**Calendar No. 477**

116TH CONGRESS
*2d Session*

SENATE

REPORT
116–233

# INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2021

JUNE 17, 2020.—Ordered to be printed

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

# R E P O R T

together with

# MINORITY VIEWS

[To accompany S. 3905]

The Select Committee on Intelligence, having considered an original bill (S. 3905) to authorize appropriations for fiscal year 2021 for intelligence and intelligence-related activities of the United States Government, the Intelligence 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 February 11, 2020, that the request for the National Intelligence Program (NIP) for Fiscal Year 2021 was $61.9 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 a classified annex to this report that contains a classified Schedule of Authorizations. The classified Schedule of Authorizations is incorporated by reference in the Intel-

ligence Authorization Act and has the legal status of public law. The classified annex is made available to the Committees on Appropriations of the Senate and the House of Representatives and to the President. It is also available for review by any Member of the Senate subject to the provisions of 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 Intelligence Authorization Act for Fiscal Year 2021 (the "Act") that was reported by the Committee.

### 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 2021.

*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 2021 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 2021.

### TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

*Section 201. Authorization of appropriations*

Section 201 authorizes appropriations for the CIA Retirement and Disability Fund for Fiscal Year 2021.

### 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. Clarification of authorities and responsibilities of National Manager for National Security Telecommunications and Information Systems Security*

Section 303 permits the National Manager for National Security Telecommunications and Information Systems Security, as designated by National Security Directive 42 (NSD–42), to delegate NSD–42 authorities to a Deputy National Manager, without further delegation. Section 303 further reinforces the National Security Agency's (NSA's) mission regarding authorities and funding programs by ensuring that the National Manager—when carrying out NSD–42 authorities—may supervise, oversee, or execute (directly or indirectly) the Information Systems Security Program (ISSP), but shall not supervise, oversee, or execute any aspect of the National Intelligence Program (NIP) or Military Intelligence Program (MIP), except as necessary to supervise, oversee, or execute the ISSP. Section 303 also provides that, upon such delegation of authority, the Deputy National Manager may supervise, oversee, or execute (directly or indirectly) the ISSP, but shall not supervise, oversee, or execute any aspect of the NIP or MIP, except as necessary to supervise, oversee, or execute the ISSP.

*Section 304. Continuity of operations plans for certain elements of the intelligence community in the case of a national emergency*

Section 304 requires the Directors of the Office of the Director of National Intelligence (ODNI), Central Intelligence Agency (CIA), National Reconnaissance Office (NRO), Defense Intelligence Agency (DIA), NSA, and National Geospatial-Intelligence Agency (NGA) to establish continuity of operations plans for use in the case of certain national emergencies as defined in statute, and share those with the congressional intelligence committees within 7 days of a national emergency being declared. Furthermore, Section 304 requires these agencies to provide the committees with any updates to those plans as the conditions of the national emergency require.

*Section 305. Application of Executive Schedule level III to positions of Director of National Security Agency and Director of National Reconnaissance Office*

Section 305 provides that the Director of the NRO and the Director of the NSA shall be designated as Level III on the Executive Schedule, the equivalent of an Under Secretary. The Committee recognizes that this provision does not affect the current Director of the NSA's military rank or pay. Section 305 is intended to provide the Committee's view as to the Director's stature in the interagency; it is not intended to signal support for a civilian nominee. The Committee further clarifies that this provision shall apply to a successor civilian occupying the position of Director of the NRO.

*Section 306. National Intelligence University*

Section 306 provides the National Intelligence University (NIU) with the authorities that the Department of Defense War Colleges have regarding faculty member hiring and compensation, and the acceptance of faculty research grants. Section 306 also sustains an

independent, external board of visitors to provide oversight of the NIU.

*Section 307. Requiring facilitation of establishment of Social Media Data and Threat Analysis Center*

Section 307 provides a requirement regarding Section 5323 of the *National Defense Authorization Act for Fiscal Year 2020* by requiring that the Social Media Data and Threat Analysis Center be established not later than 180 days after enhancement of this Act.

