Calendar No. 97

116TH CONGRESS
1st Session

SENATE

REPORT
116–47

DAMON PAUL NELSON AND MATTHEW YOUNG POLLARD INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEARS 2018, 2019, AND 2020

JUNE 11, 2019.—Ordered to be printed

Mr. BURR, from the Select Committee on Intelligence, submitted the following

R E P O R T

together with

ADDITIONAL VIEWS

[To accompany S. 1589]

The Select Committee on Intelligence, having considered an original bill (S. 1589) to authorize appropriations for fiscal years 2018, 2019, and 2020 for intelligence and intelligence-related activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes, reports favorably thereon and recommends that the bill do pass.

CLASSIFIED ANNEXES TO THE COMMITTEE REPORT

Pursuant to Section 364 of the Intelligence Authorization Act for Fiscal Year 2010 (Public Law 111–259), the Director of National Intelligence (DNI) publicly disclosed on June 12, 2017, that the President's aggregate request for the National Intelligence Program (NIP) for Fiscal Year 2018 was $57.7 billion; on February 27, 2018, that the request for the NIP for Fiscal Year 2019 was $59.9 billion; and on March 18, 2019, that the request for the NIP for Fiscal Year 2020 was $62.8 billion. Other than for limited unclassified appropriations—primarily the Intelligence Community Management Account—the classified nature of United States intelligence activities precludes any further disclosure, including by the Committee, of the details of its budgetary recommendations. Accordingly, the

Committee has prepared classified annexes to this report for Fiscal Years 2018, 2019 and 2020, with Schedules of Authorizations for Fiscal Years 2019 and 2020. Funding for Fiscal Year 2018 is deemed authorized, without a specific Schedule of Authorization.

The classified Schedules of Authorizations for Fiscal Years 2019 and 2020 are incorporated by reference in the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 and have the legal status of public law. The classified annexes are made available to the Committees on Appropriations of the Senate and the House of Representatives and to the President. The classified annexes are also available for review by any Member of the Senate subject to Senate Resolution 400 of the 94th Congress (1976).

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") that was reported by the Committee.

DIVISION A—INTELLIGENCE AUTHORIZATIONS FOR FISCAL YEAR 2020

TITLE I—INTELLIGENCE ACTIVITIES

Section 101. Authorization of appropriations

Section 101 lists the United States Government departments, agencies, and other elements for which the Act authorizes appropriations for intelligence and intelligence-related activities for Fiscal Year 2020.

Section 102. Classified schedule of authorizations

Section 102 provides that the details of the amounts authorized to be appropriated for intelligence and intelligence-related activities 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 103. Intelligence community management account

Section 103 authorizes appropriations for the Intelligence Community Management Account (ICMA) of the ODNI for Fiscal Year 2020.

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

Section 201. Authorization of appropriations

Section 201 authorizes appropriations in the amount of $514,000,000 for the CIA Retirement and Disability Fund for Fiscal Year 2020.

Section 202. Modification of amount of Central Intelligence Agency voluntary separation pay

Section 202 provides the DNI and the Director of the CIA with authorities to increase voluntary separation payments to $40,000,

with future automatic adjustments according to the Consumer Price Index.

TITLE III—INTELLIGENCE COMMUNITY MATTERS

SUBTITLE A—GENERAL INTELLIGENCE COMMUNITY MATTERS

Section 301. Restriction on conduct of intelligence activities

Section 301 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 302. Increase in employee compensation and benefits authorized by law

Section 302 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 303. Improving the onboarding methodology for certain intelligence personnel

Section 303 requires the Secretary of Defense and the DNI to report on common methodology for onboarding in the Intelligence Community (IC), as well as metrics, collaboration, and automation throughout the process. Section 303 further requires IC surveys regarding the onboarding process.

Section 304. Intelligence community public-private talent exchange

Section 304 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 304 further sets forth the employment detail requirements for such agreement terms and conditions, termination, duration, employment status, pay, and benefits.

Section 305. Expansion of scope of protections for identities of covert agents

Section 305 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 of government service.

Section 306. Inclusion of security risks in program management plans required for acquisition of major systems in National Intelligence Program

Section 306 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 307. Paid parental leave

Section 307 requires the DNI to issue a policy to make available 12 weeks of paid administrative leave for the IC personnel in the event of the birth of a child, including adoptive and foster parents. Section 307 further requires ODNI to submit a plan for implementation to the congressional intelligence committees within one year after enactment, and directs implementation within 90 days thereafter.

SUBTITLE B—OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Section 311. Exclusivity, consistency, and transparency in security clearance procedures and right to appeal

Section 311 requires the Executive Branch to publish adjudicative guidelines for determining eligibility to access classified information and makes these guidelines the exclusive basis for granting, denying, and revoking clearances in order to increase transparency, accountability, and due process. Section 311 further codifies the right of government employees to appeal unfavorable eligibility determinations to an agency-level panel. Section 311 also creates a higher level review by a government-wide appeals panel, chaired by the DNI as the government's Security Executive Agent, to review certain agency-level panel determinations involving allegations of constitutional violations or discrimination. This DNI-led panel can remand decisions to the employing agency for reevaluation if they find valid cause.

Section 312. Limitation on transfer of National Intelligence University

Section 312 prohibits the DNI and the Secretary of Defense from undertaking any activity to transfer the National Intelligence University (NIU) out of the Defense Intelligence Agency (DIA) until the DNI and the Secretary jointly certify that: the NIU has had its regional academic accreditation restored to full standing; the NIU has exclusivity for providing advanced intelligence education for Department of Defense (DoD) personnel; military personnel will receive joint professional military education credit; ODNI has degree-granting authority; and a joint governance model between ODNI and DoD is in place. Section 312 further requires the DNI and Secretary of Defense to submit to appropriate congressional committees cost estimates for NIU's operation, and for transferring the NIU to another agency.

Section 313. Improving visibility into the security clearance process

Section 313 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.

Section 314. Making certain policies and execution plans relating to personnel clearances available to industry partners

Section 314 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 In-

dustrial Security Program (NISP) goals. Section 314 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.

SUBTITLE C—INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY

Section 321. Definitions

Section 321 provides definitions for terminology used throughout this Subtitle.

Section 322. Inspector General external review panel

Section 322 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 322 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 323. Harmonization of whistleblower processes and procedures

Section 323 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 of policies and directives related to whistleblower claims and appeals processes and procedures. Section 323 further requires the IC IG to maximize transparency regarding these processes and procedures.

Section 324. Intelligence community oversight of agency whistleblower actions

Section 324 requires the IC IG, in consultation with the IC Inspectors General Forum, to complete a feasibility study on establishing a hotline whereby whistleblower complaints relating to the IC are automatically referred to the IC IG. Section 324 further requires that the IC IG establish a system whereby the IC IG is provided in near real-time all information relating to whistleblower complaints relating to the programs and activities under the DNI's jurisdiction, as well as any IG actions relating to such complaints.

Section 325. Report on cleared whistleblower attorneys

Section 325 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.

TITLE IV—REPORTS AND OTHER MATTERS

Section 401. Study on foreign employment of former personnel of intelligence community

Section 401 requires the DNI, in coordination with the Secretary of Defense and Secretary of State, to conduct a study of issues per-

taining to former IC employees working with, or in support of, foreign governments; to provide a report to the appropriate committees on the study's findings, including necessary legislative or administrative action; and to assess how requirements could be imposed for compliance reporting.

Section 402. Comprehensive economic assessment of investment in key United States technologies by companies or organizations linked to China

Section 402 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 403. Analysis and periodic briefings on major initiatives of intelligence community in artificial intelligence and machine learning

Section 403 requires the DNI, in coordination with other appropriate IC elements, to provide to the congressional intelligence committees an analysis of the IC's major initiatives in artificial intelligence and machine learning. Section 403 further requires semi-annual briefings for two years, followed by annual briefings for the five years thereafter.

Section 404. Encouraging cooperative actions to detect and counter foreign influence operations

Section 404 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 Analysis Center ("Center"). Section 404 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 404 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 405. Oversight of foreign influence in academia

Section 405 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 405 further requires the report to identify specific national security-related threats to research conducted at higher education institutions.

