[Congressional Record Volume 165, Number 199 (Thursday, December 12, 2019)]
[House]
[Pages H10237-H10254]

EXPLANATORY MATERIAL STATEMENT ON INTELLIGENCE AUTHORIZATION MEASURES FOR FISCAL YEARS 2018, 2019, AND 2020, SUBMITTED BY MR. SCHIFF, CHAIRMAN OF THE HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE

The following is the explanation of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (hereinafter, ``the Act'').

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

The explanation 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 HPSCI and SSCI (collectively, 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 (IC) 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 congressional intelligence committees. They reconcile the differences between the congressional intelligence committees' respective versions of the bill for the National Intelligence Program (NIP) for Fiscal Years 2018, 2019, and 2020. The Agreement also makes recommendations for the Military Intelligence Program (MIP) and the Information Systems Security Program (ISSP), consistent with the National Defense Authorization Act for Fiscal Year 2020, and provides certain direction for these two programs. The Agreement applies to IC activities for Fiscal Year 2020.

The classified Schedule of Authorizations is incorporated into the bill pursuant to Section 5102 of Subdivision 1. 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 congressional intelligence committees view direction and recommendations, whether contained in this explanation or in the classified annex, as requiring compliance by the Executive Branch.

Part II: Select Unclassified Congressional Direction

Unclassified Direction related to Subdivision 1 of the Act relates to Fiscal Year 2020. Unclassified Direction related

to Subdivision 2 originated in Fiscal Years 2018 and 2019. The term ``Committees'' refers to both SSCI and HPSCI.

[[Page H10238]]

Unclassified Direction Related to Subdivision 1

Plans for Operations During Government Shutdowns by All Elements of the Intelligence Community.

The Committees have an active interest in the impact of government shutdowns on the intelligence mission. Office of Management and Budget (OMB) Circular A-11, Section 124, outlines how agencies are supposed to plan for operations during government shutdowns, and Section 124.2 provides that agencies must share those plans with OMB. Additionally, Section 323 of the Intelligence Authorization Act for Fiscal Year 2014 requires the Office of the Director of National Intelligence (ODNI), the Central Intelligence Agency (CIA), and IC elements within the Department of Defense (DoD) to share those same plans with specified congressional committees, including the congressional intelligence committees.

These requirements, however, omit IC elements that are not separate ``agencies'' for the purposes of OMB Circular A-11, Section 124, and are not ODNI, CIA, or elements within the DoD for the purposes of the IAA for Fiscal Year 2014. As a result, no such reporting requirement currently exists for IC elements within the Departments of Justice, Treasury, Energy, State, and Homeland Security. For that reason, when portions of the federal government were shut down between December 2018 and February 2019, the Committees had little to no insight into the effects of the shutdown on these and other important segments of the IC.

Therefore, the Committees direct IC elements within the Departments of Justice, Treasury, Energy, State, and Homeland Security to submit to the congressional intelligence committees--on the same day as the host department's issuance of any plan for a government shutdown--the number of personnel in their respective elements that will be furloughed.

Program Manager-Information Sharing Environment Review.

Section 1016 of the Intelligence Reform and Terrorism Protection Act of 2004 (IRTPA) created a Program Manager-Information Sharing Environment (PM-ISE), administered from within the ODNI, to better facilitate the interagency sharing of terrorism-related information. Section 1016 also designated the PM-ISE as a presidentially-appointed position. Section 6402 of Subdivision 2 of the Act amends the IRTPA, so that the PM-ISE is subject to appointment by the Director of National Intelligence (DNI), not the President. Since the establishment of the PM-ISE, the Federal government has created entities, procedures, and processes to address directly the mandate for improved terrorism information sharing. Accordingly, the Committees find it appropriate to reconsider the future of the PM-ISE's mission.

Therefore, the Committees direct the ODNI, in consultation with appropriate Federal departments, agencies, and components, within 180 days of enactment of this Act, to conduct a review of the PM-ISE's terrorism information sharing mission, associated functions, and organizational role within the ODNI and provide findings and recommendations on the future of the PM-ISE to Congress.

Leveraging Academic Institutions in the Intelligence Community.

The Committees encourage the DNI and the Director of the

DIA to ensure that IC elements continue to forge tighter partnerships with leading universitiesand their affiliated research centers in order to enhance mutual awareness of domestic and international challenges, leverage subject matter experts from higher education in a manner that uses cutting edge technologies and methods, and bolsters the recruitment of top-notch, diverse, and technically proficient talent into the IC's workforce.

The Committees further believe that IC-sponsored academic programs such as the Intelligence Community Centers for Academic Excellence (IC-CAE) should work closely with educational institutions that offer interdisciplinary courses of study and learning opportunities in national and international security; geopolitical affairs, international relations and national security; interdisciplinary courses of study in the culture, history, languages, politics, and religions of major world regions; foreign language instruction; computer and data science; or cybersecurity.

The DNI shall ensure that such programs are facilitated via the streamlining of the security clearance process for graduating students from such universities who receive offers of employment from IC elements, provide for the temporary exchange of faculty and IC professionals, including as visiting fellows, and technical training opportunities for faculty, students, and IC personnel.

Therefore, the Committees direct all IC agencies to support the IC-CAE effort by tracking recruits and new hires who have graduated from IC-CAE-designated institutions, promptly reporting these numbers to the office in charge of IC-CAE implementation, and increasing all IC agencies' efforts to recruit from such institutions.

Access to Sensitive Compartmented Information Facilities.

The Committees remain concerned about impediments for companies with appropriately cleared personnel being able to perform work for government entities and the effects of these impediments on IC access to innovative products and services. For example, businesses without access to a Sensitive Compartmented Information Facility (SCIF), which includes many small businesses and non-traditional contractors, find it difficult to perform classified work for the IC. Construction and accreditation of SCIF spaces may be cost-prohibitive for small business and non-traditional government contractors.

Additionally, SCIF construction timelines often exceed the period of performance of a contract. A modern trend for innovative and non-traditional government contractors is the use of co-working space environments. Additionally, public and private entities are partnering to create emerging regional innovation hubs to help identify technology solutions and products in the private sector that can be utilized by the DoD and IC. These innovation hubs currently produce an agile, neutral, but largely unclassified, development environment.

Therefore, the Committees direct the ODNI to submit a report to the congressional intelligence committees on:

1. Processes and procedures necessary to build, certify, and maintain certifications for multi-use sensitive compartmented facilities not tied to a single contract and where multiple companies can securely work on multiple projects at different security levels;

2. Analysis of the advantages and disadvantages of issuing DoD Contract Security Specification (DD Form 254s) to Facilities'' as opposed to Contracts'';

3. Options for classified co-use and shared workspace environments such as innovation, incubation, catalyst, and accelerator environments;

4. Pros and cons for public, private, government, or combination owned facilities that can operate at different classification levels; and

5. Any other opportunities to support companies with appropriately cleared personnel but without effective access to a neutral SCIF.

Inclusion of Security Risks in Program Management Plans Required for Acquisition of Major Systems in the National Intelligence Program.

Section 5305 of Subdivision 1 of the Act adds security risk as a factor for the DNI to include in the annual Program Management Plans for major system acquisitions submitted to the congressional intelligence committees pursuant to Section 102A(q)(1)(A) of the National Security Act of 1947 (50 U.S.C. 3024(q)(1)(A)). The Committees are increasingly concerned with the security risks to IC acquisitions. The Joint Explanatory Statement accompanying the Intelligence Authorization Act for Fiscal Year 2017 directed updates to Intelligence Community Directive 731, Supply Chain Risk Management, and Committee leadership has engaged senior industry representatives about the threats to the national security industrial base posed by adversaries and competitors, including China. Over the past few years, the Department of Defense has been elevating security as a ``fourth pillar'' (to complement cost, schedule, and performance) in reviewing defense acquisitions, embodied in the Under Secretary of Defense for Intelligence's ``Deliver Uncompromised'' initiative.

Section 5305 of the Act extends that focus to the IC, requiring the annual Program Management Plans to include security risks in major system acquisitions, in addition to cost, schedule, and performance. The Committees recognize that security can be applied across a number of areas (facilities, personnel, information, and supply chain) and may vary by program, to appropriately ensure system integrity and mission assurance.

Therefore, for the purposes of implementing section 5305 of the Act, the Committees direct the Director of National Intelligence, with the Director of the National Counterintelligence and Security Center, to develop parameters for including security risks (and risk management measures) in the annual Program Management Plans to assist congressional oversight.

Intelligence Community Public-Private Talent Exchange.

The Committees fully support section 5306 of Subdivision 1's implementation in accordance with applicable federal ethics laws, regulations, and policies.

Expansion of Scope of Protections for Identities of Covert Agents.

Section 5303 of Subdivision 1 of the Act removes temporal and geographic limitations on the definition of ``covert agent'', as that term was defined by Section 606 of the Intelligence Identities Protection Act of 1982, P.L. 97-200 (Jun. 23, 1982) (IIPA).

Such limitations originally carved out of the IIPA unauthorized disclosures of certain kinds of classified identity information--those generally involving persons who have not served or acted abroad in the last five years--on grounds that such disclosures are generally less harmful to national security, and therefore undeserving of IIPA protections. But experience since then has proven otherwise. With the benefit of experience, the Committees have concluded that any disclosure of currently classified identity information, without regard to the location or recency of the activities of the person whose information is disclosed, can risk serious harm to national security. That being the case, such disclosures should potentially present a basis, under appropriate circumstances, for prosecution under the IIPA.

[[Page H10239]]

The Committees wish to stress, however, that the change

does not imply any enhanced risk of IIPA liability for journalists.

In the thirty-seven years since enactment, the statute has never been used to prosecute members of the media. In fact, prosecutors have charged violations of the IIPA in only two cases, both of which involved unauthorized disclosures by former federal government employees of classified information obtained during their employment. The Committees view this spare record, so far as traditional newsgathering and publication is concerned, as reflecting the heavy, constraining influence of the First Amendment's Press Clause. Journalists continue to this day to report aggressively on intelligence matters.

The IIPA's enforcement history also reflects the narrowness of Section 601(c), a provision which some have interpreted to expose traditional journalists to the risk of liability under the statute. But in the Committees' view, that provision does not cover responsibly investigating and reporting news in the public interest. There is a high burden for conviction under Section 601(c). It requires a prosecutor to prove beyond a reasonable doubt, among other things, that a defendant engaged in a ``pattern of activities'': a series of acts with the common purpose or objective of identifying and publicly exposing covert agents. Such conduct entails ``engag[ing] in a purposeful enterprise of revealing covert identities'' or being in the ``business of naming names,'' as the Conference Report to the IIPA put it in 1982. H.R. Rep. No. 97-580, at 9 (1982).

Traditional news gathering and publication--including on abuses of power, violations of law and civil liberties, and other controversial activity--does not require, or even typically involve, such conduct. Indeed, as the Conferees illustrated the point:

The reporters who have investigated the activities of Wilson and Terpil, former CIA employees who allegedly supplied explosives and terrorist training to Libya, would not be covered even if they revealed the identity of covert agents if their pattern of activities was intended to investigate illegal or controversial activities, and not to identify covert agents. Similarly, David Garrow would not be within the scope of the statute even though he purported to give the identity of covert agents in his book, ``The FBI and Martin Luther King, Jr.: from `Solo' to Memphis.'' His intent presumably was to explain what drove the FBI to wiretap Martin Luther King and not to identify and expose covert agents.

H.R. Rep. No. 97-580, at 10. The same holds true for traditional, responsible journalists today. Even after amendments made by the Act, their work does not risk liability under the revised IIPA.

Furthermore, section 5303 has no effect on what information may be withheld under the Freedom of Information Act, 5 U.S.C. Sec. 552 (FOIA). Section 5303 expands the universe of ``covert agents'' whose classified relationship with the United States Government is protected by the criminal law. All of the people protected by the expanded ``covert agent'' definition have a relationship with the United States government that is already classified. If an individual's relationship with the government is classified, it may be withheld under FOIA. Consequently, even before passage of section 5303, identifying information for all of the individuals covered by the IIPA expansion could already have been withheld under FOIA's (b)(1) exemption for national security information. In general, when justifying withholding under FOIA information that tends to identify covert agents, agencies should use (b)(1) classification exemptions, not (b)(3) exemptions regarding the IIPA and other statutes. 5 U.S.C. Sec. Sec. 552(b)(1), (3).

Section 5303 is not intended to--and does not--affect

Congress' authority to oversee the IC. Section 5303 is not intended to--and does not--affect the protections afforded to whistleblowers to disclose violations of law and waste, fraud, and abuse to Inspectors General or to Congress.

Intelligence Community Cooperation with the Government Accountability Office.

The Committees believe the Government Accountability Office (GAO) adds significant value to the Committees' oversight efforts. For example, the GAO's designation in 2018 of the government-wide Personnel Security Clearance process to its high-risk list of federal areas needing reform to prevent waste, fraud, abuse, and mismanagement, was important to the Committees' efforts to legislate on security clearance reform, including in this Act. The Committees expect that all IC elements will fully and promptly comply with requests from the GAO made to support studies requested by, or of interest to, the Committees.

Clarification of Death Benefits for Survivors of Central Intelligence Agency Personnel.

The Committees concur with the Executive Branch that section 5341 of Subdivision 1 of the Act shall apply retroactively from the date of enactment of this Act.

Intelligence Community Leave Policies.

The Committees find it imperative that the federal government, to include the IC, recruit, hire, and retain a highly qualified workforce. That depends in part on offering federal personnel a competitive benefits package--including with respect to parental leave and related benefits. Toward that end, the Committees strongly believe the federal government must align such benefits to the fullest extent possible with those of leading U.S. private sector companies and other industrialized countries.

In furtherance of that objective, the Committees in their respective bills supported a provision to provide twelve weeks of paid parental leave to all IC employees. The Committees further support the succeeding provision in the National Defense Authorization Act (NDAA) for Fiscal Year 2020 that provides government employees, to include those in the IC, with twelve weeks of paid administrative leave in the event of birth of a child, or the placement of a child for purposes of adoptive or foster care. This is consistent with, and supersedes, provisions that were contained in the House-passed and Senate-passed Intelligence Authorization Acts for Fiscal Years 2018, 2019, and 2020. Importantly, that NDAA provision does not modify or otherwise affect the eligibility of an IC employee for benefits relating to leave under any other provision of law, to include the provisions of the Family and Medical Leave Act (FMLA), 29 U.S.C. Sec. 2601, et seq.

Moreover, so far as concerns the provision's implementation, the Committees direct the DNI, within 180 days after enactment of this Act, to provide a briefing for the Committees on how each element of the IC will implement 5 U.S.C. section 6382(d)(2), as provided by this Act.

Transfer of National Intelligence University.

The Committees have been closely watching the evolution of how the IC provides for advanced intelligence education. The Defense Intelligence Agency (DIA) has hosted an intelligence college since 1962, which has been academically accredited since 1983. When the ODNI was created in the Intelligence Reform and Terrorism Prevention Act of 2004, ODNI created a separate National Intelligence University (NIU) under its auspices as a complement to DIA's intelligence effort. In response to a report from the President's Intelligence Advisory Board that accused the ODNI of being inadequately focused, the ODNI in 2011 transferred the NIU to DIA's intelligence college and rebranded the new combined institution as NIU.

Pursuant to the Joint Explanatory Statement to the

Intelligence Authorization Act for Fiscal Year 2017, an independent panel offered alternative governance models to enhance NIU, to include a more prominent role for ODNI. In parallel, analyses of DIA by the Secretary of Defense and the HPSCI during the 115th Congress concluded that DIA would benefit from moving NIU elsewhere in the IC.