*Section 308. Data collection on attrition in intelligence community*

Section 308 requires the DNI to set standards and issue an annual report on the reasons why different categories of Intelligence Community (IC) employees separate from service or applicants to IC positions withdraw from the hiring process after they have been issued a conditional offer of employment. Data on workforce attrition should include demographics, specialties, and length of service. Such reasons may include an alternative job opportunity, a loss of interest in joining the IC, or the length of time to complete the clearance process.

*Section 309. Limitation on delegation of responsibility for program management of information-sharing environment*

Section 309 stipulates that the President must delegate responsibilities under Section 1016(b) of the *Intelligence Reform and Terrorism Prevention Act of 2004* to an official other than the ODNI on or after October 1, 2020.

*Section 310. Improvements to provisions relating to intelligence community information technology environment*

Section 310 streamlines current reporting requirements by requiring the Director of National Intelligence (DNI) to develop and maintain a long-term roadmap for the Intelligence Community Information Technology Environment (IC ITE). Section 310 further requires the DNI to develop and maintain a business plan to implement the long-term IC ITE roadmap.

*Section 311. Requirements and authorities for Director of the Central Intelligence Agency to improve education in science, technology, engineering, arts, and mathematics*

Section 311 ensures that the Director of the CIA has the legal authorities required to improve the skills in science, technology, engineering, arts, and mathematics (known as STEAM) necessary to meet long-term national security needs.

SUBTITLE B—INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY

*Section 321. Prohibition against disclosure of whistleblower identity as reprisal against whistleblower disclosure by employees and contractors in the intelligence community*

Section 321 adds to prohibited personnel practices a knowing, willful or negligent disclosure that reveals an IC Whistleblower's identifying information without consent. Section 321 further provides an IC Whistleblower with a private right of action if such dis-

closure is taken as a reprisal against the IC Whistleblower for bringing a complaint.

*Section 322. Clarification of standards regarding whistleblower complaints and information of urgent concern received by Inspector General of the Intelligence Community*

Section 322 clarifies the definition of "urgent concern" regarding whistleblower complaints and ensures that the Inspector General of the Intelligence Community (IC IG) has authority over determining whether a matter falls within the "urgent concern" definition.

*Section 323. Clarification regarding submittal of complaints and information by whistleblowers in the intelligence community to Congress*

Section 323 clarifies that IC Whistleblowers can give their complaints to the intelligence committees—as long as the complaint is provided to both Chairman and Vice Chairman or Ranking Member or designated nonpartisan staff—regardless of whether they are determined to be urgent concerns. Section 323 further provides new security protocols in the instances where complaints include classified information.

*Section 324. Limitation on sharing of intelligence community whistleblower complaints with persons named in such complaints*

Section 324 prohibits Federal government agents and employees from sharing an IC Whistleblower complaint that has been submitted to an IC element's IG with a named subject of the complaint, unless the IC Whistleblower provides written consent or information sharing is required as part of the investigation. Section 324 further provides that any violation is subject to criminal fines and/or two-year imprisonment and requires notification to the congressional intelligence committees.

SUBTITLE C—REPORTS AND ASSESSMENTS PERTAINING TO THE INTELLIGENCE COMMUNITY

*Section 331. Assessment by the Comptroller General of the United States on efforts of the Intelligence Community and the Department of Defense to identify and mitigate risks posed to the Intelligence Community and the Department of Defense by the use of direct-to-consumer genetic testing by the Government of the People's Republic of China*

Section 331 directs the Comptroller General to assess efforts in the IC and Department of Defense (DoD) to identify and mitigate the risks posed to the IC and DoD by direct-to-consumer genetic testing by the Government of the People's Republic of China. Section 331 further requires the report to include key national security risks and vulnerabilities, an assessment of the IC's and DoD's identification and mitigation of such risks and vulnerabilities, and recommendations for the IC and DoD to improve identification and mitigation of such risks and vulnerabilities.

*Section 332. Report on use by intelligence community of hiring flexibilities and expedited human resources practices to assure quality and diversity in the workforce of the intelligence community*

Section 332 requires the DNI to submit a report describing how IC elements are exercising hiring flexibilities and expedited human resources practices afforded under 5 U.S.C. § 3326 and related regulations, including the identification of any obstacles encountered by the IC in exercising such authorities.

