling, or publishing of or in any way making such information available to an unauthorized recipient.

c. Classified information includes information classified at any level pursuant to EO 13526, *Classified National Security Information*, including Confidential, Secret, or Top Secret.

8. All polygraph examinations for personnel security vetting within the IC shall be conducted in accordance with this Guidance, applicable laws, and regulations.

9. CSP and ESP examinations may only be conducted by IC elements with programs that comply with the National Center for Credibility Assessment (NCCA) standards, education, and training requirements. Examinations conducted consistent with Security Executive Agent Directive 2, Section E.6; NCCA standards; and this Guidance shall be reciprocally accepted.

10. Pre-examination explanations shall contain the requisite level of detail to ensure a thorough review of the topic, ensuring that the examinee understands the full meaning and implications of each topic. Examination questions will be formulated based upon pre-examination discussion and consistent with agency and NCCA guidance.

11. Polygraph examinations for joint duty, rotational, detail, task force, or similar assignments requiring mobility in support of IC mission requirements shall be conducted in accordance with ICD 709, *Reciprocity for IC Personnel Mobility*.

E. PRINCIPLES OF POLYGRAPH: IC elements shall adhere to the following principles in administering their polygraph programs:

1. Polygraph examination types and their completion dates shall be recorded in Scattered Castles or successor systems, unless otherwise authorized by the DNI.

2. 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.

3. The following activities could result in additional review or an adverse security determination regarding the individual's eligibility for access to classified information:

a. refusal, without reasonable cause (as determined by the head of the IC element), to undergo a polygraph examination;

b. failure to cooperate during a polygraph examination; or

c. purposeful non-cooperation during a polygraph examination, including confirmed use of polygraph countermeasures.

4. Questions used in polygraph examinations, except for technical and diagnostic questions, shall be relevant to established national adjudicative guidelines and shall cover only the topic areas identified in this Guidance for the type of polygraph in question.

5. IC elements conducting polygraph examinations shall act upon and share relevant reported information of law enforcement, security, or CI concerns with appropriate officials consistent with D.6 of this Guidance, in accordance with civil liberties and privacy protections, and in accordance with the consent form signed by the examinee pursuant to Section E.2 of this Guidance.

6. Polygraph programs shall include standardized training and educational certification of polygraph examiners to ensure consistency, fair process, and reciprocity. 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 department or agency consistent with NCCA standards.

7. Polygraph programs shall undergo NCCA quality assurance audits on a biennial basis.

F. ROLES AND RESPONSIBILITIES

1. The Director of the National Counterintelligence and Security Center (D/NCSC) may, in addition to any guidance issued pursuant to SEAD 2:

a. Establish the process and procedures for IC elements to notify the DNI and the NCCA of the initiation of a polygraph program; and

b. Establish the notification process for agencies incorporating an ESP examination into an existing CSP program.

2. Heads of IC elements shall:

a. Notify the DNI and NCCA of their planned implementation of a new CSP or ESP program in accordance with the process and procedures established by the D/NCSC.

b. Ensure CSP and ESP programs are conducted consistent with NCCA standards, education, and training requirements as well as applicable Departmental guidance.

c. Ensure internal policies and procedures governing the collection and use of polygraph-derived information are in accordance with all applicable laws, Executive Orders, DNI policies, and whistleblowing, civil liberties, and privacy regulations.

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

e. Coordinate polygraph-related research with the D/NCSC and the 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. EFFECTIVE DATE: This Policy Guidance becomes effective on the date of signature.

