116TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
116–24

CBRN INTELLIGENCE AND INFORMATION SHARING ACT OF 2019

MARCH 28, 2019.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. THOMPSON of Mississippi, from the Committee on Homeland Security, submitted the following

R E P O R T

[To accompany H.R.1589]

The Committee on Homeland Security, to whom was referred the bill (H.R. 1589) to amend the Homeland Security Act of 2002 to establish chemical, biological, radiological, and nuclear intelligence and information sharing functions of the Office of Intelligence and Analysis of the Department of Homeland Security and to require dissemination of information analyzed by the Department to entities with responsibilities relating to homeland security, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "CBRN Intelligence and Information Sharing Act of 2019".

SEC. 2. CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR INTELLIGENCE AND INFORMATION SHARING.

(a) IN GENERAL.—Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is amended by inserting after section 210E the following new section:

"SEC. 210F. CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR INTELLIGENCE AND INFORMATION SHARING.

"(a) IN GENERAL.—The Office of Intelligence and Analysis of the Department of Homeland Security shall—

"(1) support homeland security-focused intelligence analysis of terrorist actors, their claims, and their plans to conduct attacks involving chemical, biological, radiological, or nuclear materials against the United States, including critical infrastructure;

"(2) support homeland security-focused intelligence analysis of global infectious disease, public health, food, agricultural, and veterinary issues;

"(3) support homeland security-focused risk analysis and risk assessments of the homeland security hazards described in paragraphs (1) and (2), including the transportation of chemical, biological, nuclear, and radiological materials, by providing relevant quantitative and nonquantitative threat information;

"(4) leverage existing and emerging homeland security intelligence capabilities and structures to enhance early detection, prevention, protection, response, and recovery efforts with respect to a chemical, biological, radiological, or nuclear attack;

"(5) share information and provide tailored analytical support on such threats to State, local, Tribal, and territorial authorities, and other Federal agencies, as well as relevant national biosecurity and biodefense stakeholders, as appropriate; and

"(6) perform other responsibilities, as assigned by the Secretary.

"(b) COORDINATION.—Where appropriate, the Office of Intelligence and Analysis shall coordinate with other relevant Department components, including the Countering Weapons of Mass Destruction Office and the National Biosurveillance Integration Center, agencies within the intelligence community, including the National Counter Proliferation Center, and other Federal, State, local, Tribal, and territorial authorities, including officials from high-threat urban areas, State and major urban area fusion centers, and local public health departments, as appropriate, and enable such entities to provide recommendations on optimal information sharing mechanisms, including expeditious sharing of classified information, and on how such entities can provide information to the Department.

"(c) DEFINITIONS.—In this section:

"(1) INTELLIGENCE COMMUNITY.—The term 'intelligence community' has the meaning given such term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

"(2) NATIONAL BIOSECURITY AND BIODEFENSE STAKEHOLDERS.—The term 'national biosecurity and biodefense stakeholders' means officials from Federal, State, local, Tribal, and territorial authorities and individuals from the private sector who are involved in efforts to prevent, protect against, respond to, and recover from a biological attack or other phenomena that may have serious health consequences for the United States, including infectious disease outbreaks.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 210E the following new item:

"Sec. 210F. Chemical, biological, radiological, and nuclear intelligence and information sharing.".

(c) REPORT.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act and annually thereafter for each of the following four years, the Secretary of Homeland Security shall report to the appropriate congressional committees on the following:

(A) The intelligence and information sharing activities under section 210F of the Homeland Security Act of 2002 (as added by subsection (a) of this section) and of all relevant entities within the Department of Homeland Se-

curity to counter the threat from attacks using chemical, biological, radiological, or nuclear materials.

(B) The Department's activities in accordance with relevant intelligence strategies.

(2) ASSESSMENT OF IMPLEMENTATION.—The reports required under paragraph (1) shall include the following:

(A) An assessment of the progress of the Office of Intelligence and Analysis of the Department of Homeland Security in implementing such section 210F.

(B) A description of the methods established to carry out such assessment.

(3) DEFINITION.—In this subsection, the term "appropriate congressional committees" means the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate and any committee of the House of Representatives or the Senate having legislative jurisdiction under the rules of the House of Representatives or Senate, respectively, over the matter concerned.