Section 406. Director of National Intelligence report on fifth-generation wireless network technology

Section 406 requires the DNI to submit a report on the threats to United States national security posed by 5G wireless network technology built by foreign companies. Section 406 further requires

the report to include threats to cybersecurity and cyber collection capabilities, as well as potential threat mitigation efforts, such as encryption and open-source technology. Section 406 requires the DNI to submit the report in unclassified form, with a classified appendix, if necessary.

Section 407. Annual report by Comptroller General of the United States on cybersecurity and surveillance threats to Congress

Section 407 requires the Comptroller General, in consultation with the DNI, Secretary of Homeland Security, and the Sergeant at Arms, to submit a report on cybersecurity and surveillance threats to Congress that includes statistics on targeted attacks or other incidents against United States Senators or their immediate families and staff.

Section 408. Director of National Intelligence assessments of foreign interference in elections

Section 408 requires the DNI, in consultation with other appropriate agencies, to conduct an assessment within 45 days following a United States election of any foreign government interference. Section 408 requires the assessment to include the nature, methods, persons involved, and responsible foreign entities. Section 408 further requires the DNI to submit the assessment to Congress and certain executive officials, and to make the assessment public (consistent with the protection of sources and methods) within 60 days after the election.

Section 409. Study on feasibility and advisability of establishing Geospatial-Intelligence Museum and learning center

Section 409 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.

Section 410. Report on death of Jamal Khashoggi

Section 410 requires the DNI, within 30 days of enactment, to submit to Congress an unclassified report on the death of Jamal Khashoggi, consistent with protecting sources and methods. Section 410 requires the report to include identification of those who carried out, participated in, ordered, or were otherwise complicit in, or responsible for, Mr. Khashoggi's death.

DIVISION B—INTELLIGENCE AUTHORIZATIONS FOR FISCAL YEARS 2018 AND 2019

TITLE I—INTELLIGENCE ACTIVITIES

Section 101. Authorization of appropriations

Section 101 lists the United States Government departments, agencies, and other elements for which the Act authorizes appropriations for intelligence and intelligence-related activities for Fiscal Year 2019. The bill deems authorized the funds already appropriated for Fiscal Year 2018.

Section 102. Classified Schedule of Authorizations

Section 102 provides that the details of the amounts authorized to be appropriated for intelligence and intelligence-related activities for Fiscal Year 2019 are contained in classified Schedule of Authorizations and that the classified Schedule of Authorizations shall be made available to the Committees on Appropriations of the Senate and House of Representatives and to the President.

Section 103. Intelligence Community Management Account

Section 104 authorizes appropriations for the Intelligence Community Management Account (ICMA) of the ODNI for Fiscal Year 2019.

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

Section 201. Authorization of appropriations

Section 201 authorizes appropriations in the amount of $514,000,000 for the CIA Retirement and Disability Fund for Fiscal Year 2019.

Section 202. Computation of annuities for employees of the Central Intelligence Agency

Section 202 makes technical changes to the CIA Retirement Act to conform with various statutes governing the Civil Service Retirement System.

TITLE III—GENERAL INTELLIGENCE COMMUNITY MATTERS

Section 301. Restriction on conduct of intelligence activities

Section 301 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 302. Increase in employee compensation and benefits authorized by law

Section 302 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 303. Modification of special pay authority for science, technology, engineering, or mathematics positions and addition of special pay authority for cyber positions

Section 303 provides an increased yearly cap for Science, Technology, Engineering, or Mathematics (STEM) employee positions in the IC that support critical cyber missions. Section 303 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 304. Modification of appointment of Chief Information Officer of the Intelligence Community

Section 304 changes the position of IC Chief Information Officer from being subject to presidential appointment to being subject to appointment by the DNI.

Section 305. Director of National Intelligence review of placement of positions within the intelligence community on the Executive Schedule

Section 305 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 306. Supply Chain and Counterintelligence Risk Management Task Force

Section 306 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 and counterintelligence risks. Section 306 further provides requirements for membership, security clearances, and annual reports.

Section 307. Consideration of adversarial telecommunications and cybersecurity infrastructure when sharing intelligence with foreign governments and entities

Section 307 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 308. Cyber protection support for the personnel of the intelligence community in positions highly vulnerable to cyber attack

Section 308 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 309. Modification of authority relating to management of supply-chain risk

Section 309 extends certain IC procurement authorities to manage and protect against supply chain risks. Section 309 further requires annual reporting on the IC's determinations and notifications made in executing these authorities.

Section 310. Limitations on determinations regarding certain security classifications

Section 310 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.

Section 311. Joint Intelligence Community Council

Section 311 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 312. Intelligence community information technology environment

Section 312 defines the roles and responsibilities for the performance of the Intelligence Community Information Technology Environment (IC ITE). Section 312 requires certain reporting and briefing requirements to the congressional intelligence committees regarding the IC's ongoing implementation of IC ITE.

Section 313. Report on development of secure mobile voice solution for intelligence community

Section 313 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 314. Policy on minimum insider threat standards

Section 314 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 315. Submission of intelligence community policies

Section 315 requires the DNI to make all ODNI policies and procedures available to the congressional intelligence committees. Section 315 also requires ODNI to notify the congressional committees of any new or rescinded policies.

Section 316. Expansion of intelligence community recruitment efforts

Section 316 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 IV—MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY

SUBTITLE A—OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Section 401. Authority for protection of current and former employees of the Office of the Director of National Intelligence

Section 401 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 402. Designation of the program manager-information sharing environment

Section 402 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 403. Technical modification to the executive schedule

Section 403 amends the Executive Schedule to make the Director of the National Counterintelligence and Security Center a Level IV position on the Executive Schedule.

Section 404. Chief Financial Officer of the Intelligence Community

Section 404 amends the National Security Act of 1947 by requiring the Chief Financial Officer of the IC to directly report to the DNI.

Section 405. Chief Information Officer of the Intelligence Community

Section 405 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 411. Central Intelligence Agency subsistence for personnel assigned to austere locations

Section 411 authorizes the Director of the CIA to approve, with or without reimbursement, subsistence to personnel assigned to an austere overseas location.

Section 412. Expansion of security protective service jurisdiction of the Central Intelligence Agency

Section 412 expands the security perimeter jurisdiction at CIA facilities from 500 feet to 500 yards.

Section 413. Repeal of foreign language proficiency requirement for certain senior level positions in the Central Intelligence Agency

Section 413 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 421. Consolidation of Department of Energy Offices of Intelligence and Counterintelligence

Section 421 amends the Department of Energy Organization Act to consolidate the offices of intelligence and counterintelligence into the DOE Office of Intelligence and Counterintelligence.

Section 422. Establishment of Energy Infrastructure Security Center

Section 422 establishes the Energy Infrastructure Security Center under the Department of Energy Office of Intelligence and Counterintelligence that will be responsible for coordinating intel-

ligence regarding the to the protection of U.S. energy infrastructure.

Section 423. Repeal of Department of Energy Intelligence Executive Committee and budget reporting requirement

Section 423 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 431. Plan for designation of counterintelligence component of the Defense Security Service as an element of intelligence community

Section 431 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 431 further mandates that the plan shall not address the DSS's personnel security functions.

Section 432. Notice not required for private entities

Section 432 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 433. Framework for roles, missions, and functions of Defense Intelligence Agency

Section 433 requires the Secretary of Defense and DNI to jointly develop a framework for the roles, missions, and functions of the DIA as an IC element and combat support agency.

Section 434. Establishment of advisory board for National Reconnaissance Office

Section 434 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 435 provides that the board shall terminate three years after the Director declares the board's first meeting.

Section 435. Collocation of certain Department of Homeland Security personnel at field locations

Section 435 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 V—ELECTION MATTERS

Section 501. Report on cyber attacks by foreign governments against United States election infrastructure

Section 501 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 501 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 502. Review of intelligence community's posture to collect against and analyze Russian efforts to influence the Presidential election

Section 502 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 502 further requires the review to include assessments of IC resources, information sharing, and legal authorities.

Section 503. Assessment of foreign intelligence threats to Federal elections

Section 503 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 503 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 504. Strategy for countering Russian cyber threats to United States elections

Section 504 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 504 further requires this strategy to include input from solicited Secretaries of State and chief election officials.

Section 505. Assessment of significant Russian influence campaigns directed at foreign elections and referenda

Section 505 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 foreign governments against such campaigns, and an assessment of the effectiveness of such foreign defenses and responses.

