The table of contents for this title is as follows:

TITLE V—PREVENTING UNAUTHORIZED DISCLOSURES OF CLASSIFIED INFORMATION

Sec. 501. Notification regarding the authorized public disclosure of national intelligence.
Sec. 502. Requirement to record authorized disclosures of classified information.
Sec. 503. Procedures for conducting administrative investigations of unauthorized disclosures.
Sec. 504. Assessment of procedures for detecting and preventing unauthorized disclosures.
Sec. 505. Prohibition on certain individuals serving as consultants.
Sec. 506. Limitation on persons authorized to communicate with the media.
Sec. 507. Responsibilities of intelligence community personnel with access to classified information.
Sec. 508. Report on improvements to the criminal process for investigating and prosecuting unauthorized disclosures of classified information.
Sec. 509. Improving insider threat initiatives.
Sec. 510. Automated insider threat detection program.
Sec. 511. Surrender of certain benefits.
Sec. 512. Prohibition on security clearances for individuals who disclose to the public evidence or information on United States covert actions.

TITLE V—PREVENTING UNAUTHORIZED DISCLOSURES OF CLASSIFIED INFORMATION

SEC. 501. NOTIFICATION REGARDING THE AUTHORIZED PUBLIC DISCLOSURE OF NATIONAL INTELLIGENCE.

(a) NOTIFICATION.—Concurrent with an authorized disclosure of national intelligence or intelligence related to national security to the persons or entities described in subsection (b), the government official responsible for authorizing the disclosure shall submit to the congressional intelligence committees a notification of the disclosure if—
(1) at the time of the disclosure—

(A) such intelligence is classified; or

(B) is declassified for the purpose of the disclosure; and

(2) the disclosure will be made by an officer, employee, or contractor of the Executive branch.

(b) Persons or Entities Described.—The persons or entities described in this subsection are as follows:

(1) Media personnel, including any person or entity under contract or other binding agreement with the media to provide analysis or commentary.

(2) Any person or entity, if the disclosure described in subsection (a) is made with the intent or knowledge that such information will be made publicly available.

(c) Content.—Each notification required under subsection (a) shall—

(1) provide the specific title and authority of the individual authorizing the disclosure;

(2) if applicable, provide the specific title and authority of the individual who authorized the declassification of the intelligence disclosed; and

(3) describe the intelligence disclosed, including the classification of the intelligence prior to its dis-
closure or declassification and the rationale for making the disclosure.

(d) EXCEPTION.—The notification requirement in this section does not apply to a disclosure made—

(1) pursuant to any statutory requirement, including to section 552 of title 5, United States Code (commonly referred to as the “Freedom of Information Act”);

(2) in connection with a civil, criminal, or administrative proceeding;

(3) as a result of a declassification review process under Executive Order 13526 (50 U.S.C. 435 note) or any successor order; or

(4) to any officer, employee, or contractor of the Federal government or member of an advisory board to an element of the intelligence community who possesses an active security clearance and a need to know the specific national intelligence or intelligence related to national security, as defined in section 3(5) of the National Security Act of 1947 (50 U.S.C. 401a(5)).

SEC. 502. REQUIREMENT TO RECORD AUTHORIZED DISCLOSURES OF CLASSIFIED INFORMATION.

(a) RECORD REQUIREMENT.—The head of each element of the intelligence community shall ensure that such
element creates and maintains a record of all authorized
disclosures of classified information to media personnel,
including any person or entity under contract or other
binding agreement with the media to provide analysis or
commentary, or to any person or entity if the disclosure
is made with the intent or knowledge that such informa-
tion will be made publicly available.

(b) Review by Congressional Intelligence
Committees.—A record under subsection (a) shall be
available for review by the congressional intelligence com-
mittees in a manner jointly agreed to by the committee
and the head of such element.

SEC. 503. PROCEDURES FOR CONDUCTING ADMINISTRA-
TIVE INVESTIGATIONS OF UNAUTHORIZED
DISCLOSURES.

(a) Requirement.—Not later than 90 days after the
date of the enactment of this Act, the Director of National
Intelligence shall—

(1) establish procedures as described in sub-
section (b); and

(2) provide a copy of the procedures to the con-
gressional intelligence committees.