SEC. 3. DISSEMINATION OF INFORMATION ANALYZED BY THE DEPARTMENT TO STATE, LOCAL, TRIBAL, TERRITORIAL, AND PRIVATE ENTITIES WITH RESPONSIBILITIES RELATING TO HOMELAND SECURITY.

Paragraph (6) of section 201(d) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)) is amended by striking "and to agencies of State" and all that follows through the period at the end and inserting "to State, local, tribal, territorial, and private entities with such responsibilities, and, as appropriate, to the public, in order to assist in preventing, deterring, or responding to acts of terrorism against the United States.".

PURPOSE AND SUMMARY

The purpose of H.R. 1589 is to amend the Homeland Security Act of 2002 to require the Office of Intelligence and Analysis (I&A) within the Department of Homeland Security to conduct analysis of terrorist capabilities related to chemical, biological, radiological, and nuclear materials, as well as threats to the homeland from global infectious disease. Additionally, it clarifies I&A's existing statutory responsibilities to encompass dissemination of information analyzed by the Department to State, local, tribal, territorial and private entities with responsibilities relating to homeland security.

BACKGROUND AND NEED FOR LEGISLATION

Terrorist groups have long aspired to employ chemical, biological, radiological, and nuclear (CBRN) materials in their attacks. Osama bin Laden saw it as an Islamic duty to acquire weapons of mass destruction (WMD); a 2010 paper issued by Harvard University's Belfer Center identified the acquisition of nuclear and strategic biological weapons as a top priority for al Qaeda.[1] In response to this threat, the Committee advanced legislation that was signed into law on December 21, 2018 to establish the Countering Weapons of Mass Destruction (CWMD) Office within the Department of Homeland Security.[2]

H.R. 1589 seeks to ensure that I&A dedicates analytical resources to the CBRN threat in coordination with the work of the CWMD office and other Federal efforts. In addition to intelligence analysis within the Department, the bill directs I&A to work with State and local officials to ensure information is shared about

[1] Rolf Mowatt-Larssen, "Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?", Belfer Center, January 2010. https://www.belfercenter.org/publication/al-qaeda-weapons-mass-destruction-threat-hype-or-reality.

[2] H.R. 7213, "Countering Weapons of Mass Destruction Act of 2018," (P.L. 115–387), as sponsored by then-Congressman Dan Donovan (R–NY).

CBRN threats. Events such as the 2013 Boston Marathon bombing illustrated the need for better information sharing between Federal and local officials. This legislation requires I&A to enhance intelligence analysis and information sharing on CBRN threats and work to ensure that State and local officials get the actionable intelligence information necessary to stop an attack.

HEARINGS

The Committee did not hold any hearings specifically on H.R. 1589 in the 116th Congress, but in the 114th Congress, the Subcommittee on Emergency Preparedness, Response, and Communications held hearings in 2015 where Subcommittee Members heard from numerous stakeholders that information sharing with appropriate state and local officials and emergency response providers about these threats are critical. On March 19, 2015, the Subcommittee held a hearing entitled "Agents of Opportunity: Responding to the Threat of Chemical Terrorism." The Subcommittee received testimony from Dr. Mark Kirk, Director, Chemical Defense Program, Office of Health Affairs, Department of Homeland Security; Dr. Christina Catlett, Associate Director, Office of Critical Event Preparedness and Response, Department of Emergency Medicine, The Johns Hopkins Hospital; Chief G. Keith Bryant, Fire Chief, Oklahoma City Fire Department, testifying on behalf of the International Association of Fire Chiefs; and Mr. Armando B. Fontoura, Sheriff, Essex County, New Jersey. This hearing provided Subcommittee Members with an opportunity to examine the threat of chemical terrorism and the steps being taken at the Federal, State, and local government levels to address the threat of chemical attacks.

On April 22, 2015, the Subcommittee held a hearing entitled "Strategic Perspectives on the Bioterrorism Threat." The Subcommittee received testimony from the Hon. Jim Talent, Former Senator from the State of Missouri and CoChair, the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism; Dr. Charles B. Cairns, Interim Dean, Health Sciences Center, University of Arizona College of Medicine; and Marisa Raphael, MPH, Deputy Commissioner, Office of Emergency Planning and Response, Department of Health and Mental Hygiene, New York City, New York. This hearing highlighted the threat of bioterrorism and assessed the Federal government's efforts to prepare for and defend against this threat.