*Section 333. Report on signals intelligence priorities and requirements*

Section 333 requires the DNI to submit a report detailing signals intelligence priorities and requirements subject to Presidential Policy Directive-28 that stipulates "why, whether, when, and how the United States conducts signals intelligence activities." This report shall be submitted in unclassified form, but may include a classified annex.

*Section 334. Assessment of demand for student loan repayment program benefit*

Section 334 requires the head of each IC element to calculate the number of personnel who qualify for a student loan repayment program benefit, and compare it to the number of personnel who apply for such a benefit. The information provided will include recommendations for how to optimize participation and enhance the effectiveness of the benefit as a retention tool, to identify any shortfall in funds or authorities needed to provide such benefit, and to include such materials with the budget request for Fiscal Year 2022.

*Section 335. Assessment of intelligence community demand for child care*

Section 335 requires the DNI in coordination with the heads of other IC elements to provide a report that includes: a calculation of the total annual demand for child care by employees at NSA, NGA, DIA, NRO, CIA, and ODNI; an identification of any shortfalls between demand and the child care support by these IC elements; an assessment of options for addressing any such shortfall; an identification of the advantages, disadvantages, security requirements, and costs associated with each option; a plan to meet, within five years after the date of the report, the demand for childcare, and an assessment of specific considerations that impact the alternatives available to these IC elements.

*Section 336. Open source intelligence strategies and plans for the intelligence community*

Section 336 requires the DNI in coordination with the heads of each IC element, to conduct a survey of the open source intelligence requirements, goals, investments, and capabilities for each element of the IC and to evaluate the usability of the Open Source Enterprise (OSE). Based on such findings, it further mandates the DNI shall develop, in coordination with the heads of each IC element, a strategy for open source intelligence collection, analysis, and production across the IC; create a plan for improving usability of the

OSE; and conduct a risk and benefit analysis of creating an independent open source center.

Using the findings above, Section 336 further requires the DNI to develop a plan for a centralized data repository of open source intelligence. Finally, it mandates the DNI develop a cost-sharing model that leverages the open source intelligence investments of each IC element for the beneficial use of the entire IC. It also requires the heads of ODNI, CIA, DIA, NGA, and NSA to jointly brief the congressional intelligence committees on the progress developing the aforementioned plans.

*Section 337. Plan for establishing an element of the intelligence community within the United States Space Force*

Section 337 requires the DNI and the Under Secretary of Defense for Intelligence and Security, in coordination with the Secretary of the Air Force and the Chief of Space Operations, to submit a plan for establishing an element of the IC within the United States Space Force.

TITLE IV—SECURITY CLEARANCES AND TRUSTED WORKFORCE

*Section 401. Exclusivity, consistency, and transparency in security clearance procedures, and right to appeal*

Section 401 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 and accountability, and ensure due process. Section 401 further codifies the right of government employees to appeal unfavorable eligibility determinations to an agency-level panel. Section 401 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 the panel finds valid cause.

*Section 402. Establishing process parity for security clearance revocations*

Section 402 requires an agency, in justifying an adverse security clearance or access determination against a whistleblower, to demonstrate by clear and convincing evidence that the agency would have made the same security clearance or access determination in the absence of the whistleblower's disclosure. Section 402 establishes parity in the legal standards applied to IC Whistleblower matters.

*Section 403. Federal policy on sharing of derogatory information pertaining to contractor employees in the trusted workforce*

Section 403 requires the DNI to issue a policy within 180 days of enactment that facilitates sharing of derogatory information the government obtains on cleared contractors (along with any mitigation measures put in place) with Federal contractor employers' chief security officers, to help companies maintain robust insider threat programs. The policy must comport with privacy rights,

allow individuals to verify the information, and stipulate that such sharing is only for purposes of security risk mitigation.

TITLE V—REPORTS AND OTHER MATTERS

*Section 501. Secure and trusted technology*

Section 501 establishes a Communications Technology Security and Innovation Fund to support the development and deployment of open standards-based compatible, interoperable equipment for fifth-generation wireless networks to create a more secure and diverse telecommunications vendor market. It also establishes a Multilateral Telecommunications Security Fund to support the adoption of secure and trusted communications technologies in key markets globally. Section 501 authorizes up to $750,000,000 for each fund and requires the administrators of each fund to provide annual reports to Congress detailing the use of proceeds.

Section 501 further requires the DNI to submit a report on political influence by adversarial nations within international forums that set standards for fifth-generation and future generations of wireless networks, including International Telecommunication Union (ITU), International Organization for Standardization (ISO), Inter-American Telecommunication Commission (CITEL), and 3rd Generation Partnership Project (3GPP). Section 501 also requires the DNI and Secretary of Defense to jointly submit a report on developing federal wireless network testbeds for development of fifth-generation technologies for U.S. military and dual-use applications using open interface standards-based compatible, interoperable equipment. This report should include an assessment of efforts by foreign governments to build wireless network testbeds for virtualized telecommunication technologies. Both reports shall be in unclassified form with a classified annex, if required.

*Section 502. Report on attempts by foreign adversaries to build telecommunications and cybersecurity equipment and services for, or to provide such equipment and services to, certain allies of the United States*

Section 502 requires the CIA, NSA, and DIA to submit to the congressional intelligence and armed services committees a joint report that describes the United States intelligence sharing and military posture in Five Eyes countries that currently have or intend to use adversary telecommunications or cybersecurity equipment, especially as provided by China or Russia, with a description of potential vulnerabilities of that information and assessment of mitigation options.

*Section 503. Report on threats posed by use by foreign governments and entities of commercially available cyber intrusion and surveillance technology*

Section 503 requires the DNI to submit a report to the congressional intelligence committees on the threats posed by foreign governments and foreign entities using and appropriating commercially available cyber intrusion and other surveillance technology.

*Section 504. Reports on recommendation of the Cyberspace Solarium Commission*

Section 504 requires the ODNI, Department of Homeland Security (acting through the Under Secretary of Homeland Security for Intelligence and Analysis), Department of Energy (acting through the Director of Intelligence and Counterintelligence of the Department of Energy), Department of Commerce, and DoD to report to Congress their assessment of the recommendations submitted by the Cyberspace Solarium Commission pursuant to Section 1652(j) of the *John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019*, and to describe actions that each agency expects to take to implement these recommendations.

*Section 505. Assessment of critical technology trends relating to artificial intelligence, microchips, and semiconductors and related supply chains*

Section 505 requires the DNI to complete an assessment of export controls related to artificial intelligence (AI), microchips, advanced manufacturing equipment, and other AI-enabled technologies, including the identification of opportunities for further cooperation with international partners.

*Section 506. Duty to report counterintelligence threats to campaigns*

Section 506 requires that Federal presidential campaigns must report to the Federal Bureau of Investigation (FBI) within one week any offers to contribute, donate, expend, disburse, or solicit as prohibited under 50 U.S.C. § 30121 by the following individuals: a foreign principal as defined in the Foreign Agent Registration Act; a person acting at the direction of a foreign principal; or a person included in the list of specially designated nationals or blocked person by the Treasury Department's Office of Foreign Asset Control. Section 506 further requires Federal campaigns to establish a policy to retain and preserve records related to reportable foreign contacts for not less than three years, and enacts criminal penalties for willful violations of this section.

*Section 507. Combating Chinese influence operations in the United States and strengthening civil liberties protections*

Section 507 provides additional requirements to annual reports in 50 U.S.C. § 3237(B) on Influence Operations and Campaigns in the United States by the Chinese Communist Party (CCP) by mandating an identification of influence operations by the CCP against the science and technology sector in the United States. Section 507 also requires the FBI to create a plan, in consultation with stakeholders outside the Intelligence Community to increase public awareness and detection of influence activities by the CCP. Finally, Section 507 requires the FBI, in consultation with the Assistant Attorney General for the Civil Rights and the Chief Privacy and Civil Liberties Officer of the Department of Justice, to develop recommendations to strengthen relationships with communities targeted by the CCP and to build trust with such communities through local and regional grassroots outreach.

*Section 508. Annual report on corrupt activities of senior officials of the Chinese Communist Party*

Section 508 requires the CIA, in coordination with the Department of Treasury's Office of Intelligence and Analysis and the FBI, to submit to designated congressional committees annually through 2025 a report that describes and assesses the wealth and corruption of senior officials of the Chinese Communist Party (CCP), as well as targeted financial measures, including potential targets for sanctions designation. Section 508 further expresses the Sense of Congress that the United States should undertake every effort and pursue every opportunity to expose the corruption and illicit practices of senior officials of the CCP, including President Xi Jinping.

*Section 509. Report on corrupt activities of Russian and other Eastern European oligarchs*

Section 509 requires the CIA, in coordination with the Department of the Treasury's Office of Intelligence and Analysis and the FBI, to submit to designated congressional committees and the Under Secretary of State for Public Diplomacy, a report that describes the corruption and corrupt or illegal activities among Russian and other Eastern European oligarchs who support the Russian government and Russian President Vladimir Putin, and the impact of those activities on the economy and citizens of Russia. Section 509 further requires the CIA, in coordination with the Department of Treasury's Office of Intelligence and Analysis, to describe potential sanctions that could be imposed for such activities.

*Section 510. Report on biosecurity risk and disinformation by the Chinese Communist Party and the Government of the People's Republic of China*

Section 510 requires the DNI to submit to the designated congressional committees a report identifying whether and how CCP officials and the Government of the People's Republic of China may have sought to suppress or exploit for national advantage information regarding the novel coronavirus pandemic, including specific related assessments. Section 510 further provides that the report shall be submitted in unclassified form, but may have a classified annex.

*Section 511. Report on effect of lifting of United Nations arms embargo on Islamic Republic of Iran*

Section 511 requires the DIA to submit to designated congressional committees a report on the Government of the Islamic Republic of Iran's plans to acquire military arms if the United Nations Security Council's resolutions' ban on arms transfers to or from the Government of the Islamic Republic of Iran is lifted, as well as the effects such arms acquisitions may have on regional security and stability.

*Section 512. Report on Iranian activities relating to nuclear nonproliferation*

Section 512 directs the DNI to submit a report on any relevant activities relating to nuclear weapons research and development by the Islamic Republic of Iran and any relevant efforts to afford or

deny international access to related facilities in accordance with international non-proliferation agreements.

*Section 513. Sense of Congress on Third Option Foundation*

Section 513 expresses the sense of Congress that the Third Option Foundation's work on behalf of the CIA's special operations community and their families is invaluable, such that the Director of the CIA should work with the Foundation to implement section 6412 of the *Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020*, which provided special rules for certain monthly workers' compensation payments and other payments to CIA personnel.

## COMMITTEE COMMENTS

*Equitable Treatment of Relocation Costs for Intelligence Community Civilians*

As demonstrated in The Intelligence Community Workforce Agility Protection Act of 2020, S. 3675, introduced by Senators Burr and Warner, the Committee strongly supports IC personnel who must make a permanent change of station to accept an IC position. The Committee recognizes such relocations pose significant financial hardships for the IC civilians who move their families to serve their country. Current law provides military members with exemptions from effective tax penalties for such relocations, but IC civilians have no similar exemptions, thus undermining the IC's ability to recruit and maintain a highly qualified and motivated workforce. The Intelligence Community Workforce Agility Protection Act of 2020 would provide equitable tax treatment for IC civilians who are subject to similar permanent change of station orders. The Committee looks forward to expeditious congressional action on this matter.

*Advanced Aerial Threats*

The Committee supports the efforts of the Unidentified Aerial Phenomenon Task Force at the Office of Naval Intelligence to standardize collection and reporting on unidentified aerial phenomenon, any links they have to adversarial foreign governments, and the threat they pose to U.S. military assets and installations. However, the Committee remains concerned that there is no unified, comprehensive process within the Federal Government for collecting and analyzing intelligence on unidentified aerial phenomena, despite the potential threat. The Committee understands that the relevant intelligence may be sensitive; nevertheless, the Committee finds that the information sharing and coordination across the Intelligence Community has been inconsistent, and this issue has lacked attention from senior leaders.

Therefore, the Committee directs the DNI, in consultation with the Secretary of Defense and the heads of such other agencies as the Director and Secretary jointly consider relevant, to submit a report within 180 days of the date of enactment of the Act, to the congressional intelligence and armed services committees on unidentified aerial phenomena (also known as "anomalous aerial vehicles"), including observed airborne objects that have not been identified.

The Committee further directs the report to include:

1. A detailed analysis of unidentified aerial phenomena data and intelligence reporting collected or held by the Office of Naval Intelligence, including data and intelligence reporting held by the Unidentified Aerial Phenomena Task Force;

2. A detailed analysis of unidentified phenomena data collected by:

a. geospatial intelligence;

b. signals intelligence;

c. human intelligence; and

d. measurement and signals intelligence;

3. A detailed analysis of data of the FBI, which was derived from investigations of intrusions of unidentified aerial phenomena data over restricted United States airspace;

4. A detailed description of an interagency process for ensuring timely data collection and centralized analysis of all unidentified aerial phenomena reporting for the Federal Government, regardless of which service or agency acquired the information;

5. Identification of an official accountable for the process described in paragraph 4;

6. Identification of potential aerospace or other threats posed by the unidentified aerial phenomena to national security, and an assessment of whether this unidentified aerial phenomena activity may be attributed to one or more foreign adversaries;

7. Identification of any incidents or patterns that indicate a potential adversary may have achieved breakthrough aerospace capabilities that could put United States strategic or conventional forces at risk; and

8. Recommendations regarding increased collection of data, enhanced research and development, and additional funding and other resources.

The report shall be submitted in unclassified form, but may include a classified annex.

*Coordination of Security for Domestic Military Installations and Other Facilities*

The Committee is concerned that, as a result of several recent incidents of attempted unauthorized access to Naval Air Station Key West and Fort Story, Virginia by Chinese nationals, several security vulnerabilities have been discovered. Foreign adversaries may be systematically probing military installations and facilities, and it is important that the Department of Defense take responsibility for ensuring security measures are adequate, unauthorized accesses are tracked, and uniform reporting requirements for attempted unauthorized accesses are established.

Therefore, the Committee directs the Under Secretary of Defense for Intelligence and Security (USD(I&S)), in coordination with the DNI and the Director of the FBI, to establish within the Office of the USD(I&S) a designee responsible for coordination of security for domestic military installations and other domestic military facilities. Specifically, the designee's responsibilities shall include tracking unauthorized incursions into domestic military installations and facilities and attempts at such incursions.

The Committee further directs that, within 180 days of enactment of this Act, such individual shall develop a strategy for security and counterintelligence collection that defines the capability requirements, responsibilities, and processes for security and counterintelligence for domestic military installations and other domestic military facilities. In addition, not less frequently than once each year, the Under Secretary shall, in consultation with the heads of other appropriate elements of the DoD and the IC, brief the intelligence and armed services committees on the:

1. Activities of the designee; and
2. Current and anticipated trends and developments in connection with security for domestic military installations and other domestic military facilities.

*Processing, Exploitation, and Dissemination Modernization and Integration Efforts of the Algorithmic Warfare Cross-functional Team of the Department of Defense*

The Committee is concerned with the intelligence silos that have resulted from isolated procurement programs that store data in individual repositories, each with its own set of cataloging procedures and proprietary technologies. This, in turn, potentially limits advantageous communications among databases, causes vital intelligence to go undetected, and causes duplication of separately-located analysts' efforts in reviewing other, less vital, intelligence information.

Therefore, the Committee directs the head of the Algorithmic Warfare Cross-Functional Team, as established in the Department of Defense by memorandum dated April 26, 2017, to submit to the congressional intelligence and armed services committees within 180 days of enactment of the Act, a report that includes:

1. Recommendations for the delineation of efforts between the Team and the Joint Artificial Intelligence Center, especially with respect to data labeling, testing and evaluation;
2. Recommendations for resource sharing across the intelligence community for test and evaluation as Project Maven transitions its independent lines of effort;
3. The plan of the Team to integrate unsupervised artificial intelligence algorithms (e.g., algorithms that learn from data without being trained, allowing the artificial intelligence to self-improve) into Project Maven;
4. The plan of the Team to incorporate independent data repositories located across the intelligence community, irrespective of the element providing the data or the domain they are resident to, into Project Maven; and
5. The plan of the Team to ensure that development of Processing, Exploitation, and Dissemination technology that will facilitate and enhance the capability of analysts to rapidly search across near real-time sensors, leverage historical data, and identify valuable intelligence is incorporated into the Defense Intelligence Agency Machine-assisted Analytic Rapid-repository System.

*Plan for Assessing Government Agency Counterintelligence Programs*

Adversary intelligence and security service efforts to monitor, access, penetrate, and/or manipulate government facilities, personnel, networks, and supply chains have become increasingly more sophisticated, as described in the National Counterintelligence Strategy of the United States. Many national security agencies, to include those in the DoD and IC, have mature and robust counterintelligence programs to preserve the integrity of their systems. However, many agencies' programs lag behind, either because they do not believe they are at risk or because of internal funding challenges. Therefore, the Committee directs the Director of the National Counterintelligence and Security Center to develop a plan within 90 days of enactment of this Act for assessing the effectiveness of all government agency counterintelligence programs. This plan should address the standards and methods of assessment that may apply for different categories of executive agencies; phasing of implementation over a five-year timeframe to cover all government counterintelligence; the periodicity for updated assessments; and annual costs to conduct these assessment and any recommendation for a cost recovery mechanism.

*Security Clearance Procedures and Rights to Appeal*

Section 401 of the Act provides appeal rights and procedures for security clearance eligibility determinations. 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 grants of access. Finally, the Committee expects the DNI-level appeals panel to exercise judgment and review only those appeals that the panel concludes have evidentiary and jurisdictional merit.

*Supporting Industry during Coronavirus*

Congress passed the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) in March 2020 to provide necessary assistance to the American economy during the coronavirus pandemic. An important element of that Act was Section 3610, which provided agencies authorities to modify contracts for companies supporting the government. This provision was critical to the defense industrial base. The Committee believes that consistent interpretation of Section 3610, particularly as it relates to work conducted at contractor facilities, cost reimbursement methodology, adjustments in payment plans, and adjustments in contract periods of performance, is essential to reducing uncertainty and sustaining a vibrant national security sector. The Committee looks forward to working with the IC elements in identifying if any additional authorities or resources are necessary and identifying lessons learned for any future national emergency.

*Efficient Use of Sensitive Compartmented Information Facilities*

The Committee is concerned that there are unnecessary challenges to the utilization of Sensitive Compartmented Information Facility (SCIF) spaces by multiple programs among IC and Depart-

ment of Defense components and their appropriately cleared government contractors. These challenges result in inefficient use of SCIFs and classified networks. The Committee finds that it is important to support collaboration and related efficiencies by sharing SCIF spaces.

Therefore, the Committee directs the DNI, in consultation with the Secretary of Defense, to issue, within 180 days after enactment of this Act, revised guidance authorizing and directing government agencies and their appropriately cleared contractors to process, store, use, and discuss sensitive compartmented information (SCI) at facilities previously approved to handle SCI, without need for further approval by agency or by site. This guidance shall apply to both IC-controlled access programs and DoD special access programs.

## COMMITTEE ACTION

On June 3, 2020, 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 Acting Chairman and Vice Chairman's bill, together with the classified annex for Fiscal Year 2021, the base text for purposes of amendment.

By voice vote, the Committee adopted *en bloc* three amendments to the classified annex, as follows: (1) a second-degree amendment by Acting Chairman Rubio; (2) an amendment by Acting Chairman Rubio; and (3) a second-degree amendment by Senator Sasse.

By voice vote, the Committee adopted *en bloc* five amendments to the bill, as follows: (1) an amendment by Senator Burr and cosponsored by Vice Chairman Warner, to improve provisions relating to the IC Information Technology Environment; (2) an amendment by Senator Risch and cosponsored by Senator King, to require reporting on Cyberspace Solarium Commission recommendations; (3) a second-degree amendment by Acting Chairman Rubio and cosponsored by Senators Risch, Blunt, Cotton, Cornyn, and Sasse, to improve Section 322; (4) an amendment by Senator Bennet and cosponsored by Vice Chairman Warner and Senators Cotton and Cornyn, to require an assessment of critical technology trends related to artificial intelligence; and (5) an amendment by Senator Cotton to require a report on Iranian activities relating to nuclear nonproliferation.

By voice vote, the Committee adopted an amendment by Senator Burr and cosponsored by Vice Chairman Warner, which provides the legal authorities required for the Director of the CIA to improve recruitment in the areas of science, technology, engineering, arts, and mathematics (known as STEAM) necessary to meet long-term national security needs.

By voice vote, the Committee adopted a second-degree amendment by Vice Chairman Warner and cosponsored by Senators Collins and Bennet, to an amendment by Vice Chairman Warner, and cosponsored by Senators Collins and Bennet, that requires Federal presidential campaigns to report to the FBI illegal offers of assistance by known foreign agents. The second-degree amendment exempted unpaid volunteers from such reporting requirements and

reduced the criminal penalties. By a vote of 8 ayes and 7 noes, the Committee adopted the amendment by Vice Chairman Warner, and cosponsored by Senators Collins and Bennet, as modified by the second-degree amendment. The votes in person were as follows: Acting Chairman Rubio—no; Senator Burr—no; Senator Risch—no; Senator Collins—aye; Senator Blunt—no; Senator Cotton—no; Senator Cornyn—no; Senator Sasse—no; Vice Chairman Warner—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Heinrich—aye; Senator King—aye; Senator Harris—aye; and Senator Bennet—aye.

By a vote of 7 ayes and 8 noes, the Committee did not adopt an amendment by Senator Wyden to establish the DNI as the Executive Agent for Federal government-wide declassification processes and requirements. The votes in person were as follows: Acting Chairman Rubio—no; Senator Burr—no; Senator Risch—no; Senator Collins—no; Senator Blunt—no; Senator Cotton—no; Senator Cornyn—no; Senator Sasse—no; 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 June 3, 2020, the Committee voted to report the bill, as amended, by a vote of 14 ayes and one no. The votes in person or by proxy were as follows: Acting Chairman Rubio—aye; Senator Burr—aye; Senator Risch—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—no; Senator Heinrich—aye; Senator King—aye; Senator Harris—aye; and Senator Bennet—aye.

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 of authorizations 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 June 8, 2020, 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.

## 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.

## MINORITY VIEWS OF SENATOR WYDEN

Despite its strong provisions, I voted against the Fiscal Year 2021 Intelligence Authorization Act because the legislation failed to reform a broken, costly declassification system. Years of reports, from the Information Security Oversight Office (ISOO) and the Public Interest Declassification Board (PIDB), have documented how a flood of digital classification has overwhelmed the federal government's obsolete declassification system. There is a consensus, inside and outside government, that the system is unsustainable.

The ISOO has determined that the cost of classification continues to increase and now exceeds $18 billion annually. A dysfunctional system that lets more and more classified records pile up wastes a significant portion of that amount, while undermining transparency and doing nothing to protect national security.

There is no dispute about the severity of the problem, nor about the solution—modernization of the declassification system. Senator Jerry Moran and I have introduced bipartisan legislation (S. 3733) to charge the Director of National Intelligence with modernizing declassification, a recommendation also made by the PIDB. I am disappointed that the Committee rejected efforts to adopt this commonsense bipartisan reform and address this ever-growing crisis.

The bill includes a number of important Intelligence Community whistleblower protection provisions, four of which were included at the behest of Vice Chairman Warner and myself. Those provisions protect from outside interference the Inspector General's determinations about what whistleblower complaints to submit to Congress, prohibit the public disclosure of whistleblowers' identities, prohibit whistleblower complaints from being shared with the subjects of those complaints, and provide a channel for whistleblowers to come directly