(b) Procedures.—The procedures described in this
subsection are procedures that shall be implemented by
each element of the intelligence community for the conduct
of administrative investigations of unauthorized disclosures of classified information and shall include—

(1) designation of an office with responsibility for proactively identifying unauthorized disclosures of classified information;

(2) submission and prioritization of crimes reports to the Attorney General for purposes of criminal investigation concerning unauthorized disclosures of classified information;

(3) conduct of independent administrative investigations of unauthorized disclosures of classified information, if a criminal investigation is not pursued or is discontinued;

(4) guidelines approved by the Attorney General that authorize the Director of the Federal Bureau of Investigation to provide relevant documents and other information in the Director’s possession to appropriate elements of the intelligence community for purposes of conducting administrative investigations of the unauthorized disclosure of classified information;

(5) procedures for the heads of elements of the intelligence community to apply disciplinary measures, if appropriate, following an administrative in-
vestigation, up to and including termination of em-
ployment;

(6) in cases where an administrative investiga-
tion identifies information that may enable or inform
a criminal investigation, procedures for providing
such information to the Attorney General;

(7) procedures for keeping the National Coun-
terintelligence Executive and the congressional intel-
ligence committees informed of the status of all ad-
ministrative investigations and crimes reports; and

(8) other procedures as determined by the Di-
rector.

SEC. 504. ASSESSMENT OF PROCEDURES FOR DETECTING
AND PREVENTING UNAUTHORIZED DISCLOSURES.

(a) DIRECTOR OF NATIONAL INTELLIGENCE ASSESS-
MENT.—Not later than 120 days after the date of the en-
actment of this Act, the Director of National Intelligence
shall provide the congressional intelligence committees
with an assessment of—

(1) the practical feasibility of extending the use
of the polygraph to additional Executive branch per-
sonnel and standardizing the questions used during
polygraph examinations regarding disclosure of clas-
sified information and contact with the media;
(2) the benefits of extending the automated insider threat detection capabilities described in section 402 of the Intelligence Authorization Act of Fiscal Year 2011 (Public Law 112–18; 50 U.S.C. 403–1 note) to sensitive compartmented information level computer systems used by agencies or personnel outside the intelligence community; and

(3) a description of actions that could be taken to address improper classification of material.

(b) Inspector General of the Intelligence Community Assessment.—Not later than 120 days after the date of the enactment of this Act, the Inspector General of the Intelligence Community shall provide the congressional intelligence committees with an assessment of the effectiveness of the process used by each element of the intelligence community for preventing, detecting, and investigating unauthorized disclosures of classified information and a description of any best practices that could be replicated throughout the intelligence community.

SEC. 505. PROHIBITION ON CERTAIN INDIVIDUALS SERVING AS CONSULTANTS.

(a) Prohibition.—No person described in subsection (b) may enter into a contract or other binding agreement with the media in order to provide, or otherwise assist in providing, analysis or commentary on matters
concerning the classified intelligence activities of any element of the intelligence community or intelligence related to national security, as defined in section 3(5) of the National Security Act of 1947 (50 U.S.C. 401a(5)).

(b) PERSON DESCRIBED.—A person described in this subsection is—

(1) any officer, employee, or contractor of the Federal government who possesses an active security clearance;

(2) any member of an advisory board to an element of the intelligence community who possesses an active security clearance; or

(3) any former officer, employee, or contractor of the Federal government or former member of an advisory board to an element of the intelligence community who—

(A) has left the employment or service of the Federal government during the previous 1 year period; and

(B) possessed a security clearance allowing access to top secret, sensitive compartmented information at any time during the 3 years prior to leaving such employment or service.
SEC. 506. LIMITATION ON PERSONS AUTHORIZED TO COMMUNICATE WITH THE MEDIA.

(a) LIMITATION.—

(1) IN GENERAL.—For each element of the intelligence community, only the Director and Deputy Director of such element, or individuals in equivalent positions within such element, and individuals in the offices of public affairs who are specifically designated by the Director (or the individual in an equivalent position), may provide background or off-the-record information regarding intelligence activities to the media, or to any person affiliated with the media.

(2) DESIGNATION IN WRITING.—Each designation made under paragraph (1) by a Director (or an individual in an equivalent position) shall be in writing.

(b) CONSTRUCTION.—Nothing in this section shall be construed to prohibit an appropriate officer or employee of an element of the intelligence community from providing authorized, unclassified, on-the-record briefings to the media, or to any person affiliated with the media.
SEC. 507. RESPONSIBILITIES OF INTELLIGENCE COMMUNITY PERSONNEL WITH ACCESS TO CLASSIFIED INFORMATION.