COMMITTEE CONSIDERATION

The Committee met on March 13, 2019, with a quorum being present, to consider H.R. 1589 and ordered the measure to be reported to the House with a favorable recommendation, with amendment, by unanimous consent.

The following amendments was offered and accepted by unanimous consent:

An amendment offered by Ms. Clarke of New York (#1) Page 2, line 19 insert ", including critical infrastructure" before the semicolon at the end.

An amendment offered by Ms. Jackson Lee (#2) Page 3, line 6, insert "early detection," before "prevention".

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

No recorded votes were requested during consideration of H.R. 1589.

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

CONGRESSIONAL BUDGET OFFICE ESTIMATE NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

With respect to the requirements of clause 3(c)(2) of rule XIII of the Rules of the House of Representatives and section 308(a) of the Congressional Budget Act of 1974 and with respect to requirements of clause (3)(c)(3) of rule XIII of the Rules of the House of Representatives and section 402 of the Congressional Budget Act of 1974, the Committee has requested but not received a cost estimate for this bill from the Director of Congressional Budget Office.

The Committee has requested but not received from the Director of the Congressional Budget Office a statement as to whether this bill contains any new budget authority, spending authority, credit authority, or an increase or decrease in revenues or tax expenditures.

FEDERAL MANDATES STATEMENT

An estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act was not made available to the Committee in time for the filing of this report. The Chairman of the Committee shall cause such estimate to be printed in the Congressional Record upon its receipt by the Committee.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 1589 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

PERFORMANCE GOALS AND OBJECTIVES

The Committee states that pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, H.R. 1589 would (1) support homeland security-focused intelligence analysis of terrorist actors, their claims, and their plans to conduct attacks involving chemical, biological, radiological, and nuclear materials against the nation and of global infectious disease, public health, food, agricultural, and veterinary issues; (2) support homeland security-focused

risk analysis and risk assessments of such homeland security hazards by providing relevant quantitative and non-quantitative threat information; (3) leverage homeland security intelligence capabilities and structures to enhance prevention, protection, response, and recovery efforts with respect to a chemical, biological, radiological, or nuclear attack; and (4) share information and provide tailored analytical support on these threats to state, local, and tribal authorities as well as other national biosecurity and biodefense stakeholders.

ADVISORY ON EARMARKS

In compliance with rule XXI of the Rules of the House of Representatives, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(d), 9(e), or 9(f) of the rule XXI.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

This Act may be cited as the "CBRN Intelligence and Information Sharing Act of 2019".

Section 2. Chemical, Biological, Radiological, and Nuclear (CBRN) intelligence and information sharing

This section amends the Homeland Security Act of 2002 (Pub. Law 107–296) to require the Office of Intelligence and Analysis (I&A) of the Department of Homeland Security (DHS) to support homeland security-focused intelligence analysis of terrorists, their claims, and their plans to conduct attacks involving CBRN materials against the nation, and of global infectious disease, public health, food, agricultural, and veterinary issues.

Additionally, this section directs I&A to support homeland security-focused risk analysis and risk assessments of those hazards by providing relevant threat information; leveraging homeland security intelligence capabilities and structures to enhance prevention, protection, response, and recovery efforts with respect to a CBRN attack; and sharing information and provide tailored analytical support on these threats to State, local, and tribal authorities; other national biosecurity and biodefense stakeholders; and other federal agencies as appropriate.

This section requires I&A to coordinate with other DHS components, including the Weapons of Mass Destruction Office, the National Biosurveillance Integration Center, the Intelligence Community, and Federal, State, local, and tribal authorities, where appro-

priate, and enable such entities to provide recommendations on optimal information sharing mechanisms and on how they can provide information to DHS.

As information and intelligence is only useful if it is shared with those who can take action, such as State, local, tribal, and private entities, the Committee directs the Office of Intelligence and Analysis to involve these partners, as appropriate, and get their feedback on mechanisms for two-way sharing of information.