Section 506. Foreign counterintelligence and cybersecurity threats to Federal election campaigns

Section 506 requires the DNI, in coordination with the DHS Under Secretary for I&A and the Director of the FBI, to publish regular public advisory reports on foreign counterintelligence and cybersecurity threats to federal election campaigns before those elections take place. Additional information may be provided to the appropriate representatives of campaigns if the FBI Director and the DHS Under Secretary for I&A jointly determine that an election campaign for federal office is subject to a heightened foreign counterintelligence or cybersecurity threat.

Section 507. Information sharing with State election officials

Section 507 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 507 also requires the DNI to assist with sharing appropriate classified information about threats to election systems.

Section 508. Notification of significant foreign cyber intrusions and active measure campaigns directed at elections for Federal offices

Section 508 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 nonstate 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 nonstate person or group.

Section 509. Designation of counterintelligence officer to lead election security matters

Section 509 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 VI—SECURITY CLEARANCES

Section 601. Definitions

Section 601 provides definitions for terminology used throughout this Title.

Section 602. Reports and plans relating to security clearances and background investigations

Section 602 requires the interagency Performance Accountability Council (Council) to provide plans to reduce the background inves-

tigation inventory and best align the investigation function between the Department of Defense and the National Background Investigation Bureau. Section 602 further requires the Council to report on the future of the clearance process and requires the DNI to notify the appropriate committees upon determining requests to change clearance standards, and the status of those requests' disposition.

Section 603. Improving the process for security clearances

Section 603 requires the DNI to review the Questionnaire for National Security positions (SF–86) and the Federal Investigative Standards to determine potential unnecessary information required and assess whether revisions are necessary to account for insider threats. Section 603 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 604. Goals for promptness of determinations regarding security clearances

Section 604 requires the Council to implement a plan to be able to process 90 percent of clearance requests at the Secret level in thirty days, and at the Top Secret level in 90 days. 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 605. Security Executive Agent

Section 605 establishes the DNI as the government's Security Executive Agent, consistent with Executive Order 13467, and sets forth relevant authorities.

Section 606. Report on unified, simplified, Governmentwide standards for positions of trust and security clearances

Section 606 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 five to three tiers.

Section 607. Report on clearance in person concept

Section 607 requires the DNI to submit a report on a concept whereby an individual can maintain eligibility for access to classified information for up to three years after access may lapse.

Section 608. Budget request documentation on funding for background investigations

Section 608 requires the President to submit to Congress with the Fiscal Year 2020 budget request exhibits that identify resources allocated by each agency for processing background investigations and continuous evaluation initiatives, identified by each respective tier, exclusive of costs for adjudications.

Section 609. Reports on reciprocity for security clearances inside of departments and agencies

Section 609 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 609 further requires the DNI to submit an annual report summarizing reciprocity.

Section 610. Intelligence community reports on security clearances

Section 610 requires the DNI to submit a report on each IC element's security clearance metrics, segregated by Federal employees and contractor employees.

Section 611. Periodic report on positions in the intelligence community that can be conducted without access to classified information, networks, or facilities

Section 611 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 612. Information sharing program for positions of trust and security clearances

Section 612 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 613. Report on protections for confidentiality of whistleblower-related communications

Section 613 requires the Security Executive Agent, in coordination with the Inspector General of the Intelligence Community, to submit a report detailing the IC's controls used to ensure continuous evaluation programs protect the confidentiality of whistleblower-related communications.

TITLE VII—REPORTS AND OTHER MATTERS

SUBTITLE A—MATTERS RELATING TO RUSSIA AND OTHER FOREIGN POWERS

Section 701. Limitation relating to establishment or support of cybersecurity unit with the Russian Federation

Section 701 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 702. Report on returning Russian compounds

Section 702 requires the IC to submit to the congressional intelligence committees, within 180 days of enactment of the Act, both classified and unclassified reports on the intelligence risks of returning the diplomatic compounds-in New York, Maryland, and California-taken from Russia as a reprisal for Russian meddling in the 2016 United States presidential election. Section 702 also establishes an ongoing requirement for producing similar assessments for future assignment of diplomatic compounds within the United States.

Section 703. Assessment of threat finance relating to Russia

Section 703 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 703 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 704. Notification of an active measures campaign

Section 704 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 704 further requires that such notification must include information on any actions that the United States has taken to expose or halt such attempts.

Section 705. Notification of travel by accredited diplomatic and consular personnel of the Russian Federation in the United States

Section 705 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 706. Report on outreach strategy addressing threats from United States adversaries to the United States technology sector

Section 706 requires the DNI to submit a report to appropriate committees on the IC's and the Defense Intelligence Enterprise's outreach to United States non-government entities (including private businesses and academia), regarding the United States' adversaries' efforts to acquire critical United States infrastructure tech-

nology, intellectual property, and research and development information.

Section 707. Report on Iranian support of proxy forces in Syria and Lebanon

Section 707 requires the DNI to submit a report to appropriate congressional committees on Iranian support of proxy forces in Syria and Lebanon and the threat posed to Israel and other United States regional allies and interests.

Section 708. Annual report on Iranian expenditures supporting foreign military and terrorist activities

Section 708 requires the DNI to submit a report to Congress describing Iranian expenditures on military and terrorist activities outside the country.

Section 709. Expansion of scope of committee to counter active measures and report on establishment of Foreign Malign Influence Center

Section 709 amends a provision in the *Intelligence Authorization Act for Fiscal Year 2017* to expand the scope of the Committee to Counter Active Measures to add China, Iran, North Korea, and other nation states. Section 709 further requires DNI, in coordination with relevant IC elements, to submit to congressional intelligence committees a report on establishing a center to assess and disseminate foreign influence activities, including the desirability and barriers to such establishment.

SUBTITLE B—REPORTS

Section 711. Technical correction to Inspector General study

Section 711 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 712. Reports on authorities of the Chief Intelligence Officer of the Department of Homeland Security

Section 712 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 713. Report on cyber exchange program

Section 713 directs the DNI to submit a report, within 90 days of enactment of the Act, on the potential establishment of a voluntary cyber exchange program between the IC and private technology companies.

Section 714. Review of intelligence community whistleblower matters

Section 714 directs the Inspector General of the IC (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 715. Report on role of Director of National Intelligence with respect to certain foreign investments

Section 715 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 716. Report on surveillance by foreign governments against United States telecommunications networks

Section 716 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 717. Biennial report on foreign investment risks

Section 717 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 718. Modification of certain reporting requirement on travel of foreign diplomats

Section 718 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 719. Semiannual reports on investigations of unauthorized disclosures of classified information

Section 719 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 refer-

rals to the Department of Justice regarding unauthorized disclosures of classified information. Section 719 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 720. Congressional notification of designation of covered intelligence officer as persona non grata

Section 720 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 721. Reports on intelligence community participation in vulnerabilities equities process of Federal Government

Section 721 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 721 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 721 also requires the DNI to submit an annual report to the congressional intelligence committees with specified information on certain VEP metrics.

Section 722. Inspectors General reports on classification

Section 722 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 722 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 723. Reports on global water insecurity and national security implications and briefing on emerging infectious disease and pandemics

Section 723 requires the DNI to submit to the congressional intelligence committees a report every five years on the implications of global water insecurity on the United States' national security interests. Section 723 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 724. 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 724 amends a provision in the *Intelligence Authorization Act for Fiscal Year 2017*, instead requiring each IC element to submit an annual report to the congressional intelligence committees that lists each significant memorandum of understanding or other agreement entered into during the preceding fiscal year. Section 724 further requires each IC element to provide such documents if an intelligence committee so requests.

Section 725. Study on the feasibility of encrypting unclassified wireline and wireless telephone calls

Section 725 requires the DNI to complete a study and report on the feasibility of encrypting unclassified wireline and wireless telephone calls between personnel in the IC.

Section 726. Modification of requirement for annual report on hiring and retention of minority employees

Section 726 expands and clarifies current IC reporting requirements on diversity of IC personnel to include five prior fiscal years and to disaggregate data by IC element.

Section 727. Reports on intelligence community loan repayment and related programs

Section 727 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 728. Repeal of certain reporting requirements

Section 728 repeals certain intelligence community reporting requirements.

Section 729. Inspector General of the Intelligence Community report on senior executives of the Office of the Director of National Intelligence

Section 729 directs the IC IG to submit a report to the congressional intelligence committees regarding senior executive service staffing at the ODNI.