(a) In General.—Not later than 120 days after the date of the enactment of this Act, the Director of National Intelligence shall—

(1) prescribe regulations outlining the responsibilities of, and a process for, all covered persons to report oral and written contact with the media to the security office of the appropriate element of the intelligence community;

(2) prescribe regulations that ensure that any covered person, prior to leaving the employment or services of the Federal Government, is informed of the ongoing responsibility to comply with all provisions of the written nondisclosure agreements governing access to classified information;

(3) establish appropriate requirements for covered persons to comply, during and subsequent to any period of employment, with all prepublication review requirements contained in any nondisclosure agreement between the covered person and any and all elements of the intelligence community to which such person has been assigned, employed, contracted, or detailed;
(4) establish appropriate requirements for covered persons, during and subsequent to any period of employment or service, to submit any written materials and anticipated oral comments for prepublication review;

(5) update, and require current acknowledgment of, the written nondisclosure agreements governing access to classified information to comply with the provisions of this Act; and

(6) prescribe regulations that specify appropriate disciplinary actions to be taken against any covered person, during and subsequent to any period of employment or service, determined by the Director of National Intelligence to have violated a written agreement under this section, which may include—

(A) issuance of letters of reprimand;

(B) placing notices of violations in personnel files and informing the congressional oversight committees of such notices;

(C) revocation of security clearances;

(D) prohibition on obtaining new security clearances; and

(E) termination of employment.
(b) COVERED PERSON DEFINED.—In this section, the term “covered person” means a current employee or contractor of, or member of an advisory board to, an element of the intelligence community who has an active security clearance.

SEC. 508. REPORT ON IMPROVEMENTS TO THE CRIMINAL PROCESS FOR INVESTIGATING AND PROSECUTING UNAUTHORIZED DISCLOSURES OF CLASSIFIED INFORMATION.

(a) REQUIREMENT FOR REPORT.—Not later than 180 days after the date of the enactment of this Act, the Attorney General, in coordination with the Director of National Intelligence, shall submit to the congressional intelligence committees and the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives a report on the effectiveness of and potential improvements to the process for investigating and prosecuting unauthorized disclosures of classified information, which shall include—

(1) potential modifications to the process used by elements of the intelligence community to submit crimes reports of unauthorized disclosures of classified information to the Attorney General;

(2) potential modifications to the policies of the Department of Justice on issuing subpoenas directed
at members of the news media, as described in section 50.10(b) of title 28, Code of Federal Regulations (or any similar successor regulation); and

(3) potential modifications to the Classified Information Procedures Act (Public Law 96–456; 94 Stat. 2025).

SEC. 509. IMPROVING INSIDER THREAT INITIATIVES.

(a) DESIGNATION OF INSIDER THREAT PROGRAM MANAGERS.—

(1) Requirement to designate.—Not later than 90 days after the date of the enactment of this Act, each head of an element of the intelligence community shall designate an insider threat program manager with responsibility for developing a comprehensive insider threat program management plan as described in subsection (b) for such element.

(2) Information access.—Each insider threat program manager designated under paragraph (1) for an element of the intelligence community shall have access to all relevant information regarding the allocation of resources to efforts by such element to counter insider threats, including resources for counterintelligence, physical security, information security, and human resources, except that such relevant information shall not be deemed
to include information concerning specific counter-
intelligence or security investigations, unless the 
head of the element so directs.

(b) Development of a Comprehensive Insider
Threat Program Management Plan.—

(1) Requirement to develop.—Not later 
than 1 year after the date of the enactment of this 
Act, each insider threat program manager des-
ignated under subsection (a)(1) for an element of 
the intelligence community shall develop, in coordi-
nation with the Office of the National Counterintel-
ligence Executive and such other components of the 
Office of the Director of National Intelligence as the 
Director of National Intelligence deems appropriate, 
a comprehensive insider threat program manage-
ment plan for such element that describes a com-
prehensive insider threat detection program for such 
element.

(2) Review and approval.—Upon completion, 
each comprehensive insider threat program manage-
ment plan developed under paragraph (1) shall be 
submitted to the head of the relevant element of the 
intelligence community for review, modification, and 
approval, and then to the Director of National Intel-
ligence, for review, modification and approval.
(3) Submission to Congress.—A copy of each comprehensive insider threat program management plan approved by the Director of National Intelligence under paragraph (2) shall be submitted—

(A) to the congressional intelligence committees, not later than 30 days after the date such plan is approved; and

(B) if such plan involves a component of a department of the United States Government, to the committees of the Senate and of the House of Representatives with jurisdiction over such department simultaneously with submission of such copy to the congressional intelligence committees under subparagraph (A).