This section directs the DHS Secretary to report annually on: (1) intelligence and information sharing activities to counter the threat from weapons of mass destruction, and (2) DHS's activities in accordance with relevant intelligence strategies. This reporting requirement will terminate five years after enactment.

Finally, this section defines the following terms in the bill: "appropriate congressional committees", "Intelligence Community", and "national biosecurity and biodefense stakeholders".

Section 3. Dissemination of information analyzed by the Department to State, local, tribal, territorial, and private entities with responsibilities related to Homeland Security

This section amends section 201(d)(6) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)(8)) to require the Secretary to ensure that homeland security information analyzed by DHS concerning terrorist threats is provided to State, local, and private entities and the public, as appropriate.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Homeland Security Act of 2002".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

TITLE II—INFORMATION ANALYSIS

Subtitle A—Information and Analysis; Access to Information

SEC. 201. INFORMATION AND ANALYSIS.

(a) INTELLIGENCE AND ANALYSIS.—There shall be in the Department an Office of Intelligence and Analysis.

(b) UNDER SECRETARY FOR INTELLIGENCE AND ANALYSIS.—

(1) OFFICE OF INTELLIGENCE AND ANALYSIS.—The Office of Intelligence and Analysis shall be headed by an Under Secretary for Intelligence and Analysis, who shall be appointed by the President, by and with the advice and consent of the Senate.

(2) CHIEF INTELLIGENCE OFFICER.—The Under Secretary for Intelligence and Analysis shall serve as the Chief Intelligence Officer of the Department.

(c) DISCHARGE OF RESPONSIBILITIES.—The Secretary shall ensure that the responsibilities of the Department relating to information analysis, including those described in subsection (d), are carried out through the Under Secretary for Intelligence and Analysis.

(d) RESPONSIBILITIES OF SECRETARY RELATING TO INTELLIGENCE AND ANALYSIS.—The responsibilities of the Secretary relating to intelligence and analysis shall be as follows:

(1) To access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information, in support of the mission responsibilities of the Department and the functions of the National Counterterrorism Center established under section 119 of the National Security Act of 1947 (50 U.S.C. 404o), in order to—

(A) identify and assess the nature and scope of terrorist threats to the homeland;

(B) detect and identify threats of terrorism against the United States; and

(C) understand such threats in light of actual and potential vulnerabilities of the homeland.

(2) To carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States (including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks).

(3) To integrate relevant information, analysis, and vulnerability assessments (regardless of whether such information, analysis or assessments are provided by or produced by the Department) in order to—

(A) identify priorities for protective and support measures regarding terrorist and other threats to homeland security by the Department, other agencies of the Federal

Government, State, and local government agencies and authorities, the private sector, and other entities; and

(B) prepare finished intelligence and information products in both classified and unclassified formats, as appropriate, whenever reasonably expected to be of benefit to a State, local, or tribal government (including a State, local, or tribal law enforcement agency) or a private sector entity.

(4) To ensure, pursuant to section 202, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this section, including obtaining such information from other agencies of the Federal Government.

(5) To review, analyze, and make recommendations for improvements to the policies and procedures governing the sharing of information within the scope of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), including homeland security information, terrorism information, and weapons of mass destruction information, and any policies, guidelines, procedures, instructions, or standards established under that section.

(6) To disseminate, as appropriate, information analyzed by the Department within the Department, to other agencies of the Federal Government with responsibilities relating to homeland security, [and to agencies of State and local governments and private sector entities with such responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States.] *to State, local, tribal, territorial, and private entities with such responsibilities, and, as appropriate, to the public, in order to assist in preventing, deterring, or responding to acts of terrorism against the United States.*

(7) To consult with the Director of National Intelligence and other appropriate intelligence, law enforcement, or other elements of the Federal Government to establish collection priorities and strategies for information, including law enforcement-related information, relating to threats of terrorism against the United States through such means as the representation of the Department in discussions regarding requirements and priorities in the collection of such information.

(8) To consult with State and local governments and private sector entities to ensure appropriate exchanges of information, including law enforcement-related information, relating to threats of terrorism against the United States.