The Committees believe transferring NIU to ODNI is now appropriate if certain conditions, contained in section 5324 of Subdivision 1 of the Act, are met. The Committees believe that clear commitment from the DNI and Principal Deputy DNI is critical to NIU's success at ODNI. The Committees look forward to working with ODNI and DoD on the successful transfer of NIU.

Associate Degree Program Eligibility.

The Committees are concerned that students enrolled in, or who have graduated from, Associate Degree programs have insufficient opportunities to gain employment in the IC. Therefore, the Committees direct the ODNI to submit a report to the congressional intelligence committees on how to expand the number of opportunities for students pursuing or having earned an Associate Degree eligible for IC academic programs. The Committees also direct the ODNI to make information about these academic programs publicly available.

Exposing Predatory and Anticompetitive Foreign Economic Influence.

The Committees are concerned about the significant threat posed by foreign governments that engage in predatory and anticompetitive behaviors aimed to undercut critical sectors of the United States economy. Therefore, the Committees direct the DNI, in consultation with the Assistant Secretary of the Treasury for Intelligence and Analysis, to submit to the congressional intelligence committees a report identifying top countries that pose a substantial threat to the United States economy regarding technology transfer issues, predatory investment practices, economic espionage, and other anticompetitive behaviors. The report shall be submitted in unclassified form to the greatest extent possible, but may include a classified annex.

Furthermore, the DNI, in consultation with the Department of the Treasury and other agencies that the Director deems appropriate,shall submit a report to the congressional intelligence committees assessing the costs and benefits of requiring a foreign person or entity that invests in the United States (and is subject to the jurisdiction of a country that poses a substantial threat to the United States economy) to submit annual disclosures to the Federal Government. Such disclosures would include all investments that the foreign person or entity made in the United States during the preceding year; the ownership structure of the entity; and any affiliation of the entity with a foreign government. The report should detail how such information could be used by the IC and other elements of the Federal government working to identify and combat foreign threats to the United States economy, and the appropriate scope and thresholds for such disclosures. The report shall be submitted in unclassified form, but may include a classified annex.

Increasing Data Security.

The Committees are aware the IC faces challenges while trying to balance mission

[[Page H10240]]

and enterprise needs with IT modernization, including the migration of data and applications to the cloud. With this in mind, the Committees encourage the IC to identify and utilize technologies that increase the security posture of data and workloads and reduce cyber risks.

The Committees further recommend that:

1. IC elements identify, develop, and implement tools for bi-directional data migration and division interoperability between data center and cloud environments;

2. These tools include, but are not limited to, encryption of data while both at rest and in motion, and micro-segmentation of networks and workloads; and

3. IC elements prioritize shifting resources towards automation as a way to respond more quickly to cyber threats.

Anonymous Annual Survey Regarding Workplace Climate.

IC elements obtain mission-critical information from the results of anonymous, annual surveys of their employees, on issues related to workplace climate and retention. As necessary as they are to the elements' own activities, survey results are also vital to the Committees' continuing oversight of elements' efforts to address workplace climate and retention issues, and to propose legislative and other remedies where appropriate.

The need for reliable information is especially acute with respect to sexual harassment and discrimination, given that--established policy and legal protections notwithstanding--an employee may fear that directly raising concerns about such matters risks exposing the employee to retaliatory personnel, security clearance, or other actions. The anonymous survey affords the element, and the Committees, a mechanism for inquiring further about the extent of this well-documented chilling effect against reporting; and about the effectiveness (or not) of ongoing programs to uncover and root out sexual harassment, discrimination, and other illegal and/or inappropriate activities at the workplace.

Therefore, the Committees direct that no later than 180 days after enactment of this Act, the DNI must certify in writing to the congressional intelligence committees that:

1. At least once a year, each element of the IC submits a survey to its employees regarding workplace climate and retention matters, and affords employees completing such surveys the option to remain anonymous;

2. Such survey includes questions regarding employees' experiences with sexual assault, discrimination, harassment, including sexual harassment, and related retaliation, including, at a minimum, the questions covering the following topics:

a. Have you witnessed sexual harassment or sexual assault?

i. Did you report it?

ii. If not, why not?

b. Have you experienced sexual harassment or sexual assault?

i. Did you report it?

ii. If not, why not?

c. Have you experienced retaliation for reporting harassment, discrimination, or sexual assault?

i. Have you faced retribution for taking leave for family, medical, or other personal reasons?

ii. Did you fear retribution for taking leave?

3. Each element includes in its survey questions regarding the job series, position, age, gender, race or ethnicity, field, and job location at the time of the survey's completion;

4. Each element tracks employees' responses according to job series, position, age, gender, race or ethnicity, field, and location at the time of the survey's completion; and

5. Each element reports the results of its survey annually to the congressional intelligence committees.

Report to Congress on the Representation of Women and Minorities in the Workforce.

The Committees continue to strongly support IC efforts to identify, recruit, and retain a highly diverse and highly qualified workforce--including, in particular, its efforts to increase the representation within elements of the IC of women and minorities.

This is a data driven exercise. Bolstering and adjusting IC workforce diversity programs depends in part on the Committees' regularly obtaining current, detailed, and reliable information, and about specific matters relevant to the broader subject of workforce diversity--such as rates and areas of promotion of women and minority employees. However, some elements may produce such information only from time to time; others may make regular submissions to the Committees but include only general information.

Therefore, the Committees direct that every six months, the head of each element of the IC shall submit to the Committees a written report that shall include, at a minimum:

1. The total number of women and minorities hired by that element during the reporting period and a calculation of that figure as a percentage of the agency's total hiring for that period;

2. The distribution of women and minorities at that element by grade level and by job series in the element's total workforce during the reporting period, together with comparisons from the immediately preceding two years;

3. The number of women and minorities who applied for promotion at the element and the final number selected for promotion during the reporting period;

4. The proportion of the total workforce of the element occupied by each group or class protected by law, as of the last day of the reporting period;

5. The numbers of minorities and women serving in positions at the element requiring advanced, specialized training or certification, as well as the proportion of the workforce those groups occupy; and

6. To the extent that such element deploys civilian employees to hazardous duty locations, the number of women and minority employees who departed government service subsequent to a deployment undertaken by an employee in the previous two years.

Report on Geospatial Commercial Activities for Basic and Applied Research and Development.

The Committees direct the Director of the National Geospatial-Intelligence Agency (NGA), in coordination with the DNI, the Director of the Central Intelligence Agency (CIA), and the Director of the National Reconnaissance Office (NRO), within 90 days of enactment of this Act, to submit to the congressional intelligence and defense committees a report on the feasibility, risks, costs, and benefits of providing the private sector and academia, on a need-driven and limited basis--consistent with the protection of sources and methods, as well as privacy and civil liberties--access to data in the possession of the NGA for the purpose of assisting the efforts of the private sector and academia in basic research, applied research, data transfers, and the development of automation, artificial intelligence, and associated algorithms. Such report shall include:

1. Identification of any additional authorities that the Director of NGA would require to provide the private sector and academia with access to relevant data on a need-driven and limited basis, consistent with applicable laws and procedures relating to the protection of sources, methods, privacy and civil liberties; and

2. Market research to assess the commercial and academic interest in such data and determine likely private-sector entities and institutions of higher education interested in public-private partnerships relating to such data.

NRO Contracting Restrictions.

The Committees continue to be very concerned that NRO imposes unnecessary contractual restrictions that prohibits or discourages a contractor from contacting or meeting with a congressional intelligence committee or intelligence committee Member offices. Therefore, the Committees direct NRO to remove all restrictions that impacts contractors from

contacting or meeting with the congressional intelligence committees or member offices in all current and future contracts to include pre-coordination with executive branch agencies.

Enhancing Automation at the National Geospatial-Intelligence Agency.

The Committees strongly support efforts to leverage commercial advances in automation of imagery such as electro-optical, infrared, Wide Area Motion Imagery (WAMI), Full Motion Video (FMV), and Synthetic Aperture Radar (SAR) products to reduce manual processing and improve information flow to users. However, the Committees are concerned that NGA does not dedicate adequate resources to integrate new automation techniques, which have resulted in years of research into the issue, but limited operation gains during day-to-day imagery processing.

Therefore, the Committees direct NGA, within 90 days of enactment of this Act, to brief the congressional intelligence and defense committees on an updated plan to reduce manual processing of imagery such as electro-optical, infrared, WAMI, FMV, and SAR to improve information flow to users. The briefing shall also address:

1. NGA's strategy to leverage commercial advances;

2. The various GEOINT automated exploitation development programs across the National System for Geospatial-Intelligence, and the associated funding and specific purpose of said programs;

3. Any similar efforts by government entities outside the National System for Geospatial-Intelligence of which NGA is aware; and

4. Which of these efforts may be duplicative.

Redundant Organic Software Development.

The Committees are concerned that NGA is developing software solutions that are otherwise available for purchase on the commercial market. This practice often increases the time it takes to deliver new capabilities to the warfighter; increases the overall cost of the solution through expensive operational and maintenance costs; and undermines the U.S. software industrial base.

Therefore, the Committees direct NGA, within 60 days of enactment of this Act, to brief the Committees, to identify all NGA developed software programs and explain why they are being developed organically instead of leveraging commercially available products.

Critical Skills Recruiting for Automation.

Although cutting edge sensors have provided the IC and Department of Defense with exquisite imagery, full motion video (FMV), and wide area motion imagery (WAMI), intelligence analysts are unable to keep pace with the volume of data being generated. This demands a transformation in the way the intelligence enterprise processes, organizes, and presents data. For that reason, the

[[Page H10241]]

Committees fully support the NGA's efforts to attract, recruit, and retain a highly competent workforce that can acquire and integrate new data automation tools.

Therefore, the Committees direct NGA, within 60 days of enactment of this Act, to brief the congressional intelligence and defense committees on NGA's efforts to recruit critical skills such as mathematicians, data scientists, and software engineers that possess critical skills needed to support NGA's objectives in automation.

Common Sensitive Compartmented Information Facility.

The Committees have become aware of several major impediments to companies performing work for agencies and organizations like the NRO. For example, businesses without ownership of a SCIF find it very difficult to perform

classified work. Additionally, these small businesses are challenged with basic obstacles such as becoming aware of classified work opportunities because it is difficult to obtain access to the IC's and DoD's classified marketplaces such as the Acquisition Resource Center (ARC). Construction and accreditation of SCIF spaces is cost-prohibitive for small business and non-traditional government contractors. Additionally, construction timeline often exceeds the period of performance of a contract.

A modern trend for innovative and non-traditional government contractors is the increased use of co-working space environments. Additionally, public and private entities are partnering to create emerging regional innovation hubs to help identify technology solutions and products in the private sector that can be utilized by the IC and DoD. These innovation hubs currently produce an agile, neutral, but largely unclassified development environment.

Therefore, the Committees direct the DNI, within 90 days of enactment of this Act, to brief the congressional intelligence committees on the following:

1. Steps necessary to establish new `Common SCIFs' in areas of high demand;

2. What approaches allow for SCIF spaces to be certified and accredited outside of a traditional contractual arrangement;

3. Analysis of the advantages and disadvantages of issuing Department of Defense Contract Security Specification (DD Form 254s) to ``Facilities,'' as opposed to ``Contracts'';

4. Options for classified co-use and shared workspace environments such as: innovation, incubation, catalyst, and accelerator environments;

5. Pros and cons for public, private, government, or combination owned classified neutral facilities; and

6. Any other opportunities to support those without ownership of a SCIF effective access to a neutral SCIF.

Improving Use of the Unclassified Marketplaces.

Another area where the Committees have become aware of major impediments for companies to perform work for agencies and organizations like the NRO are unclassified marketplaces such as the Acquisition Resource Center (ARC). Instead of posting data to unclassified marketplaces, unclassified NRO postings often refer to the classified side for critical yet unclassified information. If the NRO is serious about embracing commercial innovation, unclassified marketplace postings should remain on the unclassified side.

Therefore, the Committees direct NRO, within 90 days of enactment of this Act, to brief the Committees on options for improving the unclassified marketplace process.

Satellite Servicing.

No later than one year after the date of the enactment of this Act, the DNI, in consultation with the Secretary of Defense, shall jointly provide the to the congressional intelligence and defense committees a briefing detailing the costs, risks, and operational benefits of leveraging commercial satellite servicing capabilities for national security satellite systems. The briefing shall include the following:

1. A prioritized list, with a rationale, of operational and planned assets of the Intelligence Community that could be enhanced by satellite servicing missions;

2. The costs, risks, and benefits of integrating satellite servicing capabilities as part of operational resilience; and

3. Potential strategies that could allow future national security space systems to leverage commercial in-orbit servicing capabilities where appropriate and feasible.

Commercial RF Mapping and SAR.

U.S. commercial companies are now offering space-based geolocation and geospatial intelligence (GEOINT) analysis of radio frequency (RF) emitters as well as synthetic aperture

radar (SAR) products. These companies can identify, locate, and analyze previously undetected activity, providing new insights for U.S. national security and defense. The IC currently has contracts that leverage commercial electro-optical satellites, however it does not have a program in place to take full advantage of these emerging commercial space-based RF GEOINT and SAR capabilities.

Therefore, the Committees direct the NRO and NGA to brief the Committees on how it will leverage these commercial companies in Fiscal Year 2020 and beyond, to include funding for, as well as testing and evaluation efforts.

Commercial Remote Sensing.

The Committees support efforts to establish a light-touch regulatory structure that enables the rapidly evolving commercial space-based imagery, RF sensing, and radar industry markets to promote U.S. leadership in these areas. However, the Committees also support the needs of the U.S. Government to protect both IC and DoD personnel and assets. The Committees believe there can be a balance that supports both national security interests and the promotion of U.S. innovation and leadership.

Therefore, the Committees direct the DNI, in consultation with the Secretary of Defense, to brief the Committees within 60 days of the date of enactment of the Act, on efforts that help address this balance and which streamline the IC and DoD involvement in the rapidly evolving U.S. commercial space-based imagery, RF sensing, and radar industries.

Deception Detection Techniques.

The U.S. Government does not have sufficient security screening capabilities available to determine deception in individuals that intend to harm the United States. The polygraph has been an effective investigative tool to detect deception, but the cost and time required to administer a polygraph examination is a major cause for security clearance backlogs, and often limits the frequency of periodic examinations to every 5-7 years. Entities within DoD and the IC including DIA, Special Operations Command, NGA, Defense Counterintelligence and Security Agency, U.S. Air Force and others have expressed a desire to begin piloting new systems such as ocular deception detection systems. However, progress is being hindered by DoD Directive 5210.91 and ODNI Security Agent Directive 2, which direct some oversight of new deception detection technologies to the DoD National Center of Credibility Assessment (NCCA), which does not have sufficient budget or other resources to expeditiously evaluate non-polygraph technologies.

Therefore, the Committees direct the DNI in coordination with the DoD to provide the congressional intelligence and defense committees with a briefing on what steps they are taking to ensure pilot programs are established to evaluate these new technologies to help reduce our backlog, improve efficiency, and reduce overall cost. Pilot programs shall evaluate current and emerging technologies to efficiently and rapidly verify the accuracy and truthfulness of statements of candidates for employment within the DoD/IC, including for interim security clearances, for periodic screening of cleared DoD/IC personnel, to screen foreign national collaborators and contractors overseas to prevent ``Green-on-Blue'' attacks, for immigration screening and for other purposes.

List of Foreign Entities That Pose a Threat to Critical Technologies.

The Committees direct the DNI, in consultation with the Secretary of Defense, to identify, compose, and maintain a list of foreign entities, including governments, corporations, nonprofit and for-profit organizations, and any subsidiary or affiliate of such an entity, that the Director determines pose a threat of espionage with respect to critical technologies or research projects, including

research conducted at institutions of higher education.

