Chairman HAL ROGERS, and Ranking Member NITA LOWEY, as well as all of the Appropriations and Intelligence Committee staff for their hard work and long hours over the last several months in getting this important legislation to the floor today and eventually to the President for his signature. I urge all Members to support the bill.

Mr. Speaker, the following consists of the joint explanatory statement to accompany Division M, the Intelligence Authorization Act for Fiscal Year 2016, of the Consolidated Appropriations Act, 2016.

This joint explanatory statement reflects the status of negotiations and disposition of issues reached between the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence (hereinafter, "the Agreement"). The joint explanatory statement shall have the same effect with respect to the implementation of this Act as if it were a joint explanatory statement of a committee of conference.

The joint explanatory statement comprises three parts: an overview of the application of the annex to accompany this statement; unclassified congressional direction; and a section-by-section analysis of the legislative text.

PART I: APPLICATION OF THE CLASSIFIED ANNEX

The classified nature of U.S. intelligence activities prevents the congressional intelligence committees from publicly disclosing many details concerning the conclusions and recommendations of the Agreement. Therefore, a classified Schedule of Authorizations and a classified annex have been prepared to describe in detail the scope and intent of the congressional intelligence committees' actions. The Agreement authorizes the Intelligence Community to obligate and expend funds not altered or modified by the classified Schedule of Authorizations as requested in the President's budget, subject to modification under applicable reprogramming procedures.

The classified annex is the result of negotiations between the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence. It reconciles the differences between the committees' respective versions of the bill for the National Intelligence Program (NIP) and the Homeland Security Intelligence Program for Fiscal Year 2016. The Agreement also makes recommendations for the Military Intelligence Program (MIP), and the Information Systems Security Program, consistent with the National Defense Authorization Act for Fiscal Year 2016, and provides certain direction for these two programs.

The Agreement supersedes the classified annexes to the reports accompanying H.R. 4127, as passed by the House on December 1, 2015, H.R. 2596, as passed by the House on June 16, 2015, and S. 1705, as reported by the Senate Select Committee on Intelligence on July 7, 2015. All references to the House-passed and Senate-reported annexes are solely to identify the heritage of specific provisions.

The classified Schedule of Authorizations is incorporated into the bill pursuant to Section 102. It has the status of law. The classified annex supplements and adds detail to clarify the authorization levels found in the bill and the classified Schedule of Authorizations. The classified annex shall have the same legal force as the report to accompany the bill.

PART II: SELECT UNCLASSIFIED CONGRESSIONAL DIRECTION

Enhancing Geographic and Demographic Diversity

The Agreement directs the Office of the Director for National Intelligence (ODNI) to conduct an awareness, outreach, and recruitment program to rural, under-represented colleges and universities that are not part of the IC Centers of Academic Excellence (IC CAE) program Further, the Agreement directs that ODNI shall increase and formally track the number of competitive candidates for IC employment or internships who studied at IC CAE schools and other scholarship programs supported by the IC.

Additionally, the Agreement directs that ODNI, acting through the Executive Agent for the IC CAE program, the IC Chief Human Capital Officer, and the Chief, Office of IC Equal Opportunity & Diversity, as appropriate, shall:

1. Add a criterion to the IC CAE selection process that applicants must be part of a consortium or actively collaborate with under-resourced schools in their area;

2. Work with CAE schools to reach out to rural and under-resourced schools, including by inviting such schools to participate in the annual IC CAE colloquium and IC recruitment events;

3. Increase and formally track the number of competitive IC internship candidates from IC CAE schools, starting with Fiscal Year 2016 IC summer internships, and provide a report, within 180 days of the enactment of this Act, on its plan to do so;

4. Develop metrics to ascertain whether IC CAE, the Pat Roberts Intelligence Scholars Program, the Louis Stokes Educational Scholarship Program, and the Intelligence Officer Training Program reach a diverse demographic and serve as feeders to the IC workforce;

5. Include in the annual report on minority hiring and retention a breakdown of the students participating in these programs who serve as IC interns, applied for full-time IC employment, received offers of employment, and entered on duty in the IC;

6. Conduct a feasibility study with necessary funding levels regarding how the IC CAE could be better tailored to serve under-resourced schools, and provide such study to the congressional intelligence committees within 180 days of the enactment of this Act;

7. Publicize all IC elements' recruitment activities, including the new Applicant Gateway and the IC Virtual Career Fair, to rural schools, Historically Black Colleges and Universities, and other minority-serving institutions that have been contacted by IC recruiters;

8. Contact new groups with the objective of expanding the IC Heritage Community Liaison Council; and

9. Ensure that IC elements add such activities listed above that may be appropriate to their recruitment plans for Fiscal Year 2016.

ODNI shall provide an interim update to the congressional intelligence committees on its efforts within 90 days of the enactment of this Act and include final results in its annual report on minority hiring and retention.

Analytic Duplication & Improving Customer Impact

The congressional intelligence committees are concerned about potential duplication in finished analytic products. Specifically, the congressional intelligence committees are concerned that contemporaneous publication of substantially similar intelligence products fosters confusion among intelligence customers (including those in Congress), impedes analytic coherence across the IC, and wastes time and effort. The congressional intelligence committees value competitive analysis, but believe there is room to reduce duplicative analytic activity and improve customer impact.

Therefore, the Agreement directs ODNI to pilot a repeatable methodology to evaluate potential duplication in finished intelligence analytic products and to report the findings to the congressional intelligence committees within 60 days of the enactment of this Act. In addition, the Agreement directs ODNI to report to the congressional intelligence committees within 180 days of enactment of this Act on how it will revise analytic practice, tradecraft, and standards to ensure customers can clearly identify how products that are produced contemporaneously and cover similar topics differ from one another in their methodological, informational, or temporal aspects, and the significance of those differences. This report is not intended to cover operationally urgent analysis or current intelligence.