James R. Clapper — 4 Feb 2015

Director of National Intelligence — Date

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

E/S 2014-00402

MEMORANDUM FOR: Distribution

SUBJECT: Reporting Possible Violations of Federal and State Criminal Law

AUTHORITIES:

A. Title 28, United States Code, Section 535(b)
B. Executive Order 12333, as amended, *United States Intelligence Activities*, 30 Jul 08
C. Executive Order 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, 30 Jun 08
D. Executive Order 12968, as amended, *Access to Classified Information*
E. *Intelligence Reform and Terrorism Prevention Act of 2004*, Section 3001
F. Memorandum of Understanding, *Reporting of Information Concerning Federal Crimes*, August 1995
G. Office of the Attorney General Memorandum, 14 Sept 07

The Inspector General of the Intelligence Community (IC) has completed a report related to polygraph examinations and the crimes reporting process, finding that there is a need to ensure that IC elements have appropriate policies regarding the reporting of possible federal and state crimes. The IC is committed to upholding and being accountable to the law. Responsible and consistent crime reporting is a fundamental part of this duty.

Title 28, United States Code, Section 535(b) imposes a statutory duty to report federal criminal activity to the Attorney General, and the 1995 Memorandum of Understanding (MOU), *Reporting of Information Concerning Federal Crimes* sets forth the procedures by which each element of the IC shall report to the Department of Justice and to federal investigative agencies information concerning possible federal crimes by employees of an intelligence agency or organization, or violations of specified federal criminal laws by any other person. IC elements shall ensure, including through written policies or procedures, that suspected federal crimes are reported to the Department of Justice consistent with the MOU and in a responsible and expeditious manner.

In addition, IC elements shall ensure that their policies or procedures provide for the reporting of possible violations of the Uniform Code of Military Justice to the Secretary of the military department concerned or the Secretary of Defense, and the applicable military criminal investigative organization in coordination with their Office of General Counsel (OGC).

SUBJECT: Reporting Possible Violations of Federal and State Criminal Law

Finally, IC elements shall ensure that their policies or procedures provide for responsible and expeditious reporting of facts that reasonably indicate the planning for or commission of state, local or tribal felony crimes identified during the process of determining an individual's eligibility for access to classified information in accordance with Executive Order 12968, *Access to Classified Information*. IC element policies and procedures shall provide for notification to the IC element's OGC and Inspector General, and for reporting to the appropriate state, local, and tribal authorities in coordination with the IC element's OGC and consistent with the terms of Standard Form 86, *Questionnaire for National Security Positions*, which provides assurances that responses and information derived from truthful responses pertaining to drug use and activity, and certain use of information technology systems will not be used as evidence in criminal proceedings.

In accordance with the above, IC elements shall review and, as necessary, update their training requirements to ensure employees are knowledgeable of and in compliance with the element's policies and procedures for reporting information regarding possible violations of federal criminal laws or of state, local or tribal felony criminal laws.

Nothing in this Executive Correspondence shall be construed to limit other crimes reporting responsibilities. Additionally, this Executive Correspondence does not in itself create any cause of action or right of relief for any party.

My point of contact on this matter is James A. Smith, Director for Policy at (703) 275-3097.

James R. Clapper

James R. Clapper

3 Jul 2014

Date

SUBJECT: Reporting Possible Violations of Federal and State Law

Distribution:
Director, Central Intelligence Agency
Director, Defense Intelligence Agency
Director, National Security Agency
Director, National Reconnaissance Office
Director, National Geospatial-Intelligence Agency
Deputy Chief of Staff, G-2, U.S. Army
Director of Naval Intelligence, U.S. Navy
Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance, A2, U.S. Air Force
Director of Intelligence, U.S. Marine Corps
Executive Assistant Director, National Security Branch, Federal Bureau of Investigation
Assistant Commandant for Intelligence and Criminal Investigations, CG-2, U.S. Coast Guard
Under Secretary of Defense for Intelligence, OUSDI
Assistant Secretary, Bureau of Intelligence and Research, Department of State
Assistant Secretary, Office of Intelligence and Analysis, Department of the Treasury
Chief, Intelligence Division, Drug Enforcement Administration
Under Secretary, Intelligence and Analysis, Department of Homeland Security
Director, Office of Intelligence and Counterintelligence, Department of Energy
Joint Staff Director for Intelligence, J2, Vice Chairman of the Joint Chiefs of Staff