Maintenance of this list will be critical to ensuring the security of the most sensitive projects relating to U.S. national security, such as defense and intelligence-related research projects. The initial list shall be available to the head of each qualified agency funding applicable projects and will include the following entities already identified as threatening: Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, and Kaspersky Lab. The DNI and the Secretary of Defense, or a delegate from each agency, shall brief the findings to the congressional intelligence and defense committees no later than 180 days after the enactment of the Act.

Protection of National Security Research.

The Committees believe that institutes of higher learning, laboratories, and other entities and organizations play critical roles in advancing national security within the U.S. science and technology ecosystem that is charged with delivering the best capabilities to the warfighter in the near, mid, and long-term. The Committees understand that near-peer competitors such as China and Russia attempt to exploit and benefit from the open and collaborative global research environment created by the Reagan Administration's National Security Decision Directive 189 on the National Policy on the transfer of Scientific, Technical and Engineering Information. This directive established that the products of ``fundamental research''--defined as ``basic and applied research in science and engineering, the results of which ordinarily are published and shared''--should remain unrestricted.

The Committees are also aware that academia is not always kept apprised by the interagency of a complete picture of potential activities and threats in the research community, such as improper technology transfer, intellectual property theft, and cyber-attacks directly attributed to nation-state governments. Elsewhere in this bill and report, the Committees include measures to promote increased information sharing across the interagency and with academia.

Therefore, the Committees direct the Secretary of Defense to provide the congressional intelligence and defense committees,

[[Page H10242]]

within 90 days of enactment of the Act, a report listing Chinese and Russian academic institutions that have a history of improper technology transfer, intellectual property theft, cyber espionage, or operate under the direction of their respective armed forces or intelligence agencies. The report should be in unclassified form, but may contain a classified annex.

Investments in Scientific and Technological Intelligence.

The Committees remain interested in the continued efforts of the DoD to improve scientific and technological intelligence (S&TI) capabilities and tradecraft across the Defense Intelligence Enterprise (DIE). The Committees recognize S&TI is critical to strategic competition with near-peer competitors by ensuring comprehensive understanding of adversary capabilities and ability to inform development of joint force fifth-generation advanced weapons systems and other emerging technologies.

Therefore, the Committees direct the USD(I) in collaboration with the Director of the DIA, to provide a briefing to the Committees and the congressional defense committees within 75 days of enactment of the Act, on the alignment of current and planned DIE S&TI investments and activities to DoD operational and strategic requirements.

The briefing shall also include information on how the DoD

will continue the maturation of S&TI capabilities and tradecraft across the DIE.

Intelligence Support to Defense Operations in the Information Environment.

The Committees support DoD efforts to improve capabilities and tradecraft to operate in the information environment. The Committees are concerned about the Defense Intelligence Enterprise's (DIE) ability to provide the information operations community with all-source intelligence support, consistent with the support provided to operations in other domains.

Therefore, the Committees direct the USD(I), in coordination with the Joint Staff's Director for Intelligence and the DNI, to provide a briefing to the congressional intelligence and defense committees within 30 days of enactment of the Act, on intelligence support to information operations. The briefing should include standardized defense intelligence lexicon for intelligence preparation of the battlefield for information operations, efforts to develop a process to ensure the full scope of emerging defense information operations threat requirements are structured to be addressed through the entirety of DIE capabilities, and how the DIE perceives the future of defense operations in the information environment.

The briefing shall also include a description of how the IC, through the National Intelligence Priorities Framework, will account for a more dynamic use of defense intelligence capabilities to augment and enhance support to DoD operations in the information environment.

ROTC IC Recruitment Trial Program.

The Senior Reserve Officers' Training Corps (ROTC) program, with units or affiliates at approximately 1,600 U.S. colleges and universities, is DoD's largest commissioning source, providing approximately 6,500 new active duty officers to the military each year.

Officer candidates enrolled in ROTC programs must meet all graduation requirements of their academic institutions, enroll in military, naval, or aerospace education courses, and attend summer military training, making them ideal candidates for IC placement. Currently, ROTC cadets only have the option to utilize their training by joining one of the military services. The Committees believe the government can find cost savings and provide a wider range of opportunities to ROTC recruits by leveraging the ROTC's existing training program for the IC.

Therefore, the Committees direct the USD(I), in coordination with ODNI, to conduct a feasibility study on creating a pathway for ROTC recruits to find employment in the IC, on a reimbursable basis. The study should examine:

1. Pros and cons of instituting an ROTC IC recruitment pipeline;
2. Approximate reimbursement cost per recruit; and
3. Legislative requirements for program execution.

The Committees direct that the study results be submitted via report to the Committees and the congressional defense committees within 90 days of enactment of the Act.

Explosive Ordinance Disposal Intelligence.

The Committees are concerned that the expertise of Explosive Ordinance Disposal (EOD) personnel is not adequately accessible and therefore, not sufficiently utilized by the Defense Intelligence Enterprise and IC to provide the combatant commands with the required intelligence to identify, combat, and deter violent extremism and other asymmetric threats.

Explosive ordnance includes all munitions, improvised explosive devices, devices containing explosives, propellants, nuclear fission or fusion materials, biological, and chemical agents. The primary consumer of this information are military tactical explosive ordnance disposal units that

employ the data for threat identification and neutralization. However, the required analysis to determine appropriate render-safe capabilities requires operational and strategic intelligence to process and analyze the data, and data management processes to promulgate the resulting information. The Committees believe DoD should modernize the processes and procedures to more comprehensively track, manage, and coordinate the capability and capacity of EOD intelligence within the IC and the DIE to support all levels of render-safe capabilities.

Therefore, the Committees direct the USD(I), in coordination with the ODNI, to provide a briefing to the congressional intelligence and defense committees within 120 days of enactment of the Act on the capability and capacity of EOD intelligence expertise across the DIE and IC. The briefing shall include:

1. An assessment of the coordination and integration of defense and national intelligence capabilities against EOD intelligence requirements, to include a mitigation strategy to address any identified gaps or deficiencies, information-sharing challenges, or any other impediments to integration of EOD expertise across the defense and intelligence communities; and

2. An assessment of the technical skills needed to address EOD intelligence requirements, while identifying any gaps or deficiencies in current personnel hiring and training structures, and a long-term plan to develop proficiency of EOD intelligence expertise in the defense and intelligence communities.

Information-Sharing Arrangements with India, Japan, and the Republic of Korea.

International alliances and partnerships are critical to the pursuit and sustainment of the United States national security objectives, built upon foundations of shared values and intent. The Committees recognize the importance of the DoD sharing information with international allies and partners in support of the planning and execution of the National Defense Strategy, as allies and third-party international partners enhance strategic stability across the Department's purview while increasing effectiveness of operations. The Committees believe the mechanisms to share information across the ``Five Eyes'' alliance continue to mature through established exercises, exchange of personnel, and virtual data sharing, while that cooperation is potentially less robust with third-party partners.

The Committees support the roles and contributions of third-party partners such as India, Japan, and the Republic of Korea, and recognizes their ongoing contribution toward maintaining peace and stability in the Indo-Pacific region. The Committees are interested in understanding the policies and procedures governing the collaboration and information sharing with India, Japan, the Republic of Korea, and the ``Five Eyes'' allies, and whether opportunities exist to strengthen those arrangements.

Therefore, the Committees direct the Under Secretary of Defense for Intelligence (USD(I)), in coordination with the ODNI, to provide a briefing to the congressional intelligence and defense committees within 60 days of enactment of the Act, on the benefits, challenges, and risks of broadening the information-sharing mechanisms between India, Japan, the Republic of Korea, and the ``Five Eyes'' allies.

Transitioning the Function of Background Investigations to the Department of Defense.

Executive Order 13869 transitions the background investigation functions of the Federal Government from the Office of Personnel Management (OPM), National Background Investigations Bureau, to the DoD, Defense Counterintelligence and Security Agency. The Committees recognize the importance of ensuring timely and efficient

background investigations to overcome workforce staffing challenges of cleared individuals across the whole of government and private sector, and to vet personnel who come into contact with the Department's personnel, installations, and technology. The Committees are aware of the temporary establishment of the Personnel Vetting Transformation Office in the OUSD(I) to manage the transition of this activity from OPM to the Department and improve the processes and procedures related to vetting personnel for clearances across the whole of government and private sector.

However, the Committees are concerned about the potential risks to personnel management and mission such a transfer may present, and believes that appropriate protections of civil liberties and privacy must be prioritized throughout the transition, through the implementation of modern and efficient vetting measures. The Committees recognize the Department's leadership, through sharing best practices with ODNI, in reforming the vetting process using modern techniques such as continuous evaluation, and expects regular updates on the Department's progress in addressing the current background investigations backlog.

Therefore, the Committees direct the USD(I), in coordination with the Director of the Defense Counterintelligence and Security Agency, to provide a briefing to the congressional intelligence and defense committees within 90 days of enactment of the Act, on how the DoD will transfer the background investigation mission and establish an effective personnel vetting capability to provide for the security of the Department, while maintaining the civil liberties and privacy protections of personnel under consideration to receive a clearance.

Joint Intelligence Operations Center Staffing.

The Committees recognize the evolving operational and strategic priorities of the

[[Page H10243]]

DoD will impact Defense Intelligence Enterprise capabilities and resources. The Committees recognize the ongoing efforts by the USD(I) to comply with direction specified by the John. S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232) to reduce and prevent imbalances in priorities and mitigate against insufficient or misaligned resources within the Defense Intelligence Enterprise.

While the Committees support the efforts by the USD(I) to create efficiencies across the Defense Intelligence Enterprise organizations, to include the Service Intelligence Centers and combatant command Joint Operations Intelligence Centers, and enable those elements to plan and posture staffing requirements accordingly, the Committees are concerned that the shifts in current and future resourcing lack coherence to support the global mandate of the Department.

Therefore, the Committees direct the USD(I), in coordination with DIA, to provide a briefing to the congressional intelligence and defense committees within 90 days of enactment of the Act on how the OUSD(I) and DIA are managing resourcing requirements to the combatant command Joint Intelligence Operations Centers to meet current and future needs of the combatant commanders and DoD.

China's Biological Weapons Program.

The Committees remain interested in ensuring the Defense Intelligence Enterprise is providing timely, accurate, and effective intelligence to support information needs of the DoD, and are aware of a recent GAO report on long-range emerging threats facing the United States that highlighted potential pursuit by near-peer competitors of biological weapons using genetic engineering and synthetic biology.

Therefore, the Committees direct the USD(I), in

coordination with the Director of the DIA, to provide a briefing to the congressional intelligence and defense committees within 30 days of enactment of the Act with an assessment of China's current and projected biological weapons program, the risks presented to the joint force, and the mitigation strategies to protect U.S. military forces against said threats.

Machine-assisted Analytic Rapid Repository System Government Accountability Office Review.

The re-emergence of great power competition will stress DIA's ability to provide foundational military intelligence for the IC and warfighters. As such, the Committees are supportive of DIA's intent to replace the Modernized Integrated Database (MIDB) with the Machine-assisted Analytic Rapid Repository System (MARS).

However, the Committees are concerned that MARS's development and procurement will entail a complex and extensive transformation that will impact the DIA's delivery of foundational military intelligence.

Therefore, the Committees direct the GAO to provide a report to the congressional intelligence and defense committees within one year of enactment of the Act that describes:

1. The envisioned users and customer base and how they will use MARS;
2. An assessment of the transition plan from MIDB to MARS with input from current and historic MIDB users, as well as customers;
3. An assessment of the resources necessary to fully implement MARS, to include funding and personnel implications;
4. An assessment of DIA's acquisition strategy for MARS to include the use of any rapid acquisition or prototyping authorities; and
5. The challenges DIA has identified that it will face in transitioning from MIDB to MARS and whether its migration plans are sufficient for addressing these challenges.

The Committees expect DIA's full cooperation with the GAO study.

Update on the DIA Strategic Approach.

In September 2018, the Defense Intelligence Agency (DIA) adopted a Strategic Approach to enhance workforce development, improve foundational military intelligence data management, address perennial intelligence issues and realign roles and missions. Improvements in these issue areas will enhance the Agency's ability to support both the National Security Strategy and National Defense Strategy.

The Committees support the DIA's initiative to improve those structures it assesses are critical to providing warfighters the information needed to prevent and, if necessary, decisively win wars, such as intelligence on foreign militaries' capabilities.

Therefore, the Committees direct DIA to provide quarterly briefings, beginning 45 days after enactment of the Act, to the congressional intelligence and defense committees on its efforts to enhance workforce development, improve foundational military intelligence data management, address perennial intelligence issues, and realign roles and missions.

Report on Chinese Efforts Targeting Democratic Elections and U.S. Alliances and Partnerships and Strategy to Counter Chinese Election Interference.

The Committees direct the DNI, in coordination with the Secretary of Defense, the Secretary of State, and the Secretary of Homeland Security, to provide a report to the Committees, the congressional defense committees, the House Committee on Foreign Affairs, the Senate Committee on Foreign Relations, the House Committee on Homeland Security, and the Senate Committee on Homeland Security and Governmental

Affairs on the Chinese government's influence operations and campaigns targeting democratic elections.

The report shall be divided into two sections, which respectively address influence operations and campaigns targeting: (1) recent and upcoming elections in the United States (dating back to January 1, 2017), and (2) military alliances and partnerships of which the United States is a member. The report should also include a strategy to counter these activities. The Committees further direct the Secretary of Defense to provide an interim report within 30 days of enactment of the Act, and a final report within a year of enactment of the Act.

The report shall be unclassified and appropriate for release to the public but may include a classified annex. At a minimum, the report should include:

1. An assessment of China's objectives in influence operations and campaigns targeting democratic elections and military alliances and partnerships of which the United States is a member, and how such objectives relate to the China's broader strategic aims;

2. The United States' strategy and capabilities for detecting, deterring, countering, and disrupting such Chinese influence operations (including recommended authorities and activities) and campaigns and a discussion of the DoD's and the IC's respective roles in the strategy;

3. A comprehensive list of specific Chinese state and non-state entities involved in supporting such Chinese influence operations and campaigns and the role of each entity in supporting them;

4. An identification of the tactics, techniques, and procedures used in previous Chinese influence operations and campaigns;

5. A comprehensive identification of countries with democratic election systems that have been targeted by Chinese influence operations and campaigns since January 1, 2017;

6. An assessment of the impact of previous Chinese influence operations and campaigns targeting democratic elections and military alliances and partnerships of which the United States is a member, including the views of senior Chinese officials about their effectiveness in achieving Chinese objectives;

7. An identification of countries with democratic elections systems that may be targeted in future Chinese influence operations and campaigns and an assessment of the likelihood that each such country will be targeted;

8. An identification of all U.S. military alliances and partnerships that have been targeted by Chinese influence operations and campaigns since January 1, 2017;

9. An identification of all U.S. military alliances and partnerships that may be targeted in future Chinese influence operations and campaigns and an assessment of the likelihood that each such country will be targeted; and

10. An identification of tactics, techniques, and procedures likely to be used in future Chinese influence operations and campaigns targeting democratic elections and military alliances and partnerships of which the United States is a member.

Report on Russian Efforts Targeting Democratic Elections and U.S. Alliances and Partnerships and Strategy to Counter Russian Election Interference.

The Committees direct the DNI, in coordination with the Secretary of Defense, the Secretary of State, and the Secretary of Homeland Security, to provide a report to the Committees, the congressional defense committees, the House Committee on Foreign Affairs, the Senate Committee on Foreign Relations, the House Committee on Homeland Security, and the Senate Committee on Homeland Security and Governmental Affairs on Russia's influence operations and campaigns

targeting democratic elections.