Countering Violent Extremism and the Islamic State of Iraq and the Levant

The Agreement directs ODNI, within 180 days of enactment of this Act and in consultation with appropriate interagency partners, to brief the congressional intelligence committees on how intelligence agencies are supporting both (1) the Administration's Countering Violent Extremism (CVE) program first detailed in the 2011 White House strategy *Empowering Local Partners to Prevent Violent Extremism in the United States*, which was expanded following the January 2015 White House Summit on Countering Violent Extremism, and (2) the Administration's *Strategy to Counter the Islamic State of Iraq and the Levant*, which was announced in September 2014.

Analytic Health Reports

The Agreement directs the Defense Intelligence Agency (DIA) to provide Analytic Health Reports to the congressional intelligence committees on a quarterly basis, including an update on the specific effect of analytic modernization on the health of the Defense Intelligence Analysis Program (DIAP) and its ability to reduce analytic risk.

All-Source Analysis Standards

The Agreement directs DIA to conduct a comprehensive evaluation of the Defense Intelligence Enterprise's all-source analysis capability and production in Fiscal Year 2015. The evaluation should assess the analytic output of both NIP and MIP funded all-source analysts, separately and collectively, and apply the following four criteria identified in the ODNI Strategic Evaluation Report for all-source analysis: 1) integrated, 2) objective, 3) timely, and 4) value-added. The results of this evaluation shall be included as part of the Fiscal Year 2017 congressional budget justification book.

Terrorism Investigations

The Agreement directs the Federal Bureau of Investigation (FBI) to submit to the congressional intelligence committees, within 180 days of enactment of this Act, a report detailing how

FBI has allocated resources between domestic and foreign terrorist threats based on numbers of investigations over the past 5 years. The report should be submitted in unclassified form but may include a classified annex.

Investigations of Minors Involved in Radicalization

The Agreement directs the FBI to provide a briefing to the congressional intelligence committees within 180 days of enactment of this Act on investigations in which minors are encouraged to turn away from violent extremism rather than take actions that would lead to Federal terrorism indictments. This briefing should place these rates in the context of all investigations of minors for violent extremist activity and should describe any FBI engagement with minors' families, law enforcement, or other individuals or groups connected to the minor during or after investigations.

Furthermore, the Agreement directs the FBI to include how often undercover agents pursue investigations based on a location of interest related to violent extremist activity compared to investigations of an individual or group believed to be engaged in such activity. Included should be the number of locations of interest associated with a religious group or entity. This briefing also should include trend analysis covering the last five years describing violent extremist activity in the U.S.

Declassification Review of Video of the 2012 Benghazi Terrorist Attacks

Numerous investigations have been conducted regarding the 2012 terrorist attack against U.S. facilities in Benghazi. The Senate Select Committee on Intelligence produced one of the first declassified Congressional reports and continues to believe that the public should have access to information about the attacks, so long as it does not jeopardize intelligence sources and methods.

The closed circuit television videos from the Temporary Mission Facility (TMF) captured some of the activity that took place at the State Department facility on September 11, 2012, and their release would contribute to the public's understanding of the event without compromising sources or methods.

Therefore, the Agreement directs the Director of National Intelligence, or the appropriate federal official, to conduct a declassification review and to facilitate the release to the public of the declassified closed circuit television videos of the September 11, 2012, terrorist attack on the TMF in Benghazi, Libya, consistent with the protection of sources and methods, not later than 120 days after the enactment of this Act.

PART III: SECTION-BY-SECTION ANALYSIS AND EXPLANATION OF LEGISLATIVE TEXT

The following is a section-by-section analysis and explanation of the Intelligence Authorization Act for Fiscal Year 2016.

TITLE I—INTELLIGENCE ACTIVITIES

Section 101. Authorization of appropriations

Section 101 lists the United States Government departments, agencies, and other elements for which the Act authorizes appropriations for intelligence and intelligence-related activities for Fiscal Year 2016.

Section 102. Classified Schedule of Authorizations

Section 102 provides that the details of the amounts authorized to be appropriated for intelligence and intelligence-related activities and the applicable personnel levels by program for Fiscal Year 2016 are contained in the classified Schedule of Authorizations and that the classified Schedule of Authorizations shall be made available to the Committees on Appropriations of the Senate and House of Representatives and to the President.

Section 103. Personnel ceiling adjustments

Section 103 is intended to provide additional flexibility to the Director of National Intelligence in managing the civilian personnel of the Intelligence Community. Section 103 provides that the Director may authorize employment of civilian personnel in Fiscal Year 2016 in excess of the number of authorized positions by an amount not exceeding three percent of the total limit applicable to each Intelligence Community element under Section 102. The Director may do so only if necessary to the performance of important intelligence functions.

Section 104. Intelligence Community Management Account

Section 104 authorizes appropriations for the Intelligence Community Management Account (ICMA) of the Director of National Intelligence and sets the authorized personnel levels for the elements within the ICMA for Fiscal Year 2016.

Section 105. Clarification regarding authority for flexible personnel management among elements of intelligence community

Section 105 clarifies that certain Intelligence Community elements may make hiring decisions based on the excepted service designation.

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

Section 201. Authorization of appropriations

Section 201 authorizes appropriations in the amount of $514,000,000 for Fiscal Year 2016 for the Central Intelligence Agency Retirement and Disability Fund.

TITLE III—GENERAL PROVISIONS

Section 301. Increase in employee compensation and benefits authorized by law

Section 301 provides that funds authorized to be appropriated by the Act for salary, pay, retirement, and other benefits for federal employees may be increased by such additional or supplemental amounts as may be necessary for increases in compensation or benefits authorized by law.

Section 302. Restriction on conduct of intelligence activities

Section 302 provides that the authorization of appropriations by the Act shall not be deemed to constitute authority for the conduct of any intelligence activity that is not otherwise authorized by the Constitution or laws of the United States.

Section 303. Provision of information and assistance to Inspector General of the Intelligence Community

Section 303 amends the National Security Act of 1947 to clarify the Inspector General of the Intelligence Community's authority to seek information and assistance from federal, state, and local agencies, or units thereof.

Section 304. Inclusion of Inspector General of Intelligence Community in Council of Inspectors General on Integrity and Efficiency

Section 304 amends Section 11(b)(1)(B) of the Inspector General Act of 1978 to reflect the correct name of the Office of the Inspector General of the Intelligence Community. The section also clarifies that the Inspector General of the Intelligence Community is a member of the Council of the Inspectors General on Integrity and Efficiency.