Section 730. Briefing on Federal Bureau of Investigation offering permanent residence to sources and cooperators

Section 730 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 731. Intelligence assessment of North Korea revenue sources

Section 731 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 732. Report on possible exploitations of virtual currencies by terrorist actors

Section 732 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 741. Public Interest Declassification Board

Section 741 reauthorizes the Public Interest Declassification Board administered by the National Archives for a term of ten years, expiring on December 31, 2028.

Section 742. Securing energy infrastructure

Section 742 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 742 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 742 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 742 further requires the Secretary, within two years of funding, to submit to the aforementioned 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.

Section 743. Bug bounty programs

Section 743 directs the Secretary of DHS, in consultation with the Secretary of Defense, to submit a strategic plan to implement bug bounty programs at appropriate agencies and departments of the United States Government. Section 743 further requires the plan to include an assessment of the "Hack the Pentagon" pilot program and subsequent bug bounty programs. Section 743 also requires the plan to provide recommendations on the feasibility of initiating bug bounty programs across the United States Government.

Section 744. Modification of authorities relating to the National Intelligence University

Section 744 provides the National Intelligence University with authorities that certain other Department of Defense educational institutions have regarding hiring faculty and accepting research grants, as well as establishing a pilot program for admission of private sector individuals.

Section 745. Technical and clerical amendments to the National Security Act of 1947

Section 745 makes certain edits to the National Security Act of 1947 as amended for technical or clerical purposes.

Section 746. Technical amendments related to the Department of Energy

Section 746 provides technical corrections to certain provisions regarding the Department of Energy's Office of Intelligence and Counterintelligence.

Section 747. Sense of Congress on notification of certain disclosures of classified information

Section 747 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 748. 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 748 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 748 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 749. Sense of Congress on WikiLeaks

Section 749 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.

COMMENTS RELATED TO DIVISION A

Comments related to Division A of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 relate to Fiscal Year 2020 and reflect the position of the Senate Select Committee on Intelligence (SSCI). Use of the term "Committee" refers to the SSCI.

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

The Committee has 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 shut-

downs, 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 ODNI, the Central Intelligence Agency (CIA), and IC elements within the 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 Committee had little to no insight into the effects of the shutdown on these and other important segments of the IC.

Therefore, the Committee directs 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 402 of Division B of the Act would amend IRTPA, so that the PM–ISE is subject to appointment by the 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 Committee finds it appropriate to reconsider the future of the PM–ISE's mission.

Therefore, the Committee directs 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 Committee encourages the DNI and the Director of the DIA to ensure that IC elements continue to forge tighter partnerships with leading universities and 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 Committee further believes 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 Committee directs 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 Committee remains concerned as to impediments for companies with appropriately cleared personnel to perform work for government entities and the effects of these impediments on IC access to innovation. 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 Committee directs 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 classified neutral facilities; 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 National Intelligence Program

Section 306 of Division A 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 Committee is 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 306 of Division A 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 Committee recognizes that security can be interpreted 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 306 of the Act, the Committee directs 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 Cooperation with the Government Accountability Office

The Committee believes the Government Accountability Office (GAO) adds significant value to the Committee's 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 Committee's own efforts to legislate on security clearance reform, including in this Act. The Committee expects 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 Committee.

Security Clearance Procedures and Rights to Appeal

Section 311 of Division A of the Act provides appeal rights and procedures for security clearance eligibility determinations. The Committee recognizes that, in the most exceptional circumstances,

national security considerations may still require denial of access and has set forth waivers accordingly. The Committee will closely monitor compliance with this provision, through the applicable reporting requirements, and consider a legislative remedy if abuses are found. This provision is not intended to impede agency decisions regarding access to classified information for a limited purpose or duration (e.g., regarding an election or one-time read-ins for a specific event or threat). The Committee does, however, expect agencies to keep Congress fully and currently informed of any limited purpose or duration uses. Finally, the Committee expects the DNI-level appeals panel to exercise judgment and review only those appeals for which the panel concludes have evidentiary and jurisdictional merit.

National Intelligence University

Section 312 of Division A of the Act prohibits the DNI and the Secretary of Defense from undertaking any activity to transfer the National Intelligence (NIU) out of the Defense Intelligence Agency (DIA) until certain criteria are met. The Committee has been closely watching the evolution of how the IC provides for advanced intelligence education. DIA has hosted an intelligence college since 1962, which has been regionally academically accredited since 1983. When the ODNI was created in the Intelligence Reform and Terrorism Prevention Act of 2004, it created a separate NIU under its auspices as a complement to DIA's intelligence effort. As a response to 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, recent analyses of DIA by the Secretary of Defense and the House Permanent Select Committee on Intelligence concluded that DIA would benefit from moving NIU elsewhere in the IC. The Committee believes transferring NIU now may be premature. It does not oppose transferring NIU to ODNI, but expects for NIU's academic health to be sound before a transfer occurs; that DoD remains intimately involved in NIU's governance; and that DoD personnel will readily attend and serve as faculty at an ODNI-led university. The Committee also intends for DoD to embrace NIU under ODNI and for it not to seek out recreation of an intelligence college.

Associate Degree Program Eligibility

The Committee is concerned that students enrolled in or who have graduated from Associate Degree programs have insufficient opportunities to gain employment in the IC. Therefore, the Committee directs 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 Committee also directs the ODNI to make information about these academic programs publicly available.

Exposing Predatory and Anticompetitive Foreign Economic Influence

The Committee is 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 Committee directs 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 national security-related value of requiring a 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 entity or person in the United States made 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.

COMMENTS RELATED TO DIVISION B

Division B of this Act is the result of SSCI's negotiations with the House Permanent Select Committee on Intelligence (HPSCI) and takes the form of a Joint Explanatory Statement (JES). As such, reference to "committees" refers to the SSCI and the HPSCI. The "Agreement" refers to the JES.

Management of Intelligence Community Workforce

The Committees repeat direction from the *Intelligence Authorization Act for Fiscal Year 2017* that Intelligence Community (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 Office of the Director of National Intelligence (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 report to accompany the *Intelligence Authorization Act for Fiscal Year 2017* directed the Director of National Intelligence (DNI) to review and consider changes to Intelligence Community Directive (ICD) 801 ("Acquisition") to reflect issuance in 2013 of ICD 731 ("Supply Chain Risk Management") and 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 congressional intelligence 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 National Reconnaissance Office (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 investigation into Russian meddling in the 2016 Presidential election and cooperation with the declassification process.

Supervisory Feedback as Part of Continuous Evaluation 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 evaluation 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 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 to "conduct independent reviews investigations, inspections, audits, and reviews on programs and activities within the responsibility and authority of the Director of National Intelligence" and to lead the IC's IG community in its activities. The Committees are concerned that this intent is not fully exercised by the IC IG and reiterates the Congress's intent that the IC IG's role be over all IC-wide activities in addition to the ODNI. To support this intent, the Committees have directed a number of requirements to strengthen the IC IG's role and expects full cooperation from all Offices of Inspector General across the IC.

The Committees also remain concerned about the level of protection afforded to whistleblowers within the IC and the level of insight congressional committees have into their disclosures. It is the Committees' expectation that all Offices of IG across the IC will fully cooperate with the direction provided elsewhere in the bill to ensure both the DNI and the congressional committees have more complete awareness of the disclosures made to any IG about any National Intelligence Program-funded activity.

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 encourages 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 Department of Defense (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 site, 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 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 productions. 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 day 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 well 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 the Fiscal Year 2019 dedicated to this analysis. 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 believes 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 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 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 413 of Division B of the Act, to engage with Virginia state and local law enforcement authorities to ensure that a memorandum of un-

derstanding, 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 719 of Division B of the Act requires all IC agencies to provide the congressional intelligence committees with a semiannual 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 justification(s) for the change.

Centers for Academic Excellence

The Committees commend the commitment demonstrated by ODNI's Centers for Academic Excellence (CAE) program managers, 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 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 CAE Program by increasing, to the fullest extent possible:

1. The number and racial and gender diversity of CAE interns;
2. The number of CAE academic institutions and their qualified internship candidates participating in the CAE Program; and
3. The number of IC elements that sponsor 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 Committees 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.