(9) To ensure that—

(A) any material received pursuant to this Act is protected from unauthorized disclosure and handled and used only for the performance of official duties; and

(B) any intelligence information under this Act is shared, retained, and disseminated consistent with the authority of the Director of National Intelligence to protect intelligence sources and methods under the National Security Act of 1947 (50 U.S.C. 401 et seq.) and related procedures and, as appropriate, similar authorities of the Attor-

ney General concerning sensitive law enforcement information.

(10) To request additional information from other agencies of the Federal Government, State and local government agencies, and the private sector relating to threats of terrorism in the United States, or relating to other areas of responsibility assigned by the Secretary, including the entry into cooperative agreements through the Secretary to obtain such information.

(11) To establish and utilize, in conjunction with the chief information officer of the Department, a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section, and to disseminate information acquired and analyzed by the Department, as appropriate.

(12) To ensure, in conjunction with the chief information officer of the Department, that any information databases and analytical tools developed or utilized by the Department—

(A) are compatible with one another and with relevant information databases of other agencies of the Federal Government; and

(B) treat information in such databases in a manner that complies with applicable Federal law on privacy.

(13) To coordinate training and other support to the elements and personnel of the Department, other agencies of the Federal Government, and State and local governments that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.

(14) To coordinate with elements of the intelligence community and with Federal, State, and local law enforcement agencies, and the private sector, as appropriate.

(15) To provide intelligence and information analysis and support to other elements of the Department.

(16) To coordinate and enhance integration among the intelligence components of the Department, including through strategic oversight of the intelligence activities of such components.

(17) To establish the intelligence collection, processing, analysis, and dissemination priorities, policies, processes, standards, guidelines, and procedures for the intelligence components of the Department, consistent with any directions from the President and, as applicable, the Director of National Intelligence.

(18) To establish a structure and process to support the missions and goals of the intelligence components of the Department.

(19) To ensure that, whenever possible, the Department—

(A) produces and disseminates unclassified reports and analytic products based on open-source information; and

(B) produces and disseminates such reports and analytic products contemporaneously with reports or analytic products concerning the same or similar information that the

Department produced and disseminated in a classified format.

(20) To establish within the Office of Intelligence and Analysis an internal continuity of operations plan.

(21) Based on intelligence priorities set by the President, and guidance from the Secretary and, as appropriate, the Director of National Intelligence—

(A) to provide to the heads of each intelligence component of the Department guidance for developing the budget pertaining to the activities of such component; and

(B) to present to the Secretary a recommendation for a consolidated budget for the intelligence components of the Department, together with any comments from the heads of such components.

(22) To perform such other duties relating to such responsibilities as the Secretary may provide.

(23)(A) Not later than six months after the date of the enactment of this paragraph, to conduct an intelligence-based review and comparison of the risks and consequences of EMP and GMD facing critical infrastructure, and submit to the Committee on Homeland Security and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Select Committee on Intelligence of the Senate—

(i) a recommended strategy to protect and prepare the critical infrastructure of the homeland against threats of EMP and GMD; and

(ii) not less frequently than every two years thereafter for the next six years, updates of the recommended strategy.

(B) The recommended strategy under subparagraph (A) shall—

(i) be based on findings of the research and development conducted under section 320;

(ii) be developed in consultation with the relevant Federal sector-specific agencies (as defined under Presidential Policy Directive-21) for critical infrastructure;

(iii) be developed in consultation with the relevant sector coordinating councils for critical infrastructure;

(iv) be informed, to the extent practicable, by the findings of the intelligence-based review and comparison of the risks and consequences of EMP and GMD facing critical infrastructure conducted under subparagraph (A); and

(v) be submitted in unclassified form, but may include a classified annex.

(C) The Secretary may, if appropriate, incorporate the recommended strategy into a broader recommendation developed by the Department to help protect and prepare critical infrastructure from terrorism, cyber attacks, and other threats if, as incorporated, the recommended strategy complies with subparagraph (B).

(e) STAFF.—

(1) IN GENERAL.—The Secretary shall provide the Office of Intelligence and Analysis with a staff of analysts having appropriate expertise and experience to assist such offices in discharging responsibilities under this section.

(2) PRIVATE SECTOR ANALYSTS.—Analysts under this subsection may include analysts from the private sector.

(3) SECURITY CLEARANCES.—Analysts under this subsection shall possess security clearances appropriate for their work under this section.

(f) DETAIL OF PERSONNEL.—

(1) IN GENERAL.—In order to assist the Office of Intelligence and Analysis in discharging responsibilities under this section, personnel of the agencies referred to in paragraph (2) may be detailed to the Department for the performance of analytic functions and related duties.

(2) COVERED AGENCIES.—The agencies referred to in this paragraph are as follows:

(A) The Department of State.

(B) The Central Intelligence Agency.

(C) The Federal Bureau of Investigation.

(D) The National Security Agency.

(E) The National Geospatial-Intelligence Agency.

(F) The Defense Intelligence Agency.

(G) Any other agency of the Federal Government that the President considers appropriate.

(3) COOPERATIVE AGREEMENTS.—The Secretary and the head of the agency concerned may enter into cooperative agreements for the purpose of detailing personnel under this subsection.

(4) BASIS.—The detail of personnel under this subsection may be on a reimbursable or non-reimbursable basis.

(g) FUNCTIONS TRANSFERRED.—In accordance with title XV, there shall be transferred to the Secretary, for assignment to the Office of Intelligence and Analysis and the Office of Infrastructure Protection under this section, the functions, personnel, assets, and liabilities of the following:

(1) The National Infrastructure Protection Center of the Federal Bureau of Investigation (other than the Computer Investigations and Operations Section), including the functions of the Attorney General relating thereto.

(2) The National Communications System of the Department of Defense, including the functions of the Secretary of Defense relating thereto.

(3) The Critical Infrastructure Assurance Office of the Department of Commerce, including the functions of the Secretary of Commerce relating thereto.

(4) The National Infrastructure Simulation and Analysis Center of the Department of Energy and the energy security and assurance program and activities of the Department, including the functions of the Secretary of Energy relating thereto.

(5) The Federal Computer Incident Response Center of the General Services Administration, including the functions of the Administrator of General Services relating thereto.

* * * * * * *

SEC. 210F. CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR INTELLIGENCE AND INFORMATION SHARING.

(a) IN GENERAL.—The Office of Intelligence and Analysis of the Department of Homeland Security shall—

(1) support homeland security-focused intelligence analysis of terrorist actors, their claims, and their plans to conduct attacks involving chemical, biological, radiological, or nuclear materials against the United States, including critical infrastructure;

(2) support homeland security-focused intelligence analysis of global infectious disease, public health, food, agricultural, and veterinary issues;

(3) support homeland security-focused risk analysis and risk assessments of the homeland security hazards described in paragraphs (1) and (2), including the transportation of chemical, biological, nuclear, and radiological materials, by providing relevant quantitative and nonquantitative threat information;

(4) leverage existing and emerging homeland security intelligence capabilities and structures to enhance early detection, prevention, protection, response, and recovery efforts with respect to a chemical, biological, radiological, or nuclear attack;

(5) share information and provide tailored analytical support on such threats to State, local, Tribal, and territorial authorities, and other Federal agencies, as well as relevant national biosecurity and biodefense stakeholders, as appropriate; and

(6) perform other responsibilities, as assigned by the Secretary.

(b) COORDINATION.—Where appropriate, the Office of Intelligence and Analysis shall coordinate with other relevant Department components, including the Countering Weapons of Mass Destruction Office and the National Biosurveillance Integration Center, agencies within the intelligence community, including the National Counter Proliferation Center, and other Federal, State, local, Tribal, and territorial authorities, including officials from high-threat urban areas, State and major urban area fusion centers, and local public health departments, as appropriate, and enable such entities to provide recommendations on optimal information sharing mechanisms, including expeditious sharing of classified information, and on how such entities can provide information to the Department.

(c) DEFINITIONS.—In this section:

(1) INTELLIGENCE COMMUNITY.—The term "intelligence community" has the meaning given such term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(2) NATIONAL BIOSECURITY AND BIODEFENSE STAKEHOLDERS.—The term "national biosecurity and biodefense stakeholders" means officials from Federal, State, local, Tribal, and territorial authorities and individuals from the private sector who are involved in efforts to prevent, protect against, respond to, and recover from a biological attack or other phenomena

that may have serious health consequences for the United States, including infectious disease outbreaks.

* * * * * * *

○