Section 305. Clarification of authority of Privacy and Civil Liberties Oversight Board

Section 305 amends the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) to clarify that nothing in the statute authorizing the Privacy and Civil Liberties Oversight Board should be construed to allow that Board to gain access to information regarding an activity covered by section 503 of the National Security Act of 1947.

Section 306. Enhancing government personnel security programs

Section 306 directs the Director of National Intelligence to develop and implement a plan for eliminating the backlog of overdue periodic investigations, and further requires the Director to direct each agency to implement a program to provide enhanced security review to individuals determined eligible for access to classified information or eligible to hold a sensitive position.

These enhanced personnel security programs will integrate information relevant and appropriate for determining an individual's suitability for access to classified information or eligibility to hold a sensitive position; be conducted at least 2 times every 5 years; and commence not later than 5 years after the date of enactment of the Fiscal Year 2016 Intelligence Authorization Act, or the elimination of the backlog of overdue periodic investigations, whichever occurs first.

Section 307. Notification of changes to retention of call detail record policies

Section 307 requires the Director of National Intelligence to notify the congressional intelligence committees in writing not later than 15 days after learning that an electronic communication service provider that generates call detail records in the ordinary course of business has changed its policy on the retention of such call details records to result in a retention period of less than 18 months. Section 307 further requires the Director to submit to the congressional intelligence committees within 30 days of enactment a report identifying each electronic communication service provider (if any) that has a current policy in place to retain call detail records for 18 months or less.

Section 308. Personnel information notification policy by the Director of National Intelligence

Section 308 requires the Director of National Intelligence to establish a policy to ensure timely notification to the congressional intelligence committees of the identities of individuals occupying senior level positions within the Intelligence Community.

Section 309. Designation of lead intelligence officer for tunnels

Section 309 requires the Director of National Intelligence to designate an official to manage

the collection and analysis of intelligence regarding the tactical use of tunnels by state and nonstate actors.

Section 310. Reporting process for tracking country clearance requests

Section 310 requires the Director of National Intelligence to establish a formal reporting process for tracking requests for country clearance submitted to overseas Director of National Intelligence representatives. Section 310 also requires the Director to brief the congressional intelligence committees on its progress.

Section 311. Study on reduction of analytic duplication

Section 311 requires the Director of National Intelligence to carry out a study to identify duplicative analytic products and the reasons for such duplication, ascertain the frequency and types of such duplication, and determine whether this review should be considered a part of the responsibilities assigned to the Analytic Integrity and Standards office inside the Office of the Director of National Intelligence. Section 311 also requires the Director to provide a plan for revising analytic practice, tradecraft, and standards to ensure customers are able to readily identify how analytic products on similar topics that are produced contemporaneously differ from one another and what is the significance of those differences.

Section 312. Strategy for comprehensive interagency review of the United States national security overhead satellite architecture

Section 312 requires the Director of National Intelligence, in collaboration with the Secretary of Defense, and the Chairman of the Joint Chiefs of Staff, to develop a strategy, with milestones and benchmarks, to ensure that there is a comprehensive interagency review of policies and practices for planning and acquiring national security satellite systems and architectures, including the capabilities of commercial systems and partner countries, consistent with the National Space Policy issued on June 28, 2010. Where applicable, this strategy shall account for the unique missions and authorities vested in the Department of Defense and the Intelligence Community.

Section 313. Cyber attack standards of measurement study

Section 313 directs the Director of National Intelligence, in consultation with the Secretary of Homeland Security, the Director of the Federal Bureau of Investigation, and the Secretary of Defense, to carry out a study to determine the appropriate standards to measure the damage of cyber incidents.

TITLE IV—MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY

SUBTITLE A—OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Section 401. Appointment and confirmation of the National Counterintelligence Executive

Section 401 makes subject to Presidential appointment and Senate confirmation, the executive branch position of National Counterintelligence Executive (NCIX), which was created by the 2002 Counterintelligence Enhancement Act. Effective December 2014, the NCIX was also dual-hatted as the Director of the National Counterintelligence and Security Center.

Section 402. Technical amendments relating to pay under title 5, United States Code

Section 402 amends 5 U.S.C. §5102(a)(1) to expressly exclude the Office of the Director of National Intelligence (ODNI) from the provisions of chapter 51 of title 5, relating to position classification, pay, and allowances for General Schedule employees, which does not apply to ODNI by virtue of the National Security Act. This proposal would have no substantive effect.

Section 403. Analytic Objectivity Review

The Office of the Director of National Intelligence's Analytic Integrity and Standards (AIS) office was established in response to the requirement in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) for the designation of an entity responsible for ensuring that the Intelligence Community's finished intelligence products are timely, objective, independent of political considerations, based upon all sources of available intelligence, and demonstrative of the standards of proper analytic tradecraft.

Consistent with responsibilities prescribed under IRTPA, Section 403 requires the AIS Chief to conduct a review of finished intelligence products produced by the CIA to assess whether the reorganization of the Agency, announced publicly on March 6, 2015, has resulted in any loss of analytic objectivity. The report is due no later than March 6, 2017.

SUBTITLE B—CENTRAL INTELLIGENCE AGENCY AND OTHER ELEMENTS

Section 411. Authorities of the Inspector General for the Central Intelligence Agency

Section 411 amends Section 17 of the Central Intelligence Agency Act of 1949 to consolidate the Inspector General's personnel authorities and to provide the Inspector General with the same authorities as other Inspectors General to request assistance and information from federal, state, and local agencies or units thereof.

Section 412. Prior congressional notification of transfers of funds for certain intelligence activities

Section 412 requires notification to the congressional intelligence committees before transferring funds from the Joint Improvised Explosive Device Defeat Fund or the Counterterrorism Partnerships Fund that are to be used for intelligence activities.

TITLE V—MATTERS RELATING TO FOREIGN COUNTRIES

SUBTITLE A—MATTERS RELATING TO RUSSIA

Section 501. Notice of deployment or transfer of Club-K container missile system by the Russian Federation

Section 501 requires the Director of National Intelligence to submit written notice to the appropriate congressional committees if the Intelligence Community receives intelligence that the Russian Federation has deployed, or is about to deploy, the Club-K container missile system through the Russian military, or transferred or sold, or intends to transfer or sell, such system to another state or non-state actor.

Section 502. Assessment on funding of political parties and nongovernmental organizations by the Russian Federation

Section 502 requires the Director of National Intelligence to submit an Intelligence Community assessment to the appropriate congressional committees concerning the funding of political parties and nongovernmental organizations in the former Soviet States and Europe by the Russian Security Services since January 1, 2006, not later than 180 days after the enactment of the Fiscal Year 2016 Intelligence Authorization Act.

Section 503. Assessment on the use of political assassinations as a form of statecraft by the Russian Federation

Section 503 requires the Director of National Intelligence to submit an Intelligence Community assessment concerning the use of political assassinations as a form of statecraft by the Russian Federation to the appropriate congressional committees, not later than 180 days after the enactment of the Fiscal Year 2016 Intelligence Authorization Act.

SUBTITLE B—MATTERS RELATING TO OTHER COUNTRIES

Section 511. Report of resources and collection posture with regard to the South China Sea and East China Sea

Section 511 requires the Director of National Intelligence to submit to the appropriate congressional committees an Intelligence Community assessment on Intelligence Community resourcing and collection posture with regard to the South China Sea and East China Sea, not later than 180 days after the enactment of the Fiscal Year 2016 Intelligence Authorization Act.

Section 512. Use of locally employed staff serving at a United States diplomatic facility in Cuba

Section 512 requires the Secretary of State, not later than 1 year after the date of the enactment of this Act, to ensure that key supervisory positions at a United States diplomatic facility in Cuba are occupied by citizens of the United States who have passed a thorough background check. Further, not later than 180 days after the date of the enactment of this Act, the provision requires the Secretary of State, in coordination with other appropriate government agencies, to submit to the appropriate congressional committees a plan to further reduce the reliance on locally employed staff in United States diplomatic facilities in Cuba. The plan shall, at a minimum, include cost estimates, timelines, and numbers of employees to be replaced.

Section 513. Inclusion of sensitive compartmented information facilities in United States diplomatic facilities in Cuba

Section 513 requires that each United States diplomatic facility in Cuba—in which classified information will be processed or in which classified communications occur—that is constructed, or undergoes a construction upgrade, be constructed to include a sensitive compartmented information facility.

Section 514. Report on use by Iran of funds made available through sanctions relief

Section 514 requires the Director of National Intelligence, in consultation with the Secretary of the Treasury, to submit to the appropriate congressional committees a report assessing the monetary value of any direct or indirect form of sanctions relief Iran has received since the Joint Plan of Action (JPOA) entered into effect, and how Iran has used funds made available through such sanctions relief. This

report shall be submitted every 180 days while the JPOA is in effect, and not later than 1 year after an agreement relating to Iran's nuclear program takes effect, and annually thereafter while that agreement remains in effect.

TITLE VI—MATTERS RELATING TO UNITED STATES NAVAL STATION, GUANTANAMO BAY, CUBA

Section 601. Prohibition on use of funds for transfer or release of individual detained at United States Naval Station, Guantanamo Bay, Cuba, to the United States

Section 601 states that no amounts authorized to be appropriated or otherwise made available to an element of the Intelligence Community may be used to transfer or release individuals detained at Guantanamo Bay to or within the United States, its territories, or possessions.

Section 602. Prohibition on use of funds to construct or modify facilities in the United States to house detainees transferred from United States Naval Station, Guantanamo Bay, Cuba

Section 602 states that no amounts authorized to be appropriated or otherwise made available to an element of the Intelligence Community may be used to construct or modify facilities in the United States, its territories, or possessions to house detainees transferred from Guantanamo Bay.

Section 603. Prohibition on use of funds for transfer or release to certain countries of individuals detained at United States Naval Station, Guantanamo Bay, Cuba

Section 603 states that no amounts authorized to be appropriated or otherwise made available to an element of the Intelligence Community may be used to transfer or release an individual detained at Guantanamo Bay to the custody or control of any country, or any entity within such country, as follows: Libya, Somalia, Syria, or Yemen.

TITLE VII—REPORTS AND OTHER MATTERS

SUBTITLE A—REPORTS

Section 701. Repeal of certain reporting requirements

Section 701 repeals certain reporting requirements.

Section 702. Reports on foreign fighters

Section 702 requires the Director of National Intelligence to submit a report every 60 days for the three years following the enactment of this Act to the congressional intelligence committees on foreign fighter flows to and from Syria and Iraq. Section 702 requires information on the total number of foreign fighters who have traveled to Syria or Iraq, the total number of United States persons who have traveled or attempted to travel to Syria or Iraq, the total number of foreign fighters in Terrorist Identities Datamart Environment, the total number of foreign fighters who have been processed with biometrics, any programmatic updates to the foreign fighter report, and a worldwide graphic that describes foreign fighter flows to and from Syria.

Section 703. Report on strategy, efforts, and resources to detect, deter, and degrade Islamic State revenue mechanisms

Section 703 requires the Director of National Intelligence to submit a report on the strategy, efforts, and resources of the Intelligence Community that are necessary to detect, deter, and degrade the revenue mechanisms of the Islamic State.

Section 704. Report on United States counterterrorism strategy to disrupt, dismantle, and defeat the Islamic State, al-Qa'ida, and their affiliated groups, associated groups, and adherents

Section 704 requires the President to submit to the appropriated congressional committees a comprehensive report on the counterterrorism strategy to disrupt, dismantle, and defeat the Islamic State, al-Qa'ida, and their affiliated groups, associated groups, and adherents.

Section 705. Report on effects of data breach of Office of Personnel Management

Section 705 requires the President to transmit to the congressional intelligence communities a report on the data breach of the Office of Personnel Management. Section 705 requires information on the impact of the breach on Intelligence Community operations abroad, in addition to an assessment of how foreign persons, groups, or countries may use data collected by the breach and what Federal Government agencies use best practices to protect sensitive data.

Section 706. Report on hiring of graduates of Cyber Corps Scholarship Program by intelligence community

Section 706 requires the Director of National Intelligence to submit to the congressional intelligence committees a report on the employment by the Intelligence Community of graduates of the Cyber Corps Scholarship Program. Section 706 requires information on the number of graduates hired by each element of the Intelligence Community, the recruitment process for each element of the Intelligence Community, and the Director recommendations for improving the hiring process.

Section 707. Report on use of certain business concerns

Section 707 requires the Director of National Intelligence to submit to the congressional intelligence committees a report of covered business concerns—including minority-owned, women-owned, small disadvantaged, service-enabled veteran-owned, and veteran-owned small businesses—among contractors that are awarded contracts by the Intelligence Community for goods, equipment, tools and services.

SUBTITLE B—OTHER MATTERS

Section 711. Use of homeland security grant funds in conjunction with Department of Energy national laboratories

Section 711 amends Section 2008 (a) of the Homeland Security Act of 2002 to clarify that the Department of Energy's national laboratories may seek access to homeland security grant funds.

Section 712. Inclusion of certain minority-serving institutions in grant program to enhance recruiting of intelligence community workforce

Section 712 amends the National Security Act of 1947 to include certain minority-serving institutions in the intelligence officer training programs established under Section 1024 of the Act.

The following consists of the joint explanatory statement to accompany Division N, the Cybersecurity Act of 2015, of the Consolidated Appropriations Act, 2016.

This joint explanatory statement reflects the status of negotiations and disposition of issues reached between the Senate Select Committee on Intelligence, the House Permanent Select Committee on Intelligence, the Senate Committee on Homeland Security and Governmental Affairs, and the House Committee on Homeland Security. The joint explanatory statement shall have the same effect with respect to the implementation of this Act as if it were a joint explanatory statement of a committee of conference.

The joint explanatory statement comprises an overview of the bill's background and objectives, and a section-by-section analysis of the legislative text.

PART I: BACKGROUND AND NEED FOR LEGISLATION

Cybersecurity threats continue to affect our nation's security and its economy, as losses to consumers, businesses, and the government from cyber attacks, penetrations, and disruptions total billions of dollars. This legislation is designed to create a voluntary cybersecurity information sharing process that will encourage public and private sector entities to share cyber threat information, without legal barriers and the threat of unfounded litigation—while protecting private information. This in turn should foster greater cooperation and collaboration in the face of growing cybersecurity threats to national and economic security.

This legislation also includes provisions to improve Federal network and information system security, provide assessments on the Federal cybersecurity workforce, and provide reporting and strategies on cybersecurity industry-related and criminal-related matters. The increased information sharing enabled by this bill is a critical step toward improving cybersecurity in America.

PART II: SECTION-BY-SECTION ANALYSIS AND EXPLANATION OF LEGISLATIVE TEXT

The following is a section-by-section analysis and explanation of the Cybersecurity Act of 2015.

TITLE I—CYBERSECURITY INFORMATION SHARING

Section 101. Short title.

Section 101 states that Title I may be cited as the ''Cybersecurity Information Sharing Act of 2015.''

Section 102. Definitions.

Section 102 defines for purposes of this title key terms such as ''cybersecurity purpose,'' ''cybersecurity threat,'' ''cyber threat indicator,'' ''defensive measure,'' and ''monitor.'' The definition of ''cybersecurity purpose'' is meant to include a broad range of activities taken to protect information and information systems from cybersecurity threats. The authorizations under this Act are tied to conduct undertaken for a ''cybersecurity purpose,'' which both clarifies their scope and ensures that the authorizations cover activities that can be performed in conjunction with one another. For instance, a private entity conducting monitoring activities to determine whether it should use an authorized ''defensive measure'' would be monitoring for a ''cybersecurity purpose.'' Significantly, the authorization for ''defensive measures'' does not include activities that are generally considered ''offensive'' in nature, such as unauthorized access of, or execution of computer code on, another entity's information systems, such as ''hacking back'' activities, or any actions that would substantially

harm another private entity's information systems, such as violations of section 1030, of title 18, United States Code.

Section 103. Sharing of information by the Federal Government.

Section 103 requires the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General to jointly develop and issue procedures for the timely sharing of classified and unclassified cyber threat indicators and defensive measures (hereinafter referenced collectively in this joint explanatory statement as, ''cyber threat information'') with relevant entities.

These procedures must also ensure the Federal Government maintains: a real-time sharing capability; a process for notifying entities that have received cyber threat information in error; protections against unauthorized access; and procedures to review and remove, prior to sharing cyber threat information, any information not directly related to a cybersecurity threat known at the time of sharing to be personal information of a specific individual or that identifies a specific individual, or to implement a technical capability to do the same. These procedures must be developed in consultation with appropriate Federal entities, including the Small Business Administration and the National Laboratories.

Section 104. Authorizations for preventing, detecting, analyzing, and mitigating cybersecurity threats.

Section 104 authorizes private entities to monitor their information systems, operate defensive measures, and share and receive cyber threat information. Private entities must, prior to sharing cyber threat information, review and remove any information not directly related to a cybersecurity threat known at the time of sharing to be personal information of a specific individual or that identifies a specific individual, or to implement and utilize a technical capability to do the same.

Section 104 permits non-Federal entities to use cyber threat information for cybersecurity purposes, to monitor, or to operate defensive measures on their information systems or on those of another entity (upon written consent). Cyber threat information shared by an entity with a State, tribal, or local department or agency may be used for the purpose of preventing, investigating, or prosecuting any of the offenses described in Section 105, below. Cyber threat information is exempt from disclosure under any State, tribal, local, or freedom of information or similar law.

Section 104 further provides that two or more private entities are not in violation of antitrust laws for exchanging or providing cyber threat information, or for assisting with the prevention, investigation, or mitigation of a cybersecurity threat.

Section 105. Sharing of cyber threat indicators and defensive measures with the Federal Government.

Section 105 directs the Attorney General and Secretary of Homeland Security to jointly develop policies and procedures to govern how the Federal Government shares information about cyber threats, including via an automated real-time process that allows for information systems to exchange identified cyber threat information without manual efforts, subject to limited exceptions that must be agreed upon in advance. Section 105 also directs the Attorney General and Secretary of Homeland Security, in coordination with heads of appropriate Federal entities and in consultation with certain privacy officials and relevant private entities, to jointly issue and make publicly available final privacy and civil liberties guidelines for Federal entity-based cyber information sharing.

Section 105 directs the Secretary of Homeland Security, in coordination with heads of appropriate Federal entities, to develop, implement, and certify the capability and process through which the Federal Government receives cyber threat information shared by a non-Federal entity with the Federal Government. This section also provides the President with the authority to designate an appropriate Federal entity, other than the Department of Defense (including the National Security Agency), to develop and implement an additional capability and process following a certification and explanation to Congress, as described in this section. The capability and process at the Department of Homeland Security, or at any additional appropriate Federal entity designated by the President, does not prohibit otherwise lawful disclosures of information related to criminal activities, Federal investigations, or statutorily or contractually required disclosures. However, this section does not preclude the Department of Defense, including the National Security Agency from assisting in the development and implementation of a capability and process established consistent with this title. It also shall not be read to preclude any department or agency from requesting technical assistance or staffing a request for technical assistance.

Section 105 further provides that cyber threat information shared with the Federal Government does not waive any privilege or protection, may be deemed proprietary information by the originating entity, and is exempt from certain disclosure laws. Cyber threat information may be used by the Federal government for: cybersecurity purposes; identifying a cybersecurity threat or vulnerability; responding to, preventing, or mitigating a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or a use of a weapon of mass destruction; responding to, investigating, prosecuting, preventing, or mitigating a serious threat to a minor; or preventing, investigating, disrupting, or prosecuting an offense arising out of certain cyber-related criminal activities.

Finally, Section 105 provides that cyber threat information shared with the Federal Government shall not be used by any Federal, State, tribal, or local government to regulate non-Federal entities' lawful activities.

Section 106. Protection from liability.

Section 106 provides liability protection for private entities that monitor, share, or receive cyber threat information in accordance with Title I, notwithstanding any other provision of Federal, State, local, or tribal law. Section 106 further clarifies that nothing in Title I creates a duty to share cyber threat information or a duty to warn or act based on receiving cyber threat information. At the same time, nothing in Title I broadens, narrows, or otherwise affects any existing duties that might be imposed by other law; Title I also does not limit any common law or statutory defenses.

Section 107. Oversight of Government activities.

Section 107 requires reports and recommendations on implementation, compliance, and privacy assessments by agency heads, Inspectors General, and the Comptroller General of the United States, to ensure that cyber threat information is properly received, handled, and shared by the Federal Government.

Section 108. Construction and preemption.

Section 108 contains Title I construction provisions regarding lawful disclosures; whistleblower protections; protection of sources and methods; relationship to other laws; prohibited conduct, such as anti-competitive activities; information sharing relationships; preservation of contractual rights and obligations; anti-tasking restrictions, including conditions on cyber threat information sharing; information use and retention; Federal preemption of State laws that restrict or regulate Title I activities, excluding those concerning the use of authorized law enforcement practices and procedures; regulatory authorities; the Secretary of Defense's authorities to conduct certain cyber operations; and Constitutional protections in criminal prosecutions.

Section 109. Report on cybersecurity threats.

Section 109 requires the Director of National Intelligence, with the heads of other appropriate Intelligence Community elements, to submit a report to the congressional intelligence committees on cybersecurity threats, including cyber attacks, theft, and data breaches.

Section 110 Exception to limitation on authority of Secretary of Defense to disseminate certain information.

Section 110 clarifies that, notwithstanding Section 393(c)(3) of title 10, United States Code, the Secretary of Defense may authorize the sharing of cyber threat indicators and defensive measures pursuant to the policies, procedures, and guidelines developed or issued under this title.

Section 111. Effective period.

Section 111 establishes Title I and the amendments therein are effective during the period beginning on the date of enactment of this Act and ending on September 30, 2025. The provisions of Title I will remain in effect however, for action authorized by Title I or information obtained pursuant to action authorized by Title I, prior to September 30, 2025.

TITLE II—NATIONAL CYBERSECURITY ADVANCEMENT

SUBTITLE A—NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

Section 201. Short title.

Section 201 establishes that Title II, Subtitle A may be cited as the ''National Cybersecurity Protection Advancement Act of 2015''.

Section 202. Definitions.

Section 202 defines for purposes of Title II, Subtitle A, the terms ''appropriate congressional committees,'' ''cybersecurity risk,'' ''incident,'' ''cyber threat indicator,'' ''defensive measure,'' ''Department,'' and ''Secretary.''

Section 203. Information sharing structure and processes.

Section 203 enhances the functions of the Department of Homeland Security's National Cybersecurity and Communications Integration Center, established in section 227 of the Homeland Security Act of 2002 (redesignated by this Act). It designates the Center as a Federal civilian interface for multi-directional and cross-sector information sharing related to cybersecurity risks, incidents, analysis and warnings for Federal and non-Federal entities, including the implementation of Title I of this Act. This section requires the Center to engage with international partners; conduct information sharing with Federal and non-Federal entities; participate in national exercises; and assess and evaluate consequence, vulnerability and threat information regarding cyber incidents to public safety communications. Additionally, this section requires the Center to collaborate with state and local governments on cybersecurity risks and incidents. The Center will comply with all policies, regulations, and laws that protect the privacy and civil liberties of United States persons, including by working with the Privacy Officer to ensure the Center follows the privacy policies and procedures established by title I of this Act.

Section 203 requires the Department of Homeland Security, in coordination with industry and other stakeholders, to develop an automated capability for the timely sharing of cyber threat indicators and defensive measures. It is critical for the Department to develop an automated system and supporting processes for the Center to disseminate cyber threat indicators and defensive measures in a timely manner.

This section permits the Center to enter into voluntary information sharing relationships with any consenting non-Federal entity for the sharing of cyber threat indicators, defensive measures, and information for cybersecurity purposes. This section is intended to provide the Department of Homeland Security additional options to enter into streamlined voluntary information sharing agreements. This section allows the Center to utilize standard and negotiated agreements as the types of agreements that non-Federal entities may enter into with the Center. However, it makes clear that agreements are not limited to just these types, and preexisting agreements between the Center and the non-Federal entity will be in compliance with this section.

Section 203 requires the Director of the Center to report directly to the Secretary for significant cybersecurity risks and incidents. This section requires the Secretary to submit to Congress a report on the range of efforts underway to bolster cybersecurity collaboration with international partners. Section 203 allows the Secretary to develop and adhere to Department policies and procedures for coordinating vulnerability disclosures.

Section 204. Information sharing and analysis organizations.

Section 204 amends Section 212 of the Homeland Security Act to clarify the functions of Information Sharing and Analysis Organizations (ISA0s) to include cybersecurity risk and incident information beyond that pertaining to critical infrastructure. ISA0s, including Information Sharing and Analysis Centers (ISACs) have an important role to play in facilitating information sharing going forward and has clarified their functions as defined in the Homeland Security Act.

Section 205. National response framework

Section 205 amends the Homeland Security Act of 2002 to require the Secretary of the Department of Homeland Security, with proper coordination, to regularly update the Cyber Incident Annex to the National Response Framework of the Department of Homeland Security.

Section 206 Report on reducing cybersecurity risks in DHS data centers.

Section 206 requires the Secretary of the Department of Homeland Security to submit a report to Congress not later than 1 year after the date of the enactment of this Act on the feasibility of using compartmentalization between systems to create conditions conducive to reduced cybersecurity risks in data centers.

Section 207. Assessment.

Section 207 requires the Comptroller General of the United States not later than 2 years after the date of enactment of this Act to submit a report on the implementation of Title II, including increases in the sharing of cyber threat indicators at the National Cybersecurity and Communications Integration Center and throughout the United States.

Section 208. Multiple simultaneous cyber incidents at critical infrastructure.

Section 208 requires the appropriate Department of Homeland Security Under Secretary to draft and submit to Congress not later than 1 year after the date of enactment of this Act a report on the feasibility of producing a risk-informed plan to address the risks of multiple simultaneous cyber incidents affecting critical infrastructure as well as cascade effects.

Section 209. Report on cybersecurity vulnerabilities of United States ports.

Section 209 requires the Secretary of Homeland Security not later than 180 days after the date of enactment of this Act to submit to Congress a report on the vulnerability of United States ports to cybersecurity incidents, as well as potential mitigations.

Section 210. Prohibition on new regulatory authority.

Section 210 clarifies that the Secretary of Homeland Security does not gain any additional regulatory authorities in this subtitle.

Section 211. Termination of reporting requirements.

Section 211 adds a 7–year sunset on the reporting requirements in Title II, Subtitle A.

SUBTITLE B—FEDERAL CYBERSECCRITY ENHANCEMENT

Section 221. Short title.

Section 221 establishes that Title II, Subtitle B may be cited as the ''Federal Cybersecurity Enhancement Act of 2015''.

Section 222. Definitions.

Section 222 defines for purposes of Title II, Subtitle B, the terms ''agency,'' ''agency information system,'' ''appropriate congressional committees,'' ''cybersecurity risk,'' ''information system,'' ''Director,'' ''intelligence community,'' ''national security system,'' and ''Secretary.''

Section 223. Improved Federal network security.

Section 223 amends the Homeland Security Act of 2002 by amending Section 228, as redesignated, to require an intrusion assessment plan for Federal agencies and adding a Section 230 to authorize a federal intrusion detection and prevention capabilities'' for Federal agencies.

Section 230 of the Homeland Security Act of 2002, as added by Section 223(a) of the bill, authorizes the Secretary of Homeland Security to employ the Department's intrusion detection and intrusion prevention capabilities, operationally implemented under the ''EINSTEIN'' programs, to scan agencies' network traffic for malicious activity and block it. The Secretary and agencies with sensitive data are expected to confer regarding the sensitivity of, and statutory protections otherwise applicable to, information on agency information systems. The Secretary is expected to ensure that the policies and procedures developed under section 230 appropriately restrict and limit Department access, use, retention, and handling of such information to protect the privacy and confidentiality of such information, including ensuring that the Department protects such sensitive data from disclosure, and trains appropriate staff accordingly.

Section 223(b) mandates that agencies deploy and adopt those capabilities within one year for all network traffic traveling to or from each information system owned or operated by the agency, or two months after the capabilities are first made available to the agency, whichever is later. The subsection also requires that agencies adopt improvements added to the intrusion detection and prevention capabilities six months after they are made available. Improvements is intended to be read broadly to describe expansion of the capabilities, new systems, and added technologies, for example: non-signature based detection systems such as heuristic- and behavior-based detection, new countermeasures to block malicious traffic beyond e-mail filtering and Domain Name System (DNS)-sinkholing,[1] and scanning techniques that allow scanning of encrypted traffic.

Section 224. Advanced internal defenses.

Section 224 directs the Secretary of Homeland Security to add advanced network security tools to the Continuous Diagnostics and Mitigation program; develop and implement a plan to ensure agency use of advanced network security tools; and, with the Director of the Office of Management and Budget, prioritize advanced security tools and update metrics used to measure security under the Federal Information Security Management Act of 2002.

Section 225. Federal cybersecurity requirements.

Section 225 adds a statutory requirement for the head of each agency not later than 1 year after the date of the enactment of this Act to implement several standards on their networks to include identification of sensitive and mission critical data, use of encryption, and multi-factor authentication.

Section 226. Assessment; reports.

Section 226 includes a requirement for a Government Accountability Office study to be conducted on the effectiveness of this approach and strategy. It also requires reports

from the Department of Homeland Security, Federal Chief Information Officer, and the Office of Management and Budget. Required reporting includes an annual report from the Department of Homeland Security on the effectiveness and privacy controls of the intrusion detection and prevention capabilities; information on adoption of the intrusion detection and capabilities at agencies in the Office of Management and Budget's annual Federal Information Security Management Act report; an assessment by the Federal Chief Information Officer within two years of enactment as to continued value of the intrusion detection and prevention capabilities; and a Government Accountability report in three years on the effectiveness of Federal agencies' approach to securing agency information systems.

Section 227. Termination.

Section 227 creates a 7-year sunset for the authorization of the intrusion detection and prevention capabilities in Section 230 of the Homeland Security Act of 2002, as added by Section 223(a).

Section 228. Identification of information systems relating to national security.

Section 228 requires the Director of National Intelligence and the Director of the Office of Management, in coordination with other agencies, not later than 180 days after the date of enactment of this Act to identify unclassified information systems that could reveal classified information, and submit a report assessing the risks associated with a breach of such systems and the costs and impact to designate such systems as national security systems.

Section 229. Direction to agencies.

Section 229 authorizes the Secretary of Homeland Security to issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of an information system for the purpose of protecting such system from an information security threat. In situations in which the Secretary has determined there is an imminent threat to an agency, the Secretary may authorize the use of intrusion detection and prevention capabilities in accordance with established procedures, including notice to the affected agency.

TITLE III—FEDERAL CYBERSECURITY WORKFORCE ASSESSMENT

Section 301. Short title.

Section 301 establishes Title III may be cited as the ''Federal Cybersecurity Workforce Assessment Act of 2015''.

Section 302. Definitions.

Section 302 defines for purposes of Title III the terms ''appropriate congressional committees,'' ''Director,'' ''National Initiative for Cybersecurity Education,'' and ''work roles.''

Section 303. National cybersecurity workforce measurement initiative.

Section 303 requires the head of each Federal agency to identify all positions within the agency that require the performance of cybersecurity or other cyber-related functions, and report the percentage of personnel in such positions holding the appropriate certifications, the level of preparedness of personnel without certifications to take certification exams, and a strategy for mitigating any identified certification and training gaps.

Section 304. Identification of cyber-related work roles of critical need.

Section 304 requires the head of each Federal agency to identify information technology, cybersecurity, or other cyber-related roles of critical need in the agency's workforce, and substantiate as such in a report to the Director of the Office of Personnel Management. Section 304 also requires the Director of the Office of Personnel Management to submit a subsequent report not later than 2 years after the date of the enactment of this Act, on critical needs for information technology, cybersecurity, or other cyber-related workforce across all Federal agencies, and the implementation of this section.

Section 305. Government Accountability Office status reports.

Section 305 requires the Comptroller General of the United States to analyze and monitor the implementation of sections 303 and 304 and not later than 3 years after the date of the enactment of this Act submit a report on the status of such implementation.

TITLE IV—OTHER CYBER MATTERS

Section 401. Study on mobile device security.

Section 401 requires the Secretary of Homeland Security not later than 1 year after the date of the enactment of this Act to conduct a study on threats relating to the security of the mobile devices used by the Federal Government, and submit a report detailing the findings and recommendations arising from such study.

Section 402. Department of State international cyberspace policy strategy.

Section 402 requires the Secretary of State not later than 90 days after the date of the enactment of this Act to produce a comprehensive strategy relating to United States international policy with regard to cyberspace, to include a review of actions taken by the Secretary of State in support of the President's International Strategy for Cyberspace and a description of threats to United States national security in cyberspace.

Section 403. Apprehension and prosecution of international cyber criminals.

Section 403 requires the Secretary of State, or a designee, to consult with countries in which international cyber criminals are physically present and extradition to the United States is unlikely, to determine what efforts the foreign country has taken to apprehend, prosecute, or otherwise prevent the carrying out of cybercrimes against United States persons or interests. Section 403 further requires an annual report that includes statistics and extradition status about such international cyber criminals.

Section 404. Enhancement of emergency services.

Section 404 requires the Secretary of Homeland Security not later than 90 days after the date of the enactment of this Act to establish a process by which a Statewide Interoperability Coordinator may report data on any cybersecurity risk or incident involving any information system or network used by emergency response providers within the state. Reported data will be analyzed and used in developing information and recommendations on security and resilience on measures for information systems and networks used by state emergency response providers.

Section 405. Improving cybersecurity in the health care industry.

Section 405 requires the Secretary of Health and Human Services to establish a task force and not later than 1 year after the date of enactment of the task force to submit a report on the Department of Health and Human Services and the health care industry's preparedness to respond to cybersecurity threats. In support of the report, the Secretary of Health and Human Services will convene health care industry stakeholders, cybersecurity experts, and other appropriate entities, to establish a task force for analyzing and disseminating information on industry-specific cybersecurity challenges and solutions.

Consistent with subsection (e), it is Congress's intention to allow Health and Human Services the flexibility to leverage and incorporate ongoing activities as of the day before the date of enactment of this act to accomplish the goals set forth for this task force.

Section 406. Federal computer security.

Section 406 requires the Inspector General of any agency operating a national security system, or a Federal computer system that provides access to personally identifiable information, not later than 240 days after the date of enactment of this Act to submit a report regarding the federal computer systems of such agency, to include information on the standards and processes for granting or denying specific requests to obtain and use information and related information processing services, and a description of the data security management practices used by the agency.

Section 407. Stopping the fraudulent sale offinancial information of people of the United States.

Section 407 amends 18 U.S. Code § 1029 by enabling the Federal Government to prosecute overseas criminals who profit from financial information that has been stolen from Americans.

ENDNOTE

[1] Use of a DNS server configured to direct attackers away from network infrastructure.

Mrs. LOWEY. Mr. Speaker, I am very pleased to yield 2 minutes to the distinguished gentlewoman from Minnesota (Ms. MCCOLLUM), the ranking minority member of the Interior, Environment, and Related Agencies Subcommittee.

Ms. MCCOLLUM. Mr. Speaker, I rise in support of this omnibus appropriations agreement.

This agreement reflects a truly bipartisan compromise that fulfills Congress' most basic responsibility: to fund the operations of the Federal Government.

As the ranking member of the Interior, Environment, and Related Agencies Subcommittee, I am thrilled to be supporting our subcommittee's section of the bill. I want to remind everyone that in July, our bill died on the floor. It was underfunded, and it was loaded with partisan riders that harmed the environment and failed to meet the needs of the American people.

This is not a perfect bill, but it is a remarkable improvement. This bill