(c) Implementing a Comprehensive Insider Threat Detection Program.—

(1) Initial operating capability.—Not later than 18 months after the date of the enactment of this Act, each head of an element of the intelligence community, in coordination with the Office of the National Counterintelligence Executive and the Office of the Director of National Intelligence, shall establish an initial operating capability for the comprehensive insider threat detection program for such element as described in the comprehensive insider
threat program management plan developed under subsection (b).

(2) **FULL OPERATING CAPABILITY.**—Not later than 2 years after the date of the enactment of this Act, the Director of National Intelligence shall—

(A) establish a full operating capability for each comprehensive insider threat detection program developed under subsection (b) for each element of the intelligence community; and

(B) ensure that each such full operating capability is reached.

**SEC. 510. AUTOMATED INSIDER THREAT DETECTION PROGRAM.**

Section 402 of the Intelligence Authorization Act for Fiscal Year 2011 (Public Law 112–18; 50 U.S.C. 403–1 note) is amended—

(1) in subsection (a), by striking “October 1, 2012,” and inserting “October 1, 2013,”; and

(2) in subsection (b), by striking “October 1, 2013,” and inserting “October 1, 2014,”.

**SEC. 511. SURRENDER OF CERTAIN BENEFITS.**

(a) **REQUIREMENT FOR PROHIBITION.**—Not later than 120 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with
the head of each element of the intelligence community, shall publish regulations that—

(1) are consistent with any procedures established by Executive order or regulation under section 801 of the National Security Act of 1947 (50 U.S.C. 435);

(2) require each employee of an element of the intelligence community to sign a written agreement as described in subsection (b); and

(3) set forth the administrative procedures applicable to an employee who violates the terms of such an agreement.

(b) AGREEMENT DESCRIBED.—An agreement described in this subsection is an agreement, with respect to an individual employed by an element of the intelligence community, that—

(1) prohibits the individual from disclosing classified information without authorization at any time during or subsequent to employment with an element of the intelligence community;

(2) requires the individual to comply with all prepublication review requirements contained in any nondisclosure agreement between the individual and an element of the intelligence community;
(3) specifies appropriate disciplinary actions, including the surrender of any current or future Federal Government pension benefit, to be taken against the individual if the Director of National Intelligence or the head of the appropriate element of the intelligence community determines that the individual has knowingly violated the prepublication review requirements contained in a nondisclosure agreement between the individual and an element of the intelligence community in a manner that disclosed classified information to an unauthorized person or entity; and

(4) describes procedures for making and reviewing determinations under paragraph (3) in a manner that is consistent with the due process and appeal rights otherwise available to an individual who is subject to the same or similar disciplinary action under other law.

(c) Federal Government Pension Benefit Described.—In this section, the term “Federal Government pension benefit” means the specific government contribution to a covered person’s Federal Government pension plan, in its fair market value, but does not include the following:
(1) Any contributions by a person to a Federal
Government pension plan, in their fair market value.

(2) Any old age benefits payable to a person
under title II of the Social Security Act (42 U.S.C.
401 et seq.).

(3) Any employee benefits or contributions of a
person under the Thrift Savings Plan under sub-
chapter III of chapter 84 of title 5, United States
Code, or any successor benefit program.

SEC. 512. PROHIBITION ON SECURITY CLEARANCES FOR IN-
DIVIDUALS WHO DISCLOSE TO THE PUBLIC
EVIDENCE OR INFORMATION ON UNITED
STATES COVERT ACTIONS.

(a) PROHIBITION.—Consistent with administrative
procedures and due process afforded under otherwise ap-
licable laws and regulations, an individual described in
subsection (b) may not receive, retain, or otherwise pos-
sess a security clearance for access to classified informa-
tion.

(b) COVERED INDIVIDUALS.—An individual described
in this subsection is any individual—

(1) who—

(A) serves as an officer, employee, con-
tractor, or member of an advisory board of the
Federal Government; or
(B) otherwise possesses an active security clearance;

(2) who is known or determined, in accordance with applicable law or regulations, to have knowingly made a public disclosure of the existence of, or discussed classified details relating to, a classified covert action (as that term is defined in section 503(e) of the National Security Act of 1947 (50 U.S.C. 413b(e)); and

(3) who makes the disclosure, or discusses the details, described in paragraph (2) without prior authorization from an original classification authority.