Improving Analytic Automation

The Committees continue to support IC and DoD efforts to gather, analyze, manage, and store large amounts of intelligence, surveillance, and reconnaissance (ISR) data from remote sources. One such effort is the NGA program called Expeditionary Large Data Object Repository for Analytics in Deployed Operations. Managing data by making information discoverable to analysts across the globe while reducing storage and analytical access costs are critical steps in the IC and DoD's efforts to leverage commercial best practices in big data analytics. While NGA is at the forefront of such efforts, the Committees are concerned by DoD and IC's slow pace in developing formal requirements for big data analytic capabilities.

The Committees understand DoD faces significant challenges in addressing combatant commanders' intelligence, surveillance, and reconnaissance (ISR) requirements, and DoD is investing in new collection capabilities that are producing growing volumes of data. However, investments in ground processing, automation, and alert functions have not kept pace. For example, wide area motion imagery collection capabilities have evolved with technology and are producing extremely valuable ISR data, but processing and integration of this data is labor intensive. DoD continues to struggle to apply commercially-available data analysis and machine learning capabilities. The Committees recognize that DoD's processing, exploitation and dissemination (PED) shortfalls cannot be addressed without integrating commercial data processing and access techniques, and automating as much of the PED workflow as possible.

Therefore, the Committees direct the Under Secretary of Defense for Intelligence (USD(I)), in coordination with the Secretary of the Army, Secretary of the Air Force, Secretary of the Navy, and the DNI, within 90 days of enactment of the Act, to brief the congressional intelligence and defense committees on efforts that allow for rapid adoption of data storage, access, and automated processing and machine learning technologies and techniques.

Project MAVEN

There has been exponential growth in the volume of data available for DoD intelligence professionals to manage, process, exploit, and disseminate. Analysts are in dire need of tools that will support simultaneous access to, and analysis of, data from a multitude of sources and disciplines.

The massive quantities of available digital data hold significant promise for improving data analytics, producing more actionable intelligence, and contributing to the employment of a more lethal force. It is critical that DoD invest in new technologies that will bring artificial intelligence, deep learning, and computer vision to streamline the process of object detection, identification, and tracking—and allow analysts to focus their valuable cognitive capacity on the hardest and highest priority problems.

The Committees believe Project MAVEN provides DoD with a critical path to the integration of big data, artificial intelligence, and machine learning across the full spectrum of military intelligence to ensure our warfighters maintain advantages over increasingly capable adversaries. Although DoD has taken tentative steps to explore the potential of artificial intelligence, big data, deep learning, and machine learning, the Committees believe Project MAVEN will accelerate DoD's efforts to turn the enormous volume of data available to analysts into actionable intelligence.

Therefore, the Committees direct the Secretary of Defense, in coordination with NGA and other relevant IC and DoD agencies, within 90 days of enactment of the Act, to brief the congressional intelligence and defense committees on Project MAVEN. Such briefing shall address:

1. Schedule and strategy for labeling classified and unclassified data;
2. Algorithm development, production, and deployment strategy;
3. Coordination of integration efforts with other DoD and IC elements;
4. Plan to implement the technologies developed by Project MAVEN technology throughout the defense intelligence enterprise;
5. Additional areas this technological advance can be implemented; and
6. Validated funding requirements and efforts that ensure spending practices are focused and efficient.

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

The Committees direct the Director of NGA, in coordination with the DNI, the Director of the CIA, and the Director of the NRO, within 90 days of enactment of the Act, to submit to the congressional intelligence and defense committees a briefing 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 briefing shall include:

1. Identification of any additional authorities 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.

Military Occupational Specialty-to-Degree Program

The Committees support the Military Occupational Specialty (MOS)-to-Degree program, which is an innovative framework that enables enlisted Marines to receive credits towards an associate's or a bachelor's degree while earning required MOS credentials. The program partners with colleges and universities to map a Marine's experience and training to equivalent credit, and provides Marines with an awareness of tuition assistance and scholarship programs to enable them to complete the remaining credits towards their degree. The Committees encourage the Marine Corps to expand the MOS-to-Degree program through further curriculum development and enhanced management of the program.

Therefore, the Committees direct the Marine Corps Intelligence Activity (MCIA), within 90 days of the enactment of the Act, to brief the congressional intelligence and defense committees on the Marine Corps' progress towards expanding the MOS-to-Degree program.

Unmanned Aircraft System Pilot Retention

The Committees support the Marine Corps' vision to grow a more diverse, lethal, amphibious, and middleweight expeditionary force by leveraging emerging technologies, particularly in the area of unmanned and manned-unmanned teaming. Additionally, the Committees are enthusiastic about the Marine Corps' efforts to equip operating forces down to the squad level with a Small Unit Remote Scouting System Family of Small Unmanned Aerial Systems (UAS) capable of operating in all weather conditions across the full spectrum of conflict. The Committees are also aware of the service's concept for a Marine Air Ground Task Force Unmanned Expeditionary (MUX) capability.

However, the Committees are concerned with the projected cost and delays associated with developing this new technology and believe the Marine Corps is ill-prepared to address the growing deficiency in expertise and the manpower challenges that will accompany expansion of the unmanned fleet. Based on observations of the Air Force's and Army's efforts, the Committees believe the Marine Corps' UAS programs will experience pilot and maintainer shortages based on inadequate training, lack of reliable equipment, and the absence of incentive.

Therefore, the Committees direct the Deputy Commandant of Aviation, within 120 days of enactment of the Act, to brief the congressional intelligence and defense committees on potential interim

solutions to the gap exposed by the long development time for MUX. Such briefing should also address the Marine Corps' UAS talent management plan, including a strategy for pilot retention and a plan to unify unmanned training that will build a base of instructors and encourage the professionalism of the community.

Remotely Piloted Aircraft Training Strategy

Referring to the directive language found in the committee report accompanying H.R. 2810, the House Armed Services Committee (HASC)-reported FY 2018 National Defense Authorization Act (NDAA) (H. Rept. 115–200), the Committees direct the Secretary of the Air Force, no later than 30 days after enactment of the Act, to brief the congressional intelligence and defense committees on the Air Force's approach to remotely piloted aircraft (RPA) aircrew training, with a particular focus on how the Air Force plans to field simulator capability and training capacity among active and reserve component units supporting RPA operations.

Wide-area Motion Imagery Intelligence Capability

Referring to the directive language found in the committee report accompanying H.R. 2810, the HASC-reported FY 2018 NDAA (H. Rept. 115–200), the Committees direct the Secretary of the Air Force no later than March 1, 2019, to provide to the congressional intelligence and defense committees a report that describes in detail the lifecycle weapon system sustainment and modernization strategy for maintaining an enduring wide-area motion imagery capability for the geographic combatant commanders.

MQ–4C Triton Unmanned Aircraft System

Referring to the directive language found in the committee report accompanying H.R. 2810, the HASC-reported FY 2018 NDAA (H. Rept. 115–200), the Committees direct the Secretary of the Navy, no later than 45 days after enactment of the Act, to brief the congressional intelligence and defense committees on MQ–4C mission execution and tasking, collection, processing, exploitation, and dissemination (TCPED) processes. The briefing shall include or explain:

1. A framework description of the manning, equipping, and training requirements for the MQ–4C system;
2. A description of the baseline architecture of the mission support infrastructure required to support MQ–4C operations;
3. How the Navy plans to support and execute the TCPED processes;
4. How the Navy plans to support flying operations from either line-of-sight or beyond-line-of-sight locations;
5. How many aircraft the Navy plans to dedicate annually to the ISR Global Force Management Allocation Process of the DoD; and
6. How many hours of collection the MQ–4C will be able to provide annually in each of the intelligence disciplines for combatant commanders.

E–8C Joint Surveillance and Target Attack Radar System

Referring to the directive language found in the committee report accompanying H.R. 2810, the HASC-reported FY 2018 NDAA (H.

Rept. 115–200), the Committees direct the Secretary of the Air Force, no later than March 1, 2019, to provide to the congressional intelligence and defense committees a report that explains in detail all aspects of how and when the Air Force will transition from legacy Joint Surveillance and Target Attack Radar System (JSTARS) aircraft capability to JSTARS recapitalization aircraft capability.

Acceleration of Increment 2 of Warfighter Information Network-Tactical Program

Referring to Section 111 of H.R. 2810, the HASC-reported FY 2018 NDAA, the Committees direct the Secretary of the Army, no later than January 30, 2019, to submit to the congressional intelligence and defense committees a report detailing potential options for the acceleration of procurement and fielding of the Warfighter Information Network-Tactical Increment 2 program.

Cost-benefit Analysis of Upgrades to MQ–9

Referring to Section 134 of H.R. 2810, the HASC-reported FY 2018 NDAA, the Committees direct the Secretary of Defense, in coordination with the Secretary of the Air Force, within 180 days of enactment of the Act, to provide the congressional intelligence and defense committees an analysis that compares the costs and benefits of the following:

1. Upgrading fielded MQ–9 Reaper aircraft to a Block 5 configuration; and
2. Proceeding with the procurement of MQ–9B aircraft instead of upgrading fielded MQ–9 Reaper aircraft to a Block 5 configuration.

Limitation on Divestment of U–2 or RQ–4 Aircraft

The Committees recognize that both piloted U–2 Dragon Lady and the remotely piloted RQ–4 Global Hawk fleets of aircraft provide essential and extremely sought after high-altitude airborne ISR capabilities for geographic combatant commanders. These platforms have been viewed as competitors for resources, with stakeholders trying to decide which should remain within the Air Force inventory for the long-term.

Although the U–2 and RQ–4 have differing attributes that may make one platform preferable depending on requirements, maintaining both platforms provides critical, complementary capabilities within DoD's portfolio of high-altitude ISR assets. Furthermore, retiring either aircraft would exacerbate an existing and significant capability shortfall in meeting combatant commanders' requirements.

The Committees expect the Secretary of the Air Force to continue current and future modernization efforts and upgrades for the U–2 and RQ–4 to increase capability, generate synergy, and foster commonality within the high-altitude airborne ISR portfolio. The Committees discourage the Secretary of the Air Force or the Chief of Staff of the Air Force from planning in the future or proposing to Congress any aircraft retirement that would create an ISR capability deficit or capacity shortfalls from existing levels until a sufficient replacement reaches full operational capability.

Therefore, referring to Section 1034 of H.R. 2810, the HASC-reported FY 2018 NDAA, the Committees direct that none of the

funds authorized to be appropriated by the Act, or otherwise made available for the DoD for any fiscal year before Fiscal Year 2024, may be obligated or expended to prepare to divest, place in storage, or place in a status awaiting further disposition of the possessing commander any U–2 or RQ–4 aircraft for the DoD. This prohibition shall not apply to an individual U–2 or RQ–4 aircraft that the Secretary of the Air Force determines, on a case-by-case basis, to be non-returnable to flying service due to any mishap, other damage, or being uneconomical to repair.

Nonconventional Assisted Recovery

Referring to Section 1053 of H.R. 2810, the HASC-reported FY 2018 NDAA, the Committees direct the Secretary of Defense, no later than March 1, 2019, to submit to the congressional intelligence and defense committees the written review and assessment of personnel recovery and nonconventional assisted recovery programs. The assessment shall include:

1. An overall strategy defining personnel recovery and nonconventional assisted recovery programs and activities, including how such programs and activities support the requirements of the geographic combatant commanders;
2. A comprehensive review and assessment of statutory authorities, policies, and interagency coordination mechanisms, including limitations and shortfalls, for personnel recovery and nonconventional assisted recovery programs and activities;
3. A comprehensive description of current and anticipated future personnel recovery and nonconventional assisted recovery requirements across the Future Years Defense Program, as validated by the Joint Staff; and
4. An overview of validated current and expected future force structure requirements necessary to meet near-, mid-, and long-term personnel recovery and nonconventional assisted recovery programs and activities of the geographic combatant commanders.

The Committees further direct the Comptroller General of the United States, within 90 days of the date on which the assessment is submitted, to submit to the congressional intelligence and defense committees a review of such assessment.

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 HASC-reported FY 2019 NDAA, the Committees direct the Chief Management Officer to provide a briefing to the congressional intelligence committees and the congressional armed services 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 Department'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 312 of Division B 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-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 404 of Division B 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 405 of Division B 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 411 of Division B 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 congressional intelligence 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 435 of Division B of the Act requires I&A to identify opportunities for collocation of I&A field officers and to submit to the congressional intelligence committees a plan for deployment.

Framework for Roles, Missions, and Functions of the Defense Intelligence Agency

The Committees commend the work of the USD(I) to answer a request in the *Intelligence Authorization Act for Fiscal Year 2017* (division N of Public Law 115–31) to review the roles and missions of the Defense Intelligence Agency (DIA). The Committees agree with the Under Secretary's finding identifying a gap in DoD coordination of the functions of the DIA, as a combat support agency (CSA) that is a member of the IC. The Director of the DIA reports to both the Secretary of Defense and the DNI; however, the agency lacks a framework to balance the resourcing and mission conflicts this bifurcated chain of command may occasionally cause.

Therefore, referring to directive language found in the committee report accompanying H.R. 5515, the HASC-reported FY 2019 NDAA, within 90 days of enactment of the Act, the Committees direct the Secretary of Defense, in collaboration with the DNI, to develop policies that outline the process to balance the missions under DIA's CSA role with the missions and functions assigned by the intelligence community. These policies must address a process for assigning and integrating any new missions assigned by the DoD or the IC. The Committees further direct the Secretary of Defense, in consultation with the DNI, to provide a briefing to the congressional intelligence committees and the congressional armed services committees not later than 60 days of enactment of the Act, on the plan to develop these policies.

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 congressional intelligence committees.

National Reconnaissance Office Contracting Restrictions

The Committees are concerned that NRO imposes unnecessary contractual restrictions that prohibit or discourage a contractor from contacting, meeting with, or providing information to the members or staff of the congressional intelligence committees. Therefore, the Committees direct NRO to eliminate any restrictions prohibiting or discouraging contractors from contacting, meeting with, or providing information to the congressional intelligence committees in all current and future contracts. Furthermore, the

Committees direct the NRO to provide a briefing to the congressional intelligence committees, within 60 days of enactment of the Act, regarding completion of the aforementioned direction.

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 congressional intelligence 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 congressional intelligence 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 Committee understands 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 Committee further understands 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 Committee directs 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 Bureau'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.

Foundational Intelligence Analysis Modernization

Referring to the directive language found in the committee report accompanying H.R. 5515, the HASC-reported FY 2019 NDAA, the Committees direct the Joint Staff Director for Intelligence, in coordination with the USD(I) and the Director of the DIA, to develop a plan within 60 days of enactment of the Act, to modernize systems used to provide foundational intelligence.

Further, the Committees direct the Joint Staff Director for Intelligence, in coordination with the DIA Director, to provide a briefing to the congressional intelligence committees and the congressional armed services committees, within 90 days after enactment of the Act, on such plan to modernize foundational intelligence systems. If a determination is made that a new system is required, the Committees expect the Battlespace Awareness Functional Capabilities Board to validate the requirements for any new system, and that the acquisition plan will follow best practices for the rapid acquisition and improvement of technology dependent systems.

Intelligence Support to Cyber Operations

Referring to the directive language found in the committee report accompanying H.R. 5515, the HASC-reported FY 2019 NDAA, the Committees direct the USD(I), in coordination with the DIA and the military services, to provide a briefing to the congressional intelligence committees and the congressional armed services committees, within 90 days after enactment of the Act, on intelligence support to cyber operations.

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 FY 2019 NDAA, the Committees direct the Director of DIA to provide a briefing to the congressional intelligence committees and the congressional armed services committees, within 90 days after enactment of the Act, 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 FY 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 committees and the congressional armed services 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 FY 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 congressional intelligence committees and the congressional armed services 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 FY 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.

Strengthening Oversight of the Military Intelligence Program Budget

In directive language found in the committee accompanying H.R. 5515, the HASC-reported FY 2019 NDAA, the House Committee on Armed Services directed the USD(I) to "review all of the Department's intelligence, counterintelligence, and related intelligence programs, projects, and activities supporting the Secretary's responsibilities and requirements." Regarding this review, the report expressed the House Committee on Armed Services' expectation that USD(I) would note that the House Committee on Armed Services believes resources for sensors integral to the function of weapon systems, sensors and systems developed for space and missile defense, and resources for activities and programs associated with Operational Preparation of the Environment and Nonconventional Assisted Recovery are in support of operational requirements, and should be excluded from designation to the MIP.

The Committees expect that USD(I), in addition to noting the belief of the House Committee on Armed Services, also will note the Committees' belief that:

1. Merely deeming certain resources to be "in support of operational requirements" is insufficient to exclude such resources from designation to the MIP; and that
2. The determination of whether to designate resources to the MIP involves a substantive examination, of whether such resources will be used for activities that are substantially similar, if not equivalent to, intelligence and intelligence activities.

Additionally, and referring to the directive language found in the committee report accompanying H.R. 5515, the HASC-reported FY 2019 NDAA, the Committees direct USD(I) to provide a briefing to the congressional intelligence committees and the congressional armed services committees, within 180 days of enactment of the Act, on the results of the USD(I) review directed by H.R. 5515, including how the review will result in clear guidance on designation of programs, projects, and activities to the MIP.

Intelligence Community Leave Policies

It is imperative that the federal government 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, including elements of the IC, must align such benefits to the fullest extent possible with those of leading U.S. private sector companies and other industrialized countries.

The Committees are concerned that IC elements may not have fully implemented revised advanced sick leave policies as outlined in the Presidential Memorandum Modernizing Federal Leave Policies for Childbirth, Adoption and Foster Care to Recruit and Retain Talent and Improve Productivity, dated January 15, 2015, or implemented them only partially. Among other things, the memorandum directs that, to the extent permitted by law, agencies shall offer 240 hours of advanced sick leave, at the request of an employee and in appropriate circumstances, in connection with the birth or adoption of a child or for other sick leave eligible uses.

Additionally, beyond the memorandum's requirements, the Committees also believe IC elements should actively be exploring ways to enhance their parental leave policies, to include paid parental leave.

Therefore, not later than 180 days after the date of enactment of the Act, the DNI shall submit a written report to the congressional intelligence committees on each IC element's implementation of the Memorandum's requirements with respect to parental leave. The report should be unclassified, but may contain a classified annex if necessary. At a minimum, such report shall:

1. Summarize each element's policies with respect to parental leave and related benefits;
2. Identify those elements fully in compliance with the Memorandum's requirements with respect to parental leave and other benefits described by the Memorandum;

3. Identify elements not in compliance with such requirements;

4. As applicable, note and evaluate the sufficiency of any claimed explanation from an IC element, as to why its policies do not yet fully comply with such requirements;

5. As applicable, identify a projected date, no later than 180 days after the report's submission, by which the Memorandum will be fully implemented by all IC elements; and

6. Describe any barriers identified by the Director or an element of the IC—including any legal and resource barriers—to the establishment, for each element of the IC, of a paid parental leave policy.

Section 307 of Division A of the Act includes a related provision, requiring the DNI to set a policy for the IC to make available 12 weeks of paid administrative leave in the event of birth of a child, including adoptive and foster parents. Section 307 of Division A further requires ODNI to submit a plan for implementation to the congressional intelligence committees within one year after enactment and directs implementation within 90 days thereafter.

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 believes that confronting foreign influence directed at the United States is of fundamental importance, and thus desires to engage in a close and regular dialogue with the FBI about the task force's activities.

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

Joint System Integration Lab Annual Briefing

The Joint System Integration Lab (JSIL) at Redstone Arsenal, Alabama enables testing of critical military intelligence capabilities, including unmanned aerial system (UAS) sensors, modeling and simulation, and integration between and among service UASs. The Committees seek to remain fully and currently informed about this important work.

Therefore, the Committees direct the JSIL, within 180 days of enactment and annually for two years thereafter, to brief the congressional intelligence and defense committees, on intelligence and intelligence-related activities conducted by the JSIL.

Management of the Centers of Academic Excellence in National Security Studies

The IC's CAE in National Security Studies program was established in 2004 to serve the mission-critical objectives of educating highly qualified students of diverse backgrounds and encouraging them to pursue careers in the IC. The ODNI has designated the DIA as the Executive Agent of the program.

In the past, the ODNI collected information about involvement in the CAE program by IC elements and educational institutions, as well as demographic (gender, minority, disability), educational, employment, and other data on the participating students. The ODNI reported this information to Congress in 2010 regarding the period covering 2004–2009. However, despite continuing Congressional interest in this program, the IC has apparently ceased collection and analysis of such data. More critically, ODNI and DIA informed the House Permanent Select Committee on Intelligence that the IC currently cannot provide statistical evidence as to whether, or to what extent, the CAE program is fulfilling its objectives.

Congress directed in Fiscal Year 2016 that ODNI establish a dedicated CAE summer internship program, but the first effort in summer 2017 did not yield the anticipated diversity of summer interns or robust participation of IC elements. The summer 2018 internship program also did not appear to be postured to demonstrate significant progress.

Accordingly, the Committees direct ODNI to serve as the Executive Agent for CAE on a permanent and non-delegable basis no later than six months into Fiscal Year 2019. In addition, the Committees direct ODNI to immediately resume collection and analysis of data necessary to evaluate the IC CAE's performance, to include educational, employment, diversity, and other data that was used to produce ODNI's 2010 report. Within 180 days of enactment of the Act, the Committees direct ODNI to submit a written report to the congressional intelligence committees containing this data from the 2016–2018 academic years, as well as metrics about the total number of students who participated in CAE courses, seminars, internships, or other events; the number of students designated as CAE scholars pursuing a certificate; and the number of CAE certificates awarded during this timeframe, with a demographic breakdown regarding diversity.

The Committees believe that the IC CAE program should undergo a fundamental review to determine what changes can be made to allow the program to achieve its intended objectives and has requested a review be conducted by the Government Accountability Office (GAO). Therefore, the Committees also direct the IC to fully cooperate with the GAO review.

Enhancing Automation at the National Geospatial-Intelligence Agency

The Committees strongly support efforts to leverage commercial advances in automation of imagery, 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 that have resulted in years of research into the issue, but limited operational gains during day to day imagery processing.

Therefore, the Committees direct NGA, in coordination with ODNI, within 90 days of enactment of the Act, to provide the congressional intelligence and defense committees with an updated plan to reduce manual processing of imagery, WAMI, FMV, and

SAR to improve information flow to users. The report shall also address:

1. NGA's strategy to leverage commercial advances;
2. The various geospatial intelligence 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 are 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 almost always 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 the Act, to brief the congressional intelligence committees, on its identification of all NGA developed software programs and explain why such programs are developed organically instead of leveraging commercially available products.

Critical Skills Recruiting for Automation

Although cutting edge sensors have provided the IC and DoD with exquisite imagery, WAMI, and FMV, 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 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 the 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.

Sensitive Compartmented Information Facilities

The Committees have become aware of several major impediments for companies with appropriately cleared personnel to perform work for agencies and organizations like the NRO and NGA. For example, businesses without ownership of a Sensitive Compartmented Information Facility (SCIF), which includes many small businesses, find it very difficult to perform classified work. Construction and accreditation of SCIF spaces may be cost-prohibitive for small business and non-traditional government contractors. Additionally, construction timelines often exceed the period of performance of a contract.

A modern trend for innovative and non-traditional government contractors is the increase use of co-working space environments. Additionally, public and private entities are partnering to create emerging regional innovation hubs to help identify technology solu-

tions 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 NRO and NGA, within 90 days of enactment of the Act, to brief the congressional intelligence committees on:

1. Potential approaches to allow for SCIF spaces to be certified and accredited outside of a traditional contractual arrangement;
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 classified neutral facilities; and
5. Any other opportunities to support companies with appropriately cleared personnel but without ownership of a SCIF effective access to a neutral SCIF.

Encouraging Innovation

The Committees are aware of and supports the NRO as it continues to pursue innovation and incorporate innovative technologies into many programs of record (POR). However, while the NRO is one of the more innovative leaders regarding government satellite matters, the NRO also struggles to leverage commercial and government research and development efforts and incorporate them in an effective and timely manner into PORs.

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

1. Opportunities that could expand innovation;
2. Any challenges for innovation; and
3. How innovative or new technologies are incorporated to support critical milestones for PORs.

Improving Use of the Unclassified Marketplaces

The Committees have become aware that a major impediment for companies to perform work for agencies and organizations like the NRO is the lack of postings on unclassified marketplaces, such as the unclassified ARC. Instead of posting data to unclassified marketplaces, NRO unclassified postings often refer to classified systems for critical, yet unclassified information. If the NRO is serious about embracing commercial innovation, unclassified marketplace postings should remain on unclassified systems.

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

Satellite Servicing

No later than one year after the date of the enactment of the Act, the DNI, in consultation with the Secretary of Defense, shall jointly provide the congressional intelligence and armed services committees upon request, a briefing detailing the costs, risks, and oper-

ation benefits of leveraging commercial satellite servicing capabilities for national security satellite systems. The briefing shall include:

1. A prioritized list (with a rationale) of the operational and planned assets of the IC 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.

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 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 encourages efficiencies and transparency in government reporting requirements related to security clearances to ensure appropriate accountability. Therefore, 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.

COMMITTEE ACTION

On May 14, 2019, a quorum being present, the Committee met to consider the bill and amendments. The Committee took the following actions:

Votes on amendments to the committee bill and the classified annex

By unanimous consent, the Committee made the Chairman and Vice Chairman's bill, together with the classified annex for Fiscal Year 2020, the base text for purposes of amendment.

By voice vote, the Committee adopted *en bloc* twelve amendments to the classified annex, as follows: (1) four amendments by Chairman Burr, and cosponsored by Vice Chairman Warner; (2) two amendments by Senator Feinstein; (3) two amendments by Senator Rubio (4) one amendment by Senator King; (5) one amendment by Senator Cotton; (6) one amendment by Senator Sasse; and (7) one amendment by Senator Bennet.

By voice vote, the Committee adopted *en bloc* ten amendments to the bill, as follows: (1) an amendment by Chairman Burr, and cosponsored by Vice Chairman Warner, to incorporate the *Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018 and 2019*; (2) an amendment by Chairman Burr, and cosponsored by Vice Chairman Warner, to modify the amount of CIA Voluntary Separation Pay; (3) an amendment by Vice Chairman Warner to implement paid parental leave for IC agencies; (4) an amendment by Vice Chairman Warner to establish a social media center for data sharing and analysis; (5) an amendment by Senator Rubio to provide oversight of foreign influence in academia; (6) an amendment by Senator Wyden, and cosponsored by Vice Chairman Warner, Senator Rubio, and Senator Bennet, to require a report on fifth-generation wireless network technology; (7) an amendment by Senator Wyden, and cosponsored by Senator Cotton, to require an annual GAO report regarding cybersecurity and surveillance threats to Congress; (8) an amendment by Senator Heinrich, and cosponsored by Senator Wyden and Senator Harris, to require DNI assessments of foreign interference in elections; (9) an amendment by Senator Heinrich to require periodic briefings on artificial intelligence and machine learning; and (10) an amendment by Senator Blunt, and cosponsored by Vice Chairman Warner, to require a study on establishing a geospatial-intelligence museum and learning center.

Senator Harris offered an amendment to the classified annex, and Vice Chairman Warner offered a second-degree amendment to Senator Harris's amendment. Both were withdrawn, pending future Committee consideration. On May 21, 2019, the Committee considered a revised second-degree amendment by Vice Chairman Warner to Senator Harris's amendment to the classified annex. By voice vote, the Committee adopted Vice Chairman Warner's second-degree amendment. By voice vote, the Committee adopted Senator Harris's amendment to the classified annex, as modified by Vice Chairman Warner's second-degree amendment.

By voice vote, the Committee adopted a second-degree amendment by Senator Collins to an amendment by Senator Wyden that required an unclassified report on the death of Jamal Khashoggi. The second-degree amendment included the phrase "consistent with protecting sources and methods." By a vote of 15 ayes and zero noes, the Committee adopted the amendment by Senator Wyden, as modified by the second-degree amendment by Senator Collins. The votes in person were as follows: Chairman Burr—aye; Senator Risch—aye; Senator Rubio—aye; Senator Collins—aye; Senator Blunt—aye; Senator Cotton—aye; Senator Cornyn—aye;

Senator Sasse—aye; Vice Chairman Warner—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Heinrich—aye; Senator King—aye; Senator Harris—aye; and Senator Bennet—aye.

Votes to report the committee bill

On May 14, 2019, the Committee voted to report the bill, as amended, by a vote of 15 ayes and zero noes. The votes in person or by proxy were as follows: Chairman Burr—aye; Senator Risch—aye; Senator Rubio—aye; Senator Collins—aye; Senator Blunt—aye; Senator Cotton—aye; Senator Cornyn—aye; Senator Sasse—aye; Vice Chairman Warner—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Heinrich—aye; Senator King—aye; Senator Harris—aye; and Senator Bennet—aye. By voice vote on May 21, 2019, the Committee unanimously voted to report the bill as further amended by Senator Harris's amendment to the classified annex, as modified by Vice Chairman Warner's second-degree amendment.

By unanimous consent, the Committee authorized the staff to make technical and conforming changes to the bill and classified annex.

COMPLIANCE WITH RULE XLIV

Rule XLIV of the Standing Rules of the Senate requires publication of a list of any "congressionally directed spending item, limited tax benefit, and limited tariff benefit" that is included in the bill or the committee report accompanying the bill. Consistent with the determination of the Committee not to create any congressionally directed spending items or earmarks, none have been included in the bill, the report to accompany it, or the classified schedule of authorizations. The bill, report, and classified schedule also contain no limited tax benefits or limited tariff benefits.

ESTIMATE OF COSTS

Pursuant to paragraph 11(a)(3) of rule XXVI of the Standing Rules of the Senate, the Committee deems it impractical to include an estimate of the costs incurred in carrying out the provisions of this report due to the classified nature of the operations conducted pursuant to this legislation. On May 23, 2019, the Committee transmitted this bill to the Congressional Budget Office and requested an estimate of the costs incurred in carrying out the unclassified provisions.

EVALUATION OF REGULATORY IMPACT

In accordance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee finds that no substantial regulatory impact will be incurred by implementing the provisions of this legislation.

ADDITIONAL VIEWS OF SENATOR WYDEN

The Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 includes four new provisions I added with the help of Vice Chairman Warner that represent an important step forward in assisting and protecting Intelligence Community whistleblowers. The first codifies an appeals process for Intelligence Community whistleblowers who have been the subject of reprisals. The second addresses what is currently a confusing set of disparate whistleblower processes and procedures across the Intelligence Community. This provision will assist whistleblowers by harmonizing those processes and procedures with an aim to maximizing transparency and whistleblower protections. The third allows the Intelligence Community Inspector General to track whistleblower complaints across the Intelligence Community, which will improve oversight and inform policies to ensure that investigations are conducted in a timely fashion and that whistleblowers are protected from reprisals. Finally, the bill includes a provision requiring a report and recommendations to ensure that Intelligence Community whistleblowers have access to attorneys with security clearances.

The bill also includes two important new amendments I introduced related to the security of communications. The first, which was co-sponsored by Senators Rubio, Warner, and Bennet, requires the DNI to provide an unclassified report on the national security implications of fifth-generation (5G) wireless technology built by foreign companies. I am particularly pleased that the report will include an assessment of possible mitigation approaches, including U.S. Government support for strong end-to-end encryption and open-source technology. This report will inform the Congress and the public as the country considers policy responses to this extremely serious and complicated national security challenge.

The bill also includes a new amendment I introduced with Senator Cotton to require the GAO to report annually on cybersecurity and surveillance threats against the U.S. Senate, including Senators and their staff and immediate family. This provision is part of a broader bipartisan effort to protect U.S. Senators' communication that is included in S. 890.

Finally, the bill includes a new amendment I offered with the support of Senators Heinrich, Harris, Feinstein, and Bennet. It requires the DNI to provide a public report identifying those who carried out, participated in, ordered, or were otherwise complicit in or responsible for the death of Jamal Khashoggi. This amendment, modified to add "consistent with protecting sources and methods" and passed by a unanimous vote, is intended to ensure that there is transparency and accountability for the Saudi murder of a U.S. resident and journalist.

I am concerned about a new provision related to the Intelligence Identities Protection Act (IIPA). In 2010, I worked to pass legislation to increase the penalties for violations of the IIPA. This bill, however, expands the bill so that it applies indefinitely, including to individuals who have been in the United States for decades and have become senior management or have retired. I am not yet convinced this expansion is necessary and am concerned that it will be employed to avoid accountability. The CIA's request that the Committee include this provision, which invoked "incidents related to past Agency programs, such as the RDI [Rendition, Detention and Interrogation] investigation," underscores my concerns.

The Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018 and 2019 (S. 3153, 115th Cong., 2d Sess.), which the Committee incorporated into this bill, includes eight additional provisions I offered. A description of those provisions, as well as my concerns about one provision in that bill, are included in S. Rept. 115–298.

CHANGES TO EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, the Committee finds that it is necessary to dispense with the requirement of paragraph 12 to expedite the business of the Senate.

○