The report shall be divided into two sections, which respectively address influence operations and campaigns targeting: (1) recent and upcoming elections in the United States (dating back to January 1, 2017) and (2) military alliances and partnerships of which the United States is a member. The report should also include a strategy to counter these activities. The Committees further direct the Secretary of Defense to provide an interim report within 30 days of enactment of the Act, and a final report within a year of enactment of the Act.

The report shall be unclassified and appropriate for release to the public but may include a classified annex. At a minimum, the report should include:

1. An assessment of Russia's objectives in influence operations and campaigns targeting democratic elections and military alliances and partnerships of which the United States is a member, and how such objectives relate to Russia's broader strategic aims;

2. The United States strategy and capabilities for detecting, deterring, countering, and disrupting such Russian influence operations (including recommended authorities and activities) and campaigns and a discussion of the DoD's and IC's respective roles in the strategy;

3. A comprehensive list of specific Russian state and non-state entities involved in supporting such Russian influence operations and campaigns and the role of each entity in supporting them;

4. An identification of the tactics, techniques, and procedures used in previous Russian influence operations and campaigns;

[[Page H10244]]

5. A comprehensive identification of countries with democratic election systems that have been targeted by Russian influence operations and campaigns since January 1, 2017;

6. An assessment of the impact of previous Russian influence operations and campaigns targeting democratic elections and military alliances and partnerships of which the United States is a member, including the views of senior Russian officials about their effectiveness in achieving Russian objectives;

7. An identification of countries with democratic elections systems that may be targeted in future Russian influence operations and campaigns and an assessment of the likelihood that each such country will be targeted;

8. An identification of all U.S. military alliances and partnerships that have been targeted by Russian influence operations and campaigns since January 1, 2017;

9. An identification of all U.S. military alliances and partnerships that may be targeted in future Russian influence operations and campaigns and an assessment of the likelihood that each such country will be targeted; and

10. An identification of tactics, techniques, and procedures likely to be used in future Russian influence operations and campaigns targeting democratic elections and military alliances and partnerships of which the United States is a member.

UNCLASSIFIED DIRECTION RELATED TO SUBDIVISION 2

Management of Intelligence Community Workforce.

The Committees repeat direction from the Intelligence Authorization Act for Fiscal Year 2017 that IC elements

should build, develop, and maintain a workforce appropriately balanced among its civilian, military, and contractor workforce sectors to meet the missions assigned to it in law and by the president. Starting in Fiscal Year 2019, the Committees no longer authorize position ceiling levels in the annual Schedule of Authorizations.

The Committees look forward to working with the ODNI as it develops an implementation strategy and sets standards for workforce cost analysis tools.

Countering Russian Propaganda.

The Committees support the IC's role in countering Russian propaganda and other active measures. The Committees are committed to providing the appropriate legal authorities, financial resources, and personnel necessary to address these hostile acts. The Committees specifically find that language capabilities are important to the IC's efforts in countering Russia's hostile acts. The Committees encourage the IC to commit considerable resources in the future to bolstering officers' existing Russian language skills, recruiting Russian language speakers, and training officers in Russian, in particular key technical language skills. This effort will require strategic planning both in recruiting and rotating officers through language training. The Committees expect to see these priorities reflected in future IC budget requests.

Protection of the Supply Chain in Intelligence Community Acquisition Decisions.

The Committees continue to have significant concerns about risks to the supply chain in IC acquisitions. The Committees encourage the Supply Chain and Counterintelligence Risk Management Task Force recommendations to support continued efforts to develop an open, interoperable information security-sharing platform to enable real-time cross-domain sharing for the IC to effectively share and analyze information on supply chain, cybersecurity vulnerabilities, and counterintelligence risks.

The report to accompany the Intelligence Authorization Act for Fiscal Year 2017 directed the DNI to review and consider changes to Intelligence Community Directive (ICD) 801 (``Acquisition'') to reflect the issuance of ICD 731 (``Supply Chain Risk Management'') in 2013 and the issues associated with cybersecurity. It specifically recommended the review examine whether to: expand risk management criteria in the acquisition process to include cyber and supply chain threats; require counterintelligence and security assessments as part of the acquisition and procurement process; propose and adopt new education requirements for acquisition professionals on cyber and supply chain threats; and factor in the cost of cyber and supply chain security. This review was due in November 2017, with a report on the process for updating ICD 801 in December 2017. The report was completed on June 18, 2018.

As a follow-on to this review, the Committees direct DNI to address three other considerations: changes in the Federal Acquisition Regulation that may be necessary; how changes should apply to all acquisition programs; and how security risks must be addressed across development, procurement, and operational phases of acquisition. The Committees further direct the DNI to submit a plan to implement necessary changes within 60 days of completion of this review.

National Geospatial-Intelligence Agency use of VERA and VSIP Authorities.

The Committees encourage the use by the National Geospatial-Intelligence Agency (NGA) of Voluntary Early Retirement Authority (VERA) and Voluntary Separation Incentive Program (VSIP) offers to meet future goals of building a workforce more attuned to automation of data production, automation of analytic processes, and establishment of development and operations (DevOps) software development processes.

Therefore, the Committees direct the NGA to report to the Committees, within 120 days of enactment of the Act, on its use to date of VERA and VSIP incentives, to include how they have been used to develop an acquisition cadre skilled in ``DevOps'' software development processes, as well as a plan for further use of these incentives. The report should specify metrics for retooling its workforce, including how it measures data literacy and computational skills in potential hires, and an accounting of the numbers of new hires who have met these higher standards.

Report on Engagement of National Reconnaissance Office with University Community.

The Committees recognize that the survivability and resiliency of United States satellites is critically important to the United States intelligence and defense communities. While the NRO engages with the university community in support of basic research and developing an education workforce pipeline to help advance new technologies and produce skilled professionals, it can do more in this regard to focus on space survivability.

Therefore, the Committees direct the NRO to report, within 120 days of enactment of the Act, on NRO's current efforts and future strategies to engage with university partners that are strategically located, host secure information facilities, and offer a strong engineering curriculum, with a particular focus on space survivability and resiliency. This report should provide a summary of NRO's current and planned university engagement programs, levels of funding, and program research and workforce objectives and metrics. The report should also include an assessment of the strategic utility of chartering a University Affiliated Research Center in this domain.

National Geospatial-Intelligence Agency Facilities.

Consistent with section 2401 of the National Defense Authorization Act for Fiscal Year 2019, the Committees authorize the President's request for $447.8 million in Fiscal Year 2019 for phase two construction activities of the Next National Geospatial-Intelligence Agency West (N2W) facility in St. Louis, Missouri. The Committees are pleased that the second phase of this $837.2 million project was included in the Fiscal Year 2019 President's budget.

Clarification of Oversight Responsibilities.

The Committees reinforce the requirement for all IC agencies funded by the NIP to respond in a full, complete, and timely manner to any request for information made by a member of the congressional intelligence committees. In addition, the Committees direct the DNI to issue guidelines, within 90 days of enactment of the Act, to ensure that the intent of section 501 of the National Security Act of 1947 (50 U.S.C. 3091) is carried out.

Clarification on Cooperation with Investigation on Russian Influence in the 2016 Election.

The Committees continue to reinforce the obligation for all IC agencies to cooperate in a full, complete, and timely manner with the Committees' ongoing investigations into Russian meddling in the 2016 Presidential election and cooperation with the declassification process.

Supervisory Feedback as Part of Continuous Vetting Program.

The Committees direct the DNI to review the results of ongoing pilot programs regarding the use of supervisory feedback as part of the periodic reinvestigation and continuous vetting process and report, within 180 days of enactment of the Act, on the establishment of a policy for its use across the IC.

National Security Threats to Critical Infrastructure.

The Committees are aware of significant threats to our critical infrastructure and industrial control systems posed by foreign adversaries. The sensitive nature of the information related to these threats make the role of the IC

of vital importance to United States defensive efforts. The Committees have grave concerns that current IC resources dedicated to analyzing and countering these threats are neither sufficient nor closely coordinated. The Committees include provisions within this legislation to address these concerns.

Framework for Cybersecurity and Intelligence Collection Doctrine.

The Committees direct the ODNI, in coordination with appropriate IC elements, to develop an analytic framework that could support the eventual creation and execution of a Government-wide cybersecurity and intelligence collection doctrine. The ODNI shall provide this framework, which may contain a classified annex, to the congressional intelligence committees, within 180 days of enactment of the Act.

This framework shall include:

1. An assessment of the current and medium-term cyber threats to the protection of the United States' national security systems and critical infrastructure;

2. IC definitions of key cybersecurity concepts, to include cyberespionage, cyber theft, cyber acts of aggression, and cyber deterrence;

3. Intelligence collection requirements to ensure identification of cyber actors targeting U.S. national security interests, and

[[Page H10245]]

to inform policy responses to cyber-attacks and computer network operations directed against the United States;

4. The IC's methodology for assessing the impacts of cyber-attacks and computer network operations incidents directed against the United States, taking into account differing levels of severity of incidents;

5. Capabilities that the IC could employ in response to cyber-attacks and computer network operations incidents, taking into account differing levels of severity of incidents;

6. A policy and architecture for sharing cybersecurity-related intelligence with government, private sector, and international partners, including existing statutory and other authorities which may be exercised in pursuit of that goal; and

7. Any necessary changes in IC authorities, governance, technology, resources, and policy to provide more capable and agile cybersecurity.

Inspector General of the Intelligence Community Role and Responsibilities.

The position of the Inspector General of the Intelligence Community (IC IG) was codified by the Intelligence Authorization Act for Fiscal Year 2010. Among other things, the IC IG's statutory purposes include ``conduct[ing] independent reviews investigations, inspections, audits, and reviews on programs and activities within the responsibility and authority of the Director of National Intelligence;'' keeping the Committees fully and currently informed of significant problems and deficiencies; and leading efforts of inspectors general within the IC.

The Committees have included provisions intended to strengthen the IC IG's role. The Committees will insist on full cooperation from the Director, ODNI offices, as well as those of inspectors general across the IC, in ensuring that the IC IG's prescribed functions are carried out to the fullest extent possible. The Committees further reiterate Congress's intent that the IC IG is obligated to identify and inform the Committees of significant problems and deficiencies ``relating to'' all intelligence programs and activities.

The Committees also remain seriously concerned about the

undermining of protections and rights afforded to whistleblowers within the IC and the level of insight congressional committees have into the handling of lawful disclosures. Without exception, the Committees must be made aware of lawful disclosures made to any inspector general within the IC, consistent with provisions added to Title 50 by sections 5331-5335 of Subdivision 1 of the Act; and of all lawful disclosures made pursuant to ICWPA and Title 50 procedures, which Intelligence Community personnel intend to be submitted to the Committees. The Committees underscore in the strongest terms that all elements of the IC are obligated, as a categorical matter, to comply with both existing law as well as direction provided elsewhere in the Act and this Explanation, with respect to inspector general and whistleblower matters.

Space Launch Facilities.

The Committees continue to believe it is critical to preserve a variety of launch range capabilities to support national security space missions, and encourage planned launches such as the U.S. Air Force Orbital/Sub-Orbital Program (OSP)-3 NRO-111 mission, to be launched in 2019 on a Minotaur 1 from the Mid-Atlantic Regional Spaceport at Wallops Flight Facility. In the Intelligence Authorization Act for Fiscal Year 2017, the Committees directed a brief from the ODNI, in consultation with the DoD and the U.S. Air Force, on their plans to utilize state-owned and operated spaceports, which leverage non-federal public and private investments to bolster United States launch capabilities and provide access to mid-to-low or polar-to-high inclination orbits for national security missions.

The Committees direct that the ODNI supplement this brief with how state investments in these spaceports may support infrastructure improvements, such as payload integration and launch capabilities, for national security launches.

Acquisition Research Center Postings.

The Committees support a flexible NRO acquisition process that allows the NRO to choose the most appropriate contracting mechanism, whether for small research and development efforts or large acquisitions. The NRO's Acquisition Research Center (ARC), a classified contracting and solicitation marketplace that NRO and other agencies use, enables this flexible acquisition process for classified efforts.

The Committees direct the NRO, within 60 days of enactment of the Act, to brief the congressional intelligence and defense committees on options for modifying ARC posting procedures to ensure fair and open competition. Those options should include ensuring that unclassified NRO solicitations are posted on the unclassified FEDBIZOPS website, and identifying ways to better utilize the ARC to encourage contract opportunities for a more diverse industrial base that includes smaller and non-traditional companies.

Ensuring Strong Strategic Analytical Tradecraft.

The Department of Homeland Security's (DHS's) Office of Intelligence and Analysis (I&A) has taken steps to improve the quality of its analysis, to identify its core customers, and to tailor its production to meet customer needs. The Committees concur with I&A's implementation of analytic standards and review mechanisms that have improved the tradecraft behind I&A products. The bedrock of these efforts has been the development of a yearly program of analysis (POA) and key intelligence questions, which are essential tools for providing a roadmap and boundaries for the office's production efforts.

Therefore, the Committees direct the Office of I&A to continue to prioritize, develop and hone its strategic intelligence capabilities and production, including the annual development of a POA. Within 90 days of enactment of the Act, and on an annual basis thereafter for two years, I&A

shall brief the congressional intelligence committees on the development and execution of its POA. These briefings should provide an overview of the POA, how customer needs have been incorporated into the POA, and an update on execution against the POA.

Cyber/Counterintelligence Analysis.

DHS's Office of I&A's Counterintelligence Mission Center analysis focuses on counterintelligence threats posed by foreign technology companies and fills a gap in IC intelligence production. Advanced technologies are increasingly ubiquitous and necessary to the function of modern society. Consequently, the scope of the threats from countries intent on using these technologies as a vector for collecting intelligence from within the United States will continue to expand. The Office of I&A is positioned to conduct a niche analysis critical to national security that combines foreign intelligence with domestic threat information.

The Committees strongly support I&A's Counterintelligence Mission Center's continued focus on these topics and the increased resources dedicated to this analysis in Fiscal Year 2019. Therefore, the Committees direct the I&A, in coordination with ODNI, to provide an update within 90 days of enactment of the Act on its recent analytic production related to counterintelligence threats posed by foreign technology companies, including a review of the countries and companies that present the greatest risks in this regard.

Intelligence Support to the Export Control Process.

The Committees have significant concerns that China poses a growing threat to United States national security, due in part to its relentless efforts to acquire United States technology. China purposely blurs the distinction between its military and civilian activities through its policy of ``military-civilian fusion,'' which compounds the risks of diversion of United States technology to the Chinese military.

The Committees conclude that the United States Government currently lacks a comprehensive policy and the tools needed to address this problem. China exploits weaknesses in existing U.S. mechanisms aimed at preventing dangerous technology transfers, including the U.S. export control system, which is run by the U.S. Department of Commerce's Bureau of Industry and Security (BIS). The Committees have specific concerns about the lack of adequate and effective IC support to BIS's export license application review process and believe more robust IC support could have prevented many of the ill-advised technology transfers that have occurred in recent years.

Therefore, the Committees directs the DNI to submit a plan, within 120 days of enactment of the Act, to describe how the IC will provide BIS with, at a minimum, basic but timely analysis of any threat to U.S. national security posed by any proposed export, re-export, or transfer of export-controlled technology. The plan shall include detailed information on the appropriate organizational structure, including how many IC personnel would be required, where they would be located (including whether they would be embedded at BIS to coordinate IC support), and the amounts of necessary funding. In formulating the plan, the DNI should study the ``National Security Threat Assessment'' process that the National Intelligence Council uses to inform the actions of the Committee on Foreign Investment in the United States. The DNI shall submit the plan to the congressional intelligence committees in classified form.

Social Media.

The Committees encourage the IC, notably the Federal Bureau of Investigation (FBI), to both continue and enhance its efforts to assist in detecting, understanding, and warning about foreign influence operations using social media tools

to target the United States. Additionally, within the scope of the IC's authorities, and with all necessary protections for U.S. person information, the Committees encourage the IC to augment and prioritize these ongoing efforts.

Trade-Based Money Laundering.

Threats to our national security posed by trade-based money laundering are concerning. Therefore, the Committees direct the DNI, within 90 days of enactment of the Act, to submit a report to the congressional intelligence committees on these threats, including an assessment of the severity of the threats posed to the United States' national security by trade-based money laundering conducted inside and outside the United States; an assessment of the scope of the financial threats to the U.S. economy and financial systems posed by trade-based money laundering; a description of how terrorist financing and drug trafficking organizations are advancing their illicit activities through

[[Page H10246]]

the use of licit trade channels; an assessment of the adequacy of the systems and tools available to the Federal Government for combating trade-based money laundering; and a description and assessment of the current structure and coordination between Federal agencies, as well as with foreign governments, to combat trade-based money laundering. The report shall be submitted in classified form with an unclassified summary to be made available to the public.

Expansions of Security Protective Service Jurisdiction of the Central Intelligence Agency.

The Committees direct the CIA, in connection with the expansion of its security protective service jurisdiction as set forth in section 6413 of Subdivision 2 of the Act, to engage with Virginia state and local law enforcement authorities to ensure that a memorandum of understanding, akin to those in place at other agencies setting forth the appropriate allocation of duties and responsibilities, is in effect.

Unauthorized Disclosures of Classified Information.

The Committees are concerned by the recent widespread media reports that purport to contain unauthorized disclosures of classified information. Protecting the nation's secrets from unauthorized disclosure is essential to safeguarding our nation's intelligence sources and methods. An unlawful disclosure of classified information can destroy sensitive collection capabilities and endanger American lives, including those individuals who take great personal risks to assist the United States in collecting vital foreign intelligence.

Federal law prohibits the unauthorized disclosure of classified information, but enforcement is often lacking or inconsistent. Accordingly, the Committees desire to better understand the number of potential unauthorized disclosures discovered and investigated on a routine basis. Moreover, the Committees have little visibility into the number of investigations initiated by each IC agency or the number of criminal referrals to the Department of Justice. Accordingly, section 6718 of Subdivision 2 of the Act requires all IC agencies to provide the congressional intelligence committees with a semi-annual report of the number of investigations of unauthorized disclosures to journalists or media organizations, including subsequent referrals made to the United States Attorney General.

Additionally, the Committees wish to better understand the role of IGs within elements of the IC, with respect to unauthorized disclosures of classified information at those elements.

Therefore, the Committees direct the IC IG, within 180 days of enactment of the Act, to provide the congressional

intelligence committees with a report regarding the role of IGs with respect to investigating unauthorized disclosures. The report shall address: the roles of IC elements' security personnel and law enforcement regarding unauthorized disclosures; the current role of IGs within IC elements regarding such disclosures; what, if any, specific actions could be taken by such IGs to increase their involvement in the investigation of such matters; any laws, rules or procedures that currently prevent IGs from increasing their involvement; and the benefits and drawbacks of increased IG involvement, to include potential impacts to IG's roles and missions.

Presidential Policy Guidance.

The Presidential Policy Guidance (PPG) dated May 22, 2013, and entitled ``Procedures for Approving Direct Action Against Terrorist Targets Located Outside the United States and Areas of Active Hostilities'' provides for the participation by elements of the IC in reviews of certain proposed counterterrorism operations. The Committees expect to remain fully and currently informed about the status of the PPG and its implementation.

Therefore, the Committees direct ODNI, within five days of any change to the PPG, or to any successor policy guidance, to submit to the congressional intelligence committees a written notification thereof, that shall include a summary of the change and the specific legal and policy justifications for the change.

Centers for Academic Excellence.

The Committees commend the commitment demonstrated by the program managers of the IC's Centers for Academic Excellence (IC-CAE), IC agencies that sponsored CAE interns, and all other personnel who contributed to the inaugural edition of the CAE Internship Program in summer 2017.

The Committees expect the IC-CAE Program to build on this foundation by showing measurable, swift progress, and ultimately fulfilling Congress's intent that the Program serve as a pipeline of the next generation of IC professionals.

Therefore, the Committees direct that the IC take all viable action to expand the IC-CAE Program by increasing, to the fullest extent possible:

1. The number and racial and gender diversity of IC-CAE interns;

2. The number of IC-CAE academic institutions and their qualified internship candidates participating in the IC-CAE Program; and

3. The number of IC elements that sponsor IC-CAE interns.

Report on Violent Extremist Groups.

Violent extremist groups like ISIS continue to exploit the Internet for nefarious purposes: to inspire lone wolves; to spread propaganda; to recruit foreign fighters; and to plan and publicize atrocities. As a former Director of the National Counterterrorism Center (NCTC) has stated publicly:

[W]e need to counter our adversaries' successful use of social media platforms to advance their propaganda goals, raise funds, recruit, coordinate travel and attack plans, and facilitate operations. . . . Our future work must focus on denying our adversaries the capability to spread their messages to at-risk populations that they can reach through the use of these platforms.

Section 403 of the Intelligence Authorization Act for Fiscal Year 2017 required the DNI, consistent with the protection of sources and methods, to assist public and private sector entities in recognizing online violent extremist content--specifically, by making publicly available a list of insignias and logos associated with foreign extremist groups designated by the Secretary of State. The Committees believe the IC can take additional steps.

Therefore, the Committees direct the Director of NCTC, in

coordination with other appropriate officials designated by the DNI, within 180 days of enactment of the Act, to brief the congressional intelligence committees on options for a pilot program to develop and continually update best practices for private technology companies to quickly recognize and lawfully take down violent extremist content online. Such briefing shall address:

1. The feasibility, risks, costs, and benefits of such a program;
2. The U.S. Government agencies and private sector entities that would participate; and
3. Any additional authorities that would be required by the program's establishment.

South China Sea.

The South China Sea is an area of great geostrategic importance to the United States and its allies. However, China's controversial territorial claims and other actions stand to undercut international norms and erode the region's stability. It is thus imperative the United States uphold respect for international law in the South China Sea. Fulfilling that objective in turn will require an optimal intelligence collection posture.

Therefore, the direct the DoD, in coordination with DNI, within 30 days of enactment of the Act, to brief the congressional intelligence and defense committees on known intelligence collection gaps, if any, with respect to adversary operations and aims in the South China Sea. The briefing shall identify the gaps and whether those gaps are driven by lack of access, lack of necessary collection capabilities or legal or policy authorities, or by other factors. The briefing shall also identify IC judgments that assess which intelligence disciplines would be best-suited to answer the existing gaps, and current plans to address the gaps over the Future Years Defense Program.

Policy on Minimum Insider Threat Standards.

Executive Order 13587 and the National Insider Threat Task Force established minimum insider threat standards. Such standards are required for the sharing and safeguarding of classified information on computer networks while ensuring consistent, appropriate protections for privacy and civil liberties. The Committees understand there are policies in place to attempt implementation of such standards; however, the Committees have found that several elements of the IC have not fully implemented such standards. Therefore, given the several high-profile insider threat issues, the Committees emphasize the importance of such minimums by statutorily requiring the DNI to establish a policy on minimum insider threat standards, consistent with the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, and IC elements should expeditiously establish their own policies and implement the DNI guidance.

Further, referring to the directive language found in the committee report accompanying H.R. 5515, the Fiscal Year 2019 NDAA reported by the House Armed Services Committee (HASC), the Committees direct the Chief Management Officer to provide a briefing to the congressional intelligence and defense committees, no later than 90 days after enactment of the Act, on the outcomes of its cost and technical analyses required by this report, and the DoD's efforts to implement enterprise-wide programs and policies for insider threat detection, user activity monitoring, and cyber-attack detection and remediation.

Intelligence Community Information Technology Environment.

The Committees remain supportive of the goals of Intelligence Community Information Technology Environment (IC ITE) and the importance of the common, secure sharing infrastructure it creates. The Committees further understand that the path to implement a complex, technical environment

such as IC ITE needs to be sufficiently flexible and agile. However, the Committees remain concerned with the lack of consistency and substance in previous reports and briefings on IC ITE. Therefore, section 6312 of Subdivision 2 of the Act requires a long-term roadmap, business plan, and security plan that shall be reported to the congressional intelligence committees at least quarterly with additional notifications as necessary.

Intelligence Community Chief Financial Officer.

The Chief Financial Officers (CFO) Act of 1990 mandated best practices for decision-

[[Page H10247]]

making and accountability, as well as improved decision-makers' access to reliable and timely financial and performance information. The CFO Act, as amended, requires that the chief financial officers of 24 departments and agencies ``report directly to the head of the agency regarding financial management matters.'' Section 6404 of Subdivision 2 of the Act brings the ODNI in line with the best practices implemented in the CFO Act.

Intelligence Community Chief Information Officer.

As codified in 44 U.S.C. 3506(a)(1)(A), each federal agency head is responsible for ``carrying out the information resources management activities to improve agency productivity, efficiency, and effectiveness.'' Accordingly, section 6405 of Subdivision 2 of the Act expresses the Committee's intent to emphasize the importance of the IC Chief Information Officer (CIO), as defined in 50 U.S.C. 3032(a), in assisting the DNI with information resource management by requiring the IC CIO to report directly to the DNI.

Central Intelligence Agency Subsistence for Personnel Assigned to Austere Locations.

Section 6411 of Subdivision 2 of the Act permits the Director of the CIA to allow subsistence for personnel assigned to austere locations. Although the statute does not define ``austere,'' the Committees believe that utilization of this authority should be minimal. Therefore, within 180 days after the enactment of the Act, the CIA shall brief the Committees on the CIA's definition of ``austere'' and the CIA regulations in place governing this authority.

Collocation of Certain Department of Homeland Security Personnel at Field Locations.

The Committees support DHS I&A's intent to integrate into operations across the broader DHS enterprise. Accordingly, section 6434 of Subdivision 2 of the Act requires I&A to identify opportunities for collocation of I&A field officers and to submit to the Committees a plan for their deployment.

Limitations on Intelligence Community Elements' Communications with Congress.

Effective oversight of the IC requires unencumbered communications between representatives of the agencies, members of Congress, and congressional staff. The Committees direct the DNI not to limit any element of the IC from having interactions with the congressional intelligence committees, including but not limited to, preclearance by the DNI of remarks, briefings, discussions of agency resources or authorities requirements, or mandatory reports to the DNI on conversations with the Committees.

Intelligence Community Support to the National Vetting Center.

On February 6, 2018, the President issued National Security Policy Memorandum (NSPM)-9, ''Presidential Memorandum on Optimizing the Use of Federal Government Information in Support of National Vetting Enterprise.'' The memorandum directs the DHS, in coordination with the ODNI and other agencies, to establish the National Vetting Center. The

memorandum also requires agencies to ``provide the Center access to relevant biographic, biometric, and related derogatory information.'' It further directs DNI, in coordination with the heads of relevant IC elements, to ``establish a support element to facilitate, guide, and coordinate all IC efforts to use classified intelligence and other relevant information within the IC holdings in support of the center.'' The Committees wish to obtain regular updates and the most current information about the activities of that support element.

Therefore, no later than 180 days after the enactment of the Act and annually thereafter, the Committees direct the DNI and the Under Secretary for Intelligence and Analysis at DHS to brief the Committees on the status of IC support to the National Vetting Center, as established by NSPM-9.

Update on Status of Attorney General-Approved U.S. Person Procedures under Executive Order 12333.

The Committees acknowledge the difficult, labor-intensive work undertaken by certain IC elements, to ensure the current effectiveness of, and in some cases to substantially revise, final Attorney General-approved procedures regarding the collection, dissemination, and retention of United States persons information. The Committees wish to better understand the status of this project, throughout the IC.

Therefore, the Committees direct that, not later than 60 days after enactment of the Act, the DNI and the Attorney General shall brief the Committees on the issuance of final, Attorney General-approved procedures by elements of the IC. Specifically, the briefing shall identify (1) any such elements that have not yet issued final procedures; and (2) with respect to such elements, the status of the procedures' development, and any interim guidance or procedures on which those elements currently rely.

Homegrown Violent Extremists Imprisoned in Department of Defense Facilities.

The Committees are concerned about an evident gap in information sharing about individuals imprisoned in DoD facilities who are categorized by the FBI as homegrown violent extremists (HVEs). A recent FBI report underscores this gap, highlighting the case of an individual who has been convicted and sentenced to death by a U.S. military court martial and remains incarcerated in a U.S. military facility. The Committees understand that, despite his incarceration, this inmate openly communicates with the outside world through written correspondence and has continued to inspire extremists throughout the world. The Committees further understand that the FBI is unable to determine the full scope of this inmate's contacts with the outside world because only a portion of his communications have been provided by the DoD.

Therefore, no later than 180 days after the enactment of the Act, the Committees direct the FBI to work with the DoD to create a process by which the DoD provides to the FBI the complete communications of individuals imprisoned in DoD facilities and who are categorized by the FBI as HVEs.

Naming of Federal Bureau of Investigation Headquarters.

According to statute enacted in 1972, the current FBI headquarters building in Washington, D.C. must be ``known and designated'' as the ``J. Edgar Hoover FBI Building.'' That tribute has aged poorly. It should be reconsidered, in view of Hoover's record on civil liberties--including the effort to disparage and undermine Dr. Martin Luther King Jr. Even today, Hoover's name evokes the FBI's sordid ``COINTELPRO'' activities.

The Committees believe Congress should consider repealing the provision requiring the existing Pennsylvania Avenue building to be known as the ``J. Edgar Hoover FBI Building.'' A new name should be determined, through a joint dialogue among Bureau leadership, law enforcement personnel, elected

officials, and civil rights leaders.

Science, Technology, Engineering, and Math careers in Defense Intelligence.

Referring to the directive language found in the committee report accompanying H.R. 5515, the HASC-reported Fiscal Year 2019 NDAA, the Committees direct the Director of DIA to provide, within 90 days after enactment of the Act, a briefing to the congressional intelligence committees and the congressional defense committees on a plan to develop a Science, Technology, Engineering, and Math career program that attracts and maintains the defense intelligence cadre of Science and Technical Intelligence analysts to meet tomorrow's threats.

Security and Intelligence Role in Export Control.

Referring to the directive language found in the committee report accompanying H.R. 5515, the HASC-reported Fiscal Year 2019 NDAA, the Committees direct the Under Secretary of Defense for Policy, in coordination with the USD(I), within 60 days of enactment of the Act, to brief the congressional intelligence and defense committees, on security support to export control.

Security Clearance Background Investigation Reciprocity.

Referring to the directive language found in the committee report accompanying H.R. 5515, the HASC-reported Fiscal Year 2019 NDAA, the Committees direct the Secretary of Defense, in coordination with the DNI and the Director of the Office of Personnel Management, within 60 days of enactment of the Act, to brief the Committees and the congressional defense committees on efforts to ensure seamless transition of investigations between authorized investigative agencies, as required by law.

Further, referring to the directive language found in the committee report accompanying H.R. 5515, the HASC-reported Fiscal Year 2019 NDAA, the Committees direct the Secretary of Defense, in coordination with the DNI and the Director of the Office of Personnel Management, within 90 days of enactment of the Act, to brief the congressional intelligence committees on efforts to ensure reciprocity is a consideration for implementation of continuous evaluation and continuous vetting across the federal government.

Foreign Influence Task Force.

The IC has warned of active measures taken by foreign actors to interfere with and undermine the U.S. democratic process, most recently and brazenly by the Russian Federation. The Committees appreciate FBI efforts to confront this challenge in part through creation of its Foreign Influence Task Force. The Committees believe that confronting foreign influence directed at the United States is of fundamental importance, and thus desire to engage in a close and regular dialogue with the FBI about the task force's activities.

Therefore, the Committees direct the FBI to provide detailed, quarterly briefings to the Committees regarding the task force's activities, to include its progress and any significant challenges.

Enhanced Oversight of IC Contractors.

A topic of sustained congressional intelligence committee interest has been improving the federal government's oversight of IC acquisition and procurement practices, including activities by poorly performing IC contractors.

A framework exists to ensure that IC elements do not award IC contracts to businesses that engage in negligence or even gross negligence, consistently fail to appropriately safeguard classified information, maintain poor financial practices, or other issues. For example, an IC element may maintain a list of contractors of concern, in order to ensure that proposals from such contractors are rejected or subjected to additional scrutiny. The Committees wish to build on these practices and are concerned about the existing

framework's adequacy.

Therefore, the Committees direct all elements of the IC, to the fullest extent consistent with applicable law and policy, to

[[Page H10248]]

share with one another information about contractors with track records of concern--such as the commission of negligence or gross negligence in the performance of IC contracts, or the repeated failure to appropriately safeguard classified information in a fashion that the contractor reasonably could have been expected to prevent.

Additionally, no later than 30 days after enactment of the Act, the DNI shall brief the Committees on the authorities of IC elements with respect to contractors with track records of concern--before, during, and after procurement. An objective of the briefing will be to discuss information sharing practices in this regard, and to identify specific areas where the oversight framework can be strengthened.

Security Clearance Reporting Requirements.

The Agreement directs the Office of Management and Budget, in coordination with members of the Performance Accountability Council, to report to Congress, within 90 days of enactment of the Act, on recommendations for harmonizing and streamlining reporting requirements related to security clearances that have been set forth in legislation.

Part III: Section-by-Section Analysis and Explanation of Legislative Text

SECTION-BY-SECTION ANALYSIS AND EXPLANATION

The following is a section-by-section analysis and explanation of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (the ``Act'').

SUBDIVISION 1--INTELLIGENCE AUTHORIZATIONS FOR FISCAL YEAR 2020

Section 5100. Table of contents.

Title LI--Intelligence Activities

Section 5101. Authorization of appropriations.

Section 5101 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 2020.

Section 5102. Classified schedule of authorizations.

Section 5102 provides that the details of the amounts authorized to be appropriated for intelligence and intelligence-related activities for Fiscal Year 2020 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 5103. Intelligence Community Management Account.

Section 5103 authorizes appropriations for the Intelligence Community Management Account (ICMA) of the ODNI for Fiscal Year 2020.

Title LII--Central Intelligence Agency Retirement and Disability System

Section 5201. Authorization of appropriations.

Section 5201 authorizes appropriations in the amount of $514,000,000 for the CIA Retirement and Disability Fund for Fiscal Year 2020.

Title LIII--Intelligence Community Matters

Subtitle A--General Intelligence Community Matters

Section 5301. Restriction on conduct of intelligence activities.

Section 5301 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 5302. Increase in employee compensation and benefits authorized by law.

Section 5302 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 5303. Expansion of scope of protections for identities of covert agents.

Section 5303 amends the definition of ``covert agent'' in the National Security Act of 1947 (50 U.S.C. 3126(4)) to protect the identities of all undercover intelligence officers, and United States citizens whose relationship to the United States is classified, regardless of the location of the individuals' government service or time since separation from government service.

Section 5304. Required counterintelligence assessments, briefings, notifications, and reports.

Section 5304 requires the DNI, in consultation with other appropriate agencies, to conduct an assessment following a United States election of any foreign government interference. Section 5304 requires the DNI to post publicly advisory reports on foreign counterintelligence and cybersecurity threats to federal election campaigns. It also requires quarterly briefings to the congressional intelligence committees regarding the Federal Bureau of Investigation's counterintelligence activities and prompt notification of an investigation carried out regarding a counterintelligence risk related to a federal election or campaign.

Section 5305. Inclusion of security risks in program management plans required for acquisition of major systems in National Intelligence Program.

Section 5305 amends the National Security Act of 1947 (50 U.S.C. 3024(q)(1)(A)) to require that the annual program management plans on major system acquisitions that the DNI submits to Congress address security risks, in addition to cost, schedule, performance goals, and program milestone criteria.

Section 5306. Intelligence community public-private talent exchange.

Section 5306 requires the DNI to develop policies, processes, and procedures to facilitate IC personnel rotations to the private sector and vice versa, to bolster skill development and collaboration. Section 5306 further sets forth requirements with which agreements governing such rotations must address, including terms and conditions, including termination, duration, employment status, pay, and benefits.

Section 5307. Assessment of contracting practices to identify certain security and counterintelligence concerns.

Section 5307 requires the DNI to conduct an assessment of the authorities, policies, processes, and standards used by the IC to ensure that the IC is weighing security and counterintelligence risks in contracting with companies that contract--or carry out joint research and development--with the People's Republic of China, the Russian Federation, the Democratic People's Republic of Korea, or the Islamic

Republic of Iran.

Subtitle B--Office of the Director of National Intelligence

Section 5321. Establishment of Climate Security Advisory Council.

Section 5321 requires the DNI to establish an advisory council to assist analytic components of the IC with incorporating analysis of climate security into their work. The council will also facilitate coordination and sharing of data between the IC and non-IC elements related to climate change.

Section 5322. Foreign Malign Influence Response Center.

Section 5322 establishes a Foreign Malign Influence Response Center within the ODNI to analyze and integrate all U.S. Government intelligence pertaining to hostile efforts undertaken by, at the direction of, or on behalf of or with the substantial support of, the government of the Russian Federation, Iran, North Korea, China, or any other country that the Director of the Center determines appropriate, to influence U.S.-based policies, activities, or public opinion.

Section 5323. Encouragement of cooperative actions to detect and counter foreign influence operations.

Section 5323 provides the DNI, in coordination with the Secretary of Defense, with the necessary authorities and ability to use up to $30 million of NIP funds, to establish an independent, non-profit Social Media Data and Threat Analysis Center (``Center''). Section 323 further provides that this Center shall establish a central portal for social media data analysis, enabling: (1) social media companies to voluntarily share data on foreign influence operations; (2) researchers to analyze that data; and (3) information sharing between and among government and private companies. Section 5323 also requires the Director of the Center to produce quarterly public reports on trends in foreign influence and disinformation operations, including any threats to campaigns and elections, as well as an annual report to Congress on the degree of cooperation and commitment from the social media companies.

Section 5324. Transfer of National Intelligence University to the Office of the Director of National Intelligence.

Section 5324 requires the Director of the DIA to transfer to the DNI the National Intelligence University, upon submission of required joint certifications to appropriate congressional committees by the Secretary of Defense and the DNI.

Subtitle C--Inspector General of the Intelligence Community

Section 5331. Definitions.

Section 5331 provides definitions for terminology used throughout this Subtitle.

Section 5332. Inspector General external review panel.

Section 5332 codifies the whistleblower protections contained in Part C of Presidential Policy Directive-19 to ensure an effective appeals process through external review panels and the reporting of waste, fraud, and abuse. Section 5332 further requires the Inspector General of the Intelligence Community (IC IG) to submit to the congressional intelligence committees a recommendation on how to ensure that a whistleblower with a complaint against an Inspector General of an IC agency has equal access to adjudication, appellate review, and external review panels.

Section 5333. Harmonization of whistleblower processes and procedures.

Section 5333 requires the IC IG, in coordination with the IC Inspectors General Forum, to develop recommendations applicable to Inspectors Generals for all IC elements regarding the harmonization, where appropriate, of policies

and directives related to whistleblower claims and appeals processes and procedures. Section 5333 further requires the IC IG to maximize transparency regarding these processes and procedures.

Section 5334. Oversight by Inspector General of the Intelligence Community over intelligence community whistleblower matters.

Section 5334 requires the IC IG, in consultation with the IC Inspectors General

[[Page H10249]]

Forum, to establish a system whereby the IC IG is provided in near real time of whistleblower complaints relating to the programs and activities under the DNI's jurisdiction, as well as any IG actions relating to such complaints.

Section 5335. Report on cleared whistleblower attorneys.

Section 5335 requires the IC IG to submit to the congressional intelligence committees a report on access to cleared attorneys by whistleblowers in the IC, including any recommended improvements to the limited security agreement process and such other options as the IC IG considers appropriate.

Subtitle D--Central Intelligence Agency

Section 5341. Clarification of certain authority of the Central Intelligence Agency.

Section 5341 clarifies current CIA authorities related to death benefits, requires the Director of the CIA to submit a report if the CIA does not modify relevant regulations, and requires a briefing on certain health care services for CIA personnel.

Title LIV--Security Clearances

Section 5401. Improving visibility into the security clearance process.

Section 5401 requires the DNI, acting as the Security Executive Agent, to issue a policy requiring the head of each Federal agency to create an electronic portal whereby the agency and its workforce applicants can review the status of their security clearance processing. An enterprise solution that is accessible to multiple agencies may meet this objective. Any portal should have appropriate security safeguards.

Section 5402. Making certain policies and execution plans relating to personnel clearances available to industry partners.

Section 5402 requires each head of a Federal agency to share security clearance policies and plans with directly affected industry partners, consistent with national security and with National Industrial Security Program (NISP) goals. Section 5402 further requires the DNI, acting as the Security Executive Agent, jointly with the Director of the NISP, to develop policies and procedures for sharing this information.

Title LV--Matters Relating to Foreign Countries

Subtitle A--Matters Relating to Russia

Section 5501. Annual reports on influence operations and campaigns in the United States by the Russian Federation.

Section 5501 requires the Director of the National Counterintelligence and Security Center to submit an annual report to the congressional intelligence committees concerning the influence operations and campaigns in the United States conducted by the Russian Federation.

Section 5502. Assessment of legitimate and illegitimate

financial and other assets of Vladimir Putin.

Section 5502 expresses the sense of Congress that the United States should do more to expose the corruption of Russian President Vladimir Putin and directs the DNI to submit to appropriate congressional committees an assessment on the net worth and financial and other assets of President Putin and his family members.

Section 5503. Assessments of intentions of political leadership of the Russian Federation.

Section 5503 directs the IC to submit assessments to certain congressional committees of the current intentions of the political leadership of the Russian Federation concerning potential military action against members of the North Atlantic Treaty Organization (NATO), responses to an enlarged United States or NATO military presence in Eastern Europe, and potential actions taken for the purpose of exploiting perceived divisions among the governments of Russia's Western adversaries.

Subtitle B--Matters Relating to China

Section 5511. Annual reports on influence operations and campaigns in the United States by the Communist Party of China.

Section 5511 requires the Director of the National Counterintelligence and Security Center to submit an annual report to the congressional intelligence committees concerning the influence operations and campaigns in the United States conducted by the Communist Party of China.

Section 5512. Report on repression of ethnic Muslim minorities in the Xinjiang region of the People's Republic of China.

Section 5512 requires the Director of National Intelligence to submit a report to the congressional intelligence committees concerning activity by the People's Republic of China to repress ethnic Muslim minorities in the Xinjiang region of China.

Section 5513. Report on efforts by People's Republic of China to influence election in Taiwan.

Section 5513 requires the DNI to submit a report within 45 days of the 2020 Taiwan Presidential and Vice Presidential elections concerning any influence operations by China to interfere in or undermine the election and efforts by the United States to disrupt those operations.

Subtitle C--Matters Relating to Other Countries

Section 5521. Sense of Congress and report on Iranian efforts in Syria and Lebanon.

Section 5521 requires the DNI, in coordination with the Secretary of State and the Secretary of Defense, to submit a report that assesses Iran's efforts to establish influence in Syria, Iran's support of proxy forces, and the resulting threats to U.S. interests and allies.

Section 5522. Assessments regarding the Northern Triangle and Mexico.

Section 5522 requires the DNI, in coordination with other IC officials, to submit a comprehensive assessment of drug trafficking, human trafficking, and human smuggling activities in the Northern Triangle and Mexico. Section 508 further requires the DNI to provide a briefing on the IC's collection priorities and activities in these areas.

Title LVI--Federal Efforts Against Domestic Terrorism

Section 5601. Definitions.

Section 5601 provides definitions for terminology used throughout this Title.

Section 5602. Strategic intelligence assessment of and

reports on domestic terrorism.
Section 5602 requires the Director of the FBI and the Secretary of Homeland Security, in consultation with the DNI, to submit a report on standardization of terminology and procedures relating to domestic terrorism, and a report containing strategic intelligence assessment and data on domestic terrorism, together with required documents and materials, with annual updates for 5 years thereafter.

Title LVII--Reports and Other Matters

Subtitle A--Reports and Briefings

Section 5701. Modification of requirements for submission to Congress of certain reports.
Section 5701 amends or cancels numerous reporting requirements under current law.
Section 5702. Increased transparency regarding counterterrorism budget of the United States.
Section 5702 makes several findings regarding the transparency of the IC's counterterrorism budget and directs a briefing from the executive branch on the feasibility of releasing additional information to the public concerning the IC's efforts on counterterrorism.
Section 5703. Study on role of retired and former personnel of intelligence community with respect to certain foreign intelligence operations.
Section 5703 requires the DNI to conduct a study on former IC personnel providing intelligence assistance to foreign governments, and to provide a report on the findings and a plan for recommendations.
Section 5704. Collection, analysis, and dissemination of workforce data.
Section 5704 requires the DNI to provide a publicly available annual report on diversity and inclusion efforts of the IC's workforce.
Section 5705. Plan for strengthening the supply chain intelligence function.
Section 5705 requires the Director of the NCSC, in coordination with interagency partners, to submit a plan for strengthening supply chain intelligence function.
Section 5706. Comprehensive economic assessment of investment in key United States technologies by companies or organizations linked to China.
Section 5706 requires the DNI, in coordination with other designated agencies, to submit to the congressional intelligence committees a comprehensive economic assessment of investment in key United States technologies, by companies or organizations linked to China, as well as the national security implications of Chinese-backed investments to the United States.
Section 5707. Report by Director of National Intelligence on fifth-generation wireless network technology.
Section 5707 directs the DNI to submit to the appropriate committees a report on the threat to the national security of the United States posed by adoption of fifth-generation wireless network built by foreign companies and possible efforts to mitigate the threat.
Section 5708. Report on use by intelligence community of facial recognition technology.
Section 5708 requires the DNI to submit a report on the IC's use of facial recognition technology.
Section 5709. Report on deepfake technology, foreign weaponization of deepfakes, and related notifications.
Section 5709 requires the DNI to submit a report on the potential national security impacts of machine-manipulated media and the use of machine-manipulated media by foreign governments to spread disinformation or engage in other malign activities.

Section 5710. Annual report by Comptroller General of the United States on cybersecurity and surveillance threats to Congress.

Section 5710 requires the Comptroller General, in consultation with the DNI, Secretary of Homeland Security, and the Sergeant at Arms, to submit a report to the Committees on cybersecurity and surveillance threats to Congress.

Section 5711. Analysis and periodic briefings on major initiatives of intelligence community in artificial intelligence and machine learning.

Section 5711 requires the DNI, in coordination with other appropriate IC elements, to provide briefings to the congressional intelligence committees on the IC's major initiatives in artificial intelligence and machine learning.

Section 5712. Report on best practices to protect privacy and civil liberties of Chinese Americans.

Section 5712 requires the DNI, through the Office of Civil Liberties, Privacy, and Transparency, and in coordination with other IC

[[Page H10250]]

civil liberty and privacy officers, to submit a report on how IC policies targeting China affect the privacy and civil liberties of certain Americans of Chinese descent, along with recommendations for necessary protections.

Section 5713. Oversight of foreign influence in academia.

Section 5713 requires the DNI, in consultation with other appropriate IC elements, to submit a report on the risks to sensitive research subjects posed by foreign entities. Section 5713 further requires the report to identify specific national security-related threats to research conducted at institutions of higher education.

Section 5714. Report on death of Jamal Khashoggi.

Section 5714 requires the DNI to submit to Congress an unclassified report on the death of Jamal Khashoggi, consistent with protecting sources and methods. The report shall include identification of those who carried out, participated in, ordered, or were otherwise complicit in, or responsible for, Mr. Khashoggi's death.

Section 5715. Report on terrorist screening database.

Section 5715 requires the DNI and the Secretary of State to jointly submit a report on the FBI's terrorist screening database.

Section 5716. Report containing threat assessment of terrorist use of conventional and advanced conventional weapons.

Section 5716 requires the Under Secretary of Homeland Security for I&A, in coordination with the Director of the FBI, to develop and submit a threat assessment regarding the availability of certain conventional weapons in support of terrorism activities.

Section 5717. Assessment of homeland security vulnerabilities associated with certain retired and former personnel of the intelligence community.

Section 5717 requires the DNI to submit an assessment of the homeland security vulnerabilities associated with retired and former personnel of the IC providing covered intelligence assistance.

Section 5718. Study on feasibility and advisability of establishing Geospatial-Intelligence Museum and learning center.

Section 5718 requires the Director of the National Geospatial-Intelligence Agency (NGA) to complete a study and report the findings on the feasibility and advisability of establishing a Geospatial-Intelligence Museum and learning center.

Subtitle B--Other Matters

Section 5721. Whistleblower disclosures to Congress and committees of Congress.

Section 5721 enables whistleblowers to provide classified disclosures to appropriate committees of Congress.

Section 5722. Task force on illicit financing of espionage and foreign influence operations.

Section 5722 requires the DNI to establish a task force to study and assess the illicit financing of espionage and foreign influence operations directed at the United States and requires the task force to issue a report on this subject to the appropriate congressional committees.

Section 5723. Establishment of fifth-generation technology prize competition.

Section 5723 establishes a program to award prizes to stimulate research and development relevant to fifth-generation wireless technology.

Section 5724. Establishment of deepfakes prize competition.

Section 5724 establishes a program to award prizes to stimulate the research, development, or commercialization of technologies to automatically detect machine-manipulated media.

Section 5725. Identification of and countermeasures against certain International Mobile Subscriber Identity-Catchers.

Section 5725 requires the DNI and the Director of the FBI, in collaboration with the Under Secretary of DHS for I&A, and other appropriate heads of Federal agencies, to undertake an effort to identify and, when appropriate, develop countermeasures against, International Mobile Subscriber Identity-Catchers operated within the United States by criminals and hostile foreign governments.

Section 5726. Securing energy infrastructure.

Section 5726 requires the Secretary of Energy, within 180 days of enactment of the Act, to establish a two-year control systems implementation pilot program within the National Laboratories. This pilot program will partner with covered entities in the energy sector to identify new security vulnerabilities, and for purposes of researching, developing, testing, and implementing technology platforms and standards in partnership with such entities. Section 5726 also requires the Secretary to establish a working group composed of identified private and public sector entities to evaluate the technology platforms and standards for the pilot program, and develop a national cyber-informed engineering strategy to isolate and defend covered entities from security vulnerabilities. Section 5726 requires the Secretary, within 180 days after the date on which funds are first disbursed, to submit to specified committees an interim report that describes the pilot program's results, provides a feasibility analysis, and describes the working group's evaluations. Section 5726 further requires the Secretary, within two years of funding, to submit to the congressional intelligence committees a progress report on the pilot program and an analysis of the feasibility of the methods studied, and a description of the working group's evaluation results.

SUBDIVISION 2--INTELLIGENCE AUTHORIZATIONS FOR FISCAL YEARS 2018 AND 2019

Section 6100. Table of contents.

Title LXI--Intelligence Activities

Section 6101. Authorization of appropriations.

Section 6101 lists the United States Government departments, agencies, and other elements for which the Act deems authorized appropriations for intelligence and

intelligence-related activities for Fiscal Years 2018 and 2019.

Section 6102. Intelligence Community Management Account.

Section 6102 provides that the amounts that were appropriated for Fiscal Years 2018 and 2019 are deemed authorized.

Title LXII--Central Intelligence Agency Retirement and Disability System

Section 6201. Authorization of appropriations.

Section 6201 deems authorized the appropriations for the CIA Retirement and Disability Fund for Fiscal Years 2018 and 2019.

Section 6202. Computation of annuities for employees of the Central Intelligence Agency.

Section 6202 makes technical changes to the CIA Retirement Act to conform with various statutes governing the Civil Service Retirement System.

Title LXIII--General Intelligence Community Matters

Section 6301. Restriction on conduct of intelligence activities.

Section 6301 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 the laws of the United States.

Section 6302. Increase in employee compensation and benefits authorized by law.

Section 6302 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 6303. Modification of special pay authority for science, technology, engineering, or mathematics positions and addition of special pay authority for cyber positions.

Section 6303 provides an increased yearly cap for Science, Technology, Engineering, or Mathematics (STEM) employee positions in the IC that support critical cyber missions. Section 6303 also permits the National Security Agency (NSA) to establish a special rate of pay for positions that perform functions that execute the agency's cyber mission.

Section 6304. Modification of appointment of Chief Information Officer of the Intelligence Community.

Section 6304 changes the position of IC Chief Information Officer from being subject to presidential appointment to being subject to appointment by the DNI.

Section 6305. Director of National Intelligence review of placement of positions within the intelligence community on the Executive Schedule.

Section 6305 requires the DNI, in coordination with the Office of Personnel Management, to conduct a review of the positions within the IC that may be appropriate for inclusion on the Executive Schedule, and the appropriate levels for inclusion.

Section 6306. Supply Chain and Counterintelligence Risk Management Task Force.

Section 6306 requires the DNI to establish a task force to standardize information sharing between the IC and the United States Government acquisition community with respect to supply chain, cybersecurity, and counterintelligence risks. Section 6306 further provides requirements for membership, security clearances, and annual reports.

Section 6307. Consideration of adversarial telecommunications and cybersecurity infrastructure when sharing

intelligence with foreign governments and entities.
Section 6307 requires the IC, when entering into foreign intelligence sharing agreements, to consider the pervasiveness of telecommunications and cybersecurity infrastructure, equipment, and services provided by United States adversaries or entities thereof.
Section 6308. Cyber protection support for the personnel of the intelligence community in positions highly vulnerable to cyber attack.
Section 6308 permits the DNI to provide cyber protection support for the personal technology devices and personal accounts of IC personnel whom the DNI determines to be highly vulnerable to cyber attacks and hostile information collection activities.
Section 6309. Elimination of sunset authority relating to management of supply-chain risk.
Section 6309 extends certain IC procurement authorities to manage and protect against supply chain risks.
Section 6310. Limitations on determinations regarding certain security classifications.
Section 6310 prohibits an officer of the IC who is nominated to a Senate-confirmed position from making certain classification determinations posing potential conflicts of interest regarding that nominee.

[[Page H10251]]

Section 6311. Joint Intelligence Community Council.
Section 6311 amends Section 101A of the National Security Act of 1947 (50 U.S.C. 3022(d)) as to the Joint Intelligence Community Council meetings and to require a report on its activities.
Section 6312. Intelligence community information technology environment.
Section 6312 defines the roles and responsibilities for the performance of the Intelligence Community Information Technology Environment (IC ITE). Section 6312 requires certain reporting and briefing requirements to the congressional intelligence committees regarding the IC's ongoing implementation of IC ITE.
Section 6313. Report on development of secure mobile voice solution for intelligence community.
Section 6313 requires the DNI, in coordination with the Directors of the CIA and NSA, provide the congressional intelligence committees with a classified report on the feasibility, desirability, cost, and required schedule associated with the implementation of a secure mobile voice solution for the IC.
Section 6314. Policy on minimum insider threat standards.
Section 6314 requires the DNI to develop minimum insider threat standards to be followed by each element of the IC, consistent with the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.
Section 6315. Submission of intelligence community policies.
Section 6315 requires the DNI to make all ODNI policies and procedures available to the congressional intelligence committees. Section 6315 also requires ODNI to notify the congressional committees of any new or rescinded policies.
Section 6316. Expansion of intelligence community recruitment efforts.
Section 6316 requires the DNI, in consultation with IC elements, to submit a plan to the congressional intelligence committees as to each element's efforts in recruitment from rural and underrepresented regions.

Title LXIV--Matters Relating to Elements of the Intelligence Community

Subtitle A--Office of the Director of National Intelligence

Section 6401. Authority for protection of current and former employees of the Office of the Director of National Intelligence.

Section 6401 amends Title 50, section 3506, to provide protection for current and former ODNI personnel and designated immediate family members, if there is a national security threat that warrants such protection.

Section 6402. Designation of the program manager-information sharing environment.

Section 6402 amends the Intelligence Reform and Terrorism Protection Act of 2004 so that the Program Manager-Information Sharing Environment (PM-ISE) is subject to appointment by the DNI, not the President.

Section 6403. Technical modification to the executive schedule.

Section 6403 amends the Executive Schedule to make the Director of the National Counterintelligence and Security Center a Level IV position on the Executive Schedule.

Section 6404. Chief Financial Officer of the Intelligence Community.

Section 6404 amends the National Security Act of 1947 by requiring the Chief Financial Officer of the IC to directly report to the DNI.

Section 6405. Chief Information Officer of the Intelligence Community.

Section 6405 amends the National Security Act of 1947 by requiring the Chief Information Officer of the IC to directly report to the DNI.

Subtitle B--Central Intelligence Agency

Section 6411. Central Intelligence Agency subsistence for personnel assigned to austere locations.

Section 6411 authorizes the Director of the CIA to approve, with or without reimbursement, subsistence to personnel assigned to an austere overseas location.

Section 6412. Special rules for certain monthly workers' compensation payments and other payments for Central Intelligence Agency personnel.

Section 6412 authorizes the Director of the CIA to provide enhanced injury benefits to a covered employee or qualifying dependents who suffer an injury overseas due to war, insurgency, hostile act, or terrorist activities.

Section 6413. Expansion of security protective service jurisdiction of the Central Intelligence Agency.

Section 6413 expands the security perimeter jurisdiction at CIA facilities from 500 feet to 500 yards.

Section 6414. Repeal of foreign language proficiency requirement for certain senior level positions in the Central Intelligence Agency.

Section 6414 repeals Title 50, section 3036(g), with conforming amendments to section 611 of the Intelligence Authorization Act for Fiscal Year 2005 (Public Law 108-487).

Subtitle C--Office of Intelligence and Counterintelligence of the Department of Energy

Section 6421. Consolidation of Department of Energy Offices of Intelligence and Counterintelligence.

Section 6421 amends the Department of Energy Organization Act to consolidate the offices of intelligence and counterintelligence into the DOE Office of Intelligence and Counterintelligence.

Section 6422. Repeal of Department of Energy Intelligence Executive Committee and budget reporting requirement.

Section 6422 amends the Department of Energy Organization

Act by repealing the Department of Energy Intelligence Executive Committee, as well as certain budgetary reporting requirements.

Subtitle D--Other Elements

Section 6431. Plan for designation of counterintelligence component of the Defense Security Service as an element of intelligence community.

Section 6431 directs the DNI and the Under Secretary of Defense for Intelligence, in coordination with the Director of the National Counterintelligence and Security Center, to provide the congressional intelligence and defense committees with an implementation plan to make the Defense Security Service's (DSS's) Counterintelligence component an element of the IC as defined in paragraph(4) of section 3 of the National Security Act of 1947 (50 U.S.C. 3003(4)), by January 1, 2020. Section 6431 further mandates that the plan shall not address the DSS's personnel security functions.

Section 6432. Notice not required for private entities.

Section 6432 provides a Rule of Construction that the Secretary of the Department of Homeland Security (DHS) is not required to provide notice to private entities before issuing directives on agency information security policies and practices.

Section 6433. Establishment of advisory board for National Reconnaissance Office.

Section 6433 amends the National Security Act of 1947 to authorize the Director of the NRO to establish an advisory board to study matters related to space, overhead reconnaissance, acquisition, and other matters. Section 6433 provides that the board shall terminate 3 years after the Director declares the board's first meeting.

Section 6434. Collocation of certain Department of Homeland Security personnel at field locations.

Section 6434 requires the Under Secretary of Homeland Security for Intelligence & Analysis (DHS I&A) to identify opportunities for collocation of I&A field officers and to submit to the congressional intelligence committees a plan for deployment.

Title LXV--Election Matters

Section 6501. Report on cyber attacks by foreign governments against United States election infrastructure.

Section 6501 directs the DHS Under Secretary for I&A to submit a report on cyber attacks and attempted cyber attacks by foreign governments on United States election infrastructure, in connection with the 2016 presidential election. Section 6501 further requires this report to include identification of the States and localities affected and include efforts to attack voter registration databases, voting machines, voting-related computer networks, and the networks of Secretaries of State and other election officials.

Section 6502. Review of intelligence community's posture to collect against and analyze Russian efforts to influence the Presidential election.

Section 6502 requires the DNI to submit to the congressional intelligence committees, within one year of enactment of the Act, a report on the Director's review of the IC's posture to collect against and analyze Russian efforts to interfere with the 2016 United States presidential election. Section 6502 further requires the review to include assessments of IC resources, information sharing, and legal authorities.

Section 6503. Assessment of foreign intelligence threats to Federal elections.

Section 6503 requires the DNI, in coordination with the

Director of the CIA, Director of the NSA, Director of the FBI, Secretary of DHS, and heads of other relevant IC elements, to commence assessments of security vulnerabilities of State election systems one year before regularly scheduled Federal elections. Section 6503 further requires the DNI to submit a report on such assessments 180 days before regularly scheduled Federal elections, and an updated assessment 90 days before regularly scheduled Federal elections.

Section 6504. Strategy for countering Russian cyber threats to United States elections.

Section 6504 requires the DNI, in coordination with the Secretary of DHS, Director of the FBI, Director of the CIA, Secretary of State, Secretary of Defense, and Secretary of the Treasury, to develop a whole-of-government strategy for countering Russian cyber threats against United States electoral systems and processes. Section 6504 further requires this strategy to include input from solicited Secretaries of State and chief election officials.

Section 6505. Assessment of significant Russian influence campaigns directed at foreign elections and referenda.

Section 6505 requires the DNI to provide a report assessing past and ongoing Russian influence campaigns against foreign elections and referenda, to include a summary of the means by which such influence campaigns have been or are likely to be conducted, a summary of defenses against or responses to such Russian influence campaigns, a summary of IC activities to assist

[[Page H10252]]

foreign governments against such campaigns, and an assessment of the effectiveness of such foreign defenses and responses.

Section 6506. Information sharing with State election officials.

Section 6506 requires the DNI, within 30 days of enactment of the Act, to support security clearances for each eligible chief election official of a State, territory, or the District of Columbia (and additional eligible designees), up to the Top Secret level. Section 6506 also requires the DNI to assist with sharing appropriate classified information about threats to election systems.

Section 6507. Notification of significant foreign cyber intrusions and active measure campaigns directed at elections for Federal offices.

Section 6507 requires the Director of the FBI, and the Secretary of Homeland Security to brief the congressional intelligence committees, congressional leadership, the armed services committees, the appropriations committees, and the homeland security committees (consistent with sources and methods) not later than 14 days after a determination has been made with moderate or high confidence that a significant foreign cyber intrusion or active measures campaign intended to influence an upcoming election for any Federal office has taken place by a foreign state or foreign non-state person, group, or other entity. The briefing shall provide a description of the significant foreign cyber intrusion or active measures campaign, including an identification of the foreign state or foreign non-state person or group.

Section 6508. Designation of counterintelligence officer to lead election security matters.

Section 6508 requires the DNI to designate a national counterintelligence officer within the National Counterintelligence and Security Center to lead, manage, and coordinate election security-related counterintelligence matters, including certain risks from foreign power interference.

Title LXVI--Security Clearances

Section 6601. Definitions.

Section 6601 provides definitions for terminology used throughout this Title.

Section 6602. Reports and plans relating to security clearances and background investigations.

Section 6602 requires the interagency Performance Accountability Council (Council) to provide plans to reduce the background investigation inventory and best align the investigation function between DoD and the National Background Investigation Bureau. Section 6602 further requires the Council to report on the future of the clearance process and requires the DNI to notify the appropriate committees of responding to official requests to change clearance standards, and the status of those requests' disposition. As with other reports in this title, these reports can be met in a consolidated format and potentially through the regularly scheduled quarterly Council briefings.

Section 6603. Improving the process for security clearances.

Section 6603 requires the DNI to review the Questionnaire for National Security positions (SF-86 or any current instantiation thereof) and the Federal Investigative Standards to determine potential unnecessary information required and assess whether revisions are necessary to account for insider threats. Section 6603 further requires the DNI, in coordination with the Council, to establish policies on interim clearances and consistency between the clearance process for contract and government personnel.

Section 6604. Goals for promptness of determinations regarding security clearances.

Section 6604 requires the Council to implement a plan to be able to process 90 percent of clearance requests at the Secret level in 30 days, and at the Top Secret-level in 90 days. The provision provides the Council with latitude to issue equivalent metrics that similarly improve the timeliness of the clearance process. The plan shall also address how to recognize reciprocity in accepting clearances among agencies within two weeks, and to require that ninety percent of clearance holders not be subject to a time-based periodic investigation.

Section 6605. Security Executive Agent.

Section 6605 establishes the DNI as the government's Security Executive Agent, consistent with Executive Order 13467, and sets forth relevant authorities.

Section 6606. Report on unified, simplified, Governmentwide standards for positions of trust and security clearances.

Section 6606 directs the DNI and the Director of the Office of Personnel Management to report on the advisability and implications of consolidating the tiers for positions of trust and security clearances from 5 to 3 tiers.

Section 6607. Report on clearance in person concept.

Section 6607 requires the DNI to submit a report on a concept whereby an individual can maintain eligibility for access to classified information for up to 3 years after access may lapse.

Section 6608. Reports on reciprocity for security clearances inside of departments and agencies.

Section 6608 requires each federal agency to submit a report to the DNI that identifies the number of clearances that take more than two weeks to reciprocally recognize and set forth the reason for any delays. Section 6608 further requires the DNI to submit an annual report summarizing reciprocity.

Section 6609. Intelligence community reports on security clearances.

Section 6609 requires the DNI to submit a report on each IC element's security clearance metrics, segregated by Federal employees and contractor employees.

Section 6610. Periodic report on positions in the intelligence community that can be conducted without

access to classified information, networks, or facilities.

Section 6610 requires the DNI to submit to the congressional intelligence committees a report on positions that can be conducted without access to classified information, networks, or facilities, or may require only a Secret-level clearance.

Section 6611. Information-sharing program for positions of trust and security clearances.

Section 6611 requires the Security Executive Agent and the Suitability and Credentialing Executive Agents to establish a program to share information between and among government agencies and industry partners to inform decisions about positions of trust and security clearances.

Section 6612. Report on protections for confidentiality of whistleblower-related communications.

Section 6612 requires the Security Executive Agent, in coordination with the IC IG, to submit a report detailing the IC's controls used to ensure continuous evaluation programs protect the confidentiality of whistleblower-related communications.

Section 6613. Reports on costs of security clearance background investigations.

Section 6613 requires the DNI to provide an annual report for three years after enactment on the resources expended by each government agency for processing security clearance background investigations and continuous evaluation programs, disaggregated by tier and employment status.

Title LXVII--Reports and Other Matters

Subtitle A--Matters Relating to Russia and Other Foreign Powers

Section 6701. Limitation relating to establishment or support of cybersecurity unit with the Russian Federation.

Section 6701 prohibits the Federal government from expending any funds to establish or support a cybersecurity unit or other cyber agreement that is jointly established or otherwise implemented by the United States Government and the Russian Federation, unless the DNI submits a report to the appropriate congressional committees at least 30 days prior to any such agreement. The report shall include the agreement's purpose, intended shared intelligence, value to national security, counterintelligence concerns, and any measures taken to mitigate such concerns.

Section 6702. Assessment of threat finance relating to Russia.

Section 6702 requires the DNI, in coordination with the Assistant Secretary of the Treasury for Intelligence and Analysis, to submit to the congressional intelligence committees, within 60 days of enactment of the Act, an assessment of Russian threat finance, based on all-source intelligence from both the IC and the Office of Terrorism and Financial Intelligence of the Treasury Department. Section 6702 further requires the assessment to include global nodes and entry points for Russian money laundering; United States vulnerabilities; connections between Russian individuals involved in money laundering and the Russian Government; counterintelligence threats to the United States posed by Russian money laundering and other forms of threat finance; and challenges to United States Government efforts to enforce sanctions and combat organized crime.

Section 6703. Notification of an active measures campaign.

Section 6703 requires the DNI to notify congressional leadership, and the Chairman and Vice Chairman or Ranking Member of the appropriate congressional committees, each time the DNI has determined there is credible information that a foreign power has attempted, is attempting, or will attempt to employ a covert influence or active measures campaign with

regard to the modernization, employment, doctrine, or force posture of the United States' nuclear deterrent or missile defense. Section 6703 further requires that such notification must include information on any actions that the United States has taken to expose or halt such attempts.

Section 6704. Notification of travel by accredited diplomatic and consular personnel of the Russian Federation in the United States.

Section 6704 requires the Secretary of State to ensure that the Russian Federation provides notification at least two business days in advance of all travel that is subject to such requirements by accredited diplomatic and consular personnel of the Russian Federation in the United States, and take necessary action to secure full compliance by Russian personnel and address any noncompliance.

Section 6705. Report and annual briefing on Iranian expenditures supporting foreign military and terrorist activities.

Section 6705 requires the DNI to submit a report to Congress describing Iranian expenditures on military and terrorist activities outside the country.

[[Page H10253]]

Section 6706. Expansion of scope of committee to counter active measures.

Section 6706 amends a provision in the Intelligence Authorization Act for Fiscal Year 2017 to expand the scope of the interagency committee to counter active measures by the Russian Federation to add China, Iran, North Korea, and other nation states.

Subtitle B--Reports

Section 6711. Technical correction to Inspector General study.

Section 6711 amends Title 50, section 11001(d), by replacing the IC IG's ``audit'' requirement for Inspectors General with employees having classified material access, with a ``review'' requirement.

Section 6712. Reports on authorities of the Chief Intelligence Officer of the Department of Homeland Security.

Section 6712 requires the Secretary of DHS, in consultation with the Under Secretary for I&A, to submit to the congressional intelligence committees a report on the adequacy of the Under Secretary's authorities required as the Chief Intelligence Officer to organize the Homeland Security Intelligence Enterprise, and the legal and policy changes necessary to coordinate, organize, and lead DHS intelligence activities.

Section 6713. Review of intelligence community whistleblower matters.

Section 6713 directs the IC IG, in consultations with the IGs of other IC agencies, to conduct a review of practices and procedures relating to IC whistleblower matters.

Section 6714. Report on role of Director of National Intelligence with respect to certain foreign investments.

Section 6714 directs the DNI to submit a report on ODNI's role in preparing analytic materials in connection with the United States Government's evaluation of national security risks associated with potential foreign investments.

Section 6715. Report on surveillance by foreign governments against United States telecommunications networks.

Section 6715 requires the DNI, in coordination with the Director of the CIA, Director of the NSA, Director of the FBI, and Secretary of DHS, to submit to the congressional

intelligence, judiciary, and homeland security committees, within 180 days of enactment of the Act, a report on known attempts by foreign governments to exploit cybersecurity vulnerabilities in United States telecommunications networks to surveil United States persons, and any actions that the IC has taken to protect United States Government agencies and personnel from such surveillance.

Section 6716. Biennial report on foreign investment risks.

Section 6716 requires the DNI to establish an IC working group on foreign investment risks and prepare a biennial report that includes an identification, analysis, and explanation of national security vulnerabilities, foreign investment trends, foreign countries' strategies to exploit vulnerabilities through the acquisition of either critical technologies (including components or items essential to national defense), critical materials (including physical materials essential to national security), or critical infrastructure (including physical or virtual systems and assets whose destruction or incapacity would have a debilitating impact on national security), and market distortions caused by foreign countries. Technologies, materials, and infrastructure are deemed to be ``critical'' under this provision if their exploitation by a foreign government could cause severe harm to the national security of the United States.

Section 6717. Modification of certain reporting requirement on travel of foreign diplomats.

Section 6717 amends a provision in the Intelligence Authorization Act for Fiscal Year 2017, to require reporting of ``a best estimate'' of known or suspected violations of certain travel requirements by accredited diplomatic and consular personnel of the Russian Federation.

Section 6718. Semiannual reports on investigations of unauthorized disclosures of classified information.

Section 6718 requires the Assistant Attorney General for National Security at the Department of Justice, in consultation with the Director of the FBI, to submit to the congressional intelligence and judiciary committees a semiannual report on the status of IC referrals to the Department of Justice regarding unauthorized disclosures of classified information. Section 6718 also directs IC elements to submit to the congressional intelligence committees a semiannual report on the number of investigations opened and completed by each agency regarding an unauthorized public disclosure of classified information to the media, and the number of completed investigations referred to the Attorney General.

Section 6719. Congressional notification of designation of covered intelligence officer as persona non grata.

Section 6719 requires, not later than 72 hours after a covered intelligence officer is designated as persona non grata, that the DNI, in consultation with the Secretary of State, submit to the designated committees a notification of that designation, to include the basis for the designation and justification for the expulsion.

Section 6720. Reports on intelligence community participation in vulnerabilities equities process of Federal Government.

Section 6720 requires the DNI to submit, within 90 days of enactment of the Act, to the congressional intelligence committees a report describing the Vulnerabilities Equities Process (VEP) roles and responsibilities for each IC element. Section 6720 further requires each IC element to report to the congressional intelligence committees within 30 days of a significant change to that respective IC element's VEP process and criteria. Section 6720 also requires the DNI to submit an annual report to the congressional intelligence committees with specified information on certain VEP metrics.

Section 6721. Inspectors General reports on classification.

Section 6721 requires each designated IG to submit to the congressional intelligence committees a report on the accuracy in the application of classification and handling markings on a representative sample of finished products, to include those with compartments. Section 6721 also directs analyses of compliance with declassification procedures and a review of the effectiveness of processes for identifying topics of public or historical importance that merit prioritization for declassification review.

Section 6722. Reports on global water insecurity and national security implications and briefing on emerging infectious disease and pandemics.

Section 6722 requires the DNI to submit to the congressional intelligence committees a report on the implications of global water insecurity on the United States' national security interests. Section 6722 further requires the DNI to provide a briefing to appropriate congressional committees on the geopolitical effects of emerging infectious disease and pandemics, and their implications on the United States' national security.

Section 6723. Annual report on memoranda of understanding between elements of intelligence community and other entities of the United States Government regarding significant operational activities or policy.

Section 6723 amends a provision in the Intelligence Authorization Act for Fiscal Year 2017, instead requiring each IC element to submit an annual report to the Committees that lists each significant memorandum of understanding or other agreement entered into during the preceding fiscal year. Section 6723 further requires each IC element to provide such documents if an intelligence committee so requests.

Section 6724. Study on the feasibility of encrypting unclassified wireline and wireless telephone calls.

Section 6724 requires the DNI to complete a study on the feasibility of encrypting unclassified wireline and wireless telephone calls between personnel in the IC.

Section 6725. Reports on intelligence community loan repayment and related programs.

Section 6725 requires the DNI, in cooperation with the heads of the elements of the IC, to submit to the congressional intelligence committees a report on potentially establishing an IC-wide program for student loan repayment and forgiveness.

Section 6726. Repeal of certain reporting requirements.

Section 6726 repeals certain IC reporting requirements.

Section 6727. Inspector General of the Intelligence Community report on senior executives of the Office of the Director of National Intelligence.

Section 6727 directs the IC IG to submit a report to the congressional intelligence committees regarding senior executive service staffing at the ODNI.

Section 6728. Briefing on Federal Bureau of Investigation offering permanent residence to sources and cooperators.

Section 6728 directs the FBI within 30 days of enactment of this Act to provide a briefing to the congressional intelligence committees regarding the FBI's ability to provide permanent U.S. residence to foreign individuals who serve as cooperators in national security-related investigations.

Section 6729. Intelligence assessment of North Korea revenue sources.

Section 6729 requires the DNI, in coordination with other relevant IC elements, to produce to the congressional intelligence committees an intelligence assessment of the North Korean regime's revenue sources.

Section 6730. Report on possible exploitations of virtual currencies by terrorist actors.

Section 6730 requires the DNI, in consultation with the

Secretary of the Treasury, to submit to Congress a report on the possible exploitation of virtual currencies by terrorist actors.

Subtitle C--Other Matters

Section 6741. Public Interest Declassification Board.

Section 6741 permanently reauthorizes the Public Interest Declassification Board administered by the National Archives and Records Administration.

Section 6742. Technical and clerical amendments to the National Security Act of 1947.

Section 6742 makes certain edits to the National Security Act of 1947 as amended for technical or clerical purposes.

Section 6743. Bug bounty programs.

Section 6743 directs the Secretary of DHS, in consultation with the Secretary of Defense, to submit a strategic plan to implement bug bounty programs at appropriate

[[Page H10254]]

agencies and departments of the United States Government. Section 6743 further requires the plan to include an assessment of the ``Hack the Pentagon'' pilot program and subsequent bug bounty programs. Section 6743 also requires the plan to provide recommendations on the feasibility of initiating bug bounty programs across the United States Government.

Section 6744. Technical amendments related to the Department of Energy.

Section 6744 provides technical corrections to certain provisions regarding the Department of Energy's Office of Intelligence and Counterintelligence.

Section 6745. Sense of Congress on notification of certain disclosures of classified information.

Section 6745 expresses the sense of Congress that, pursuant to the requirement for the IC to keep the congressional intelligence committees ``fully and currently informed'' in Section 502 of the National Security Act of 1947, IC agencies must submit prompt written notification after becoming aware that an individual in the executive branch has disclosed certain classified information outside established intelligence channels to foreign adversaries--North Korea, Iran, China, Russia, or Cuba.

Section 6746. Sense of Congress on consideration of espionage activities when considering whether or not to provide visas to foreign individuals to be accredited to a United Nations mission in the United States.

Section 6746 provides a Sense of Congress that, as to foreign individuals to be accredited to a United Nations mission, the Secretary of State should consider known and suspected intelligence and espionage activities, including activities constituting precursors to espionage, carried out by such individuals against the United States, or against foreign allies or partners of the United States. Section 6746 further provides that the Secretary of State should consider an individual's status as a known or suspected intelligence officer for a foreign adversary.

Section 6747. Sense of Congress on WikiLeaks.

Section 6747 provides a Sense of Congress that WikiLeaks and its senior leadership resemble a non-state hostile intelligence service, often abetted by state actors, and should be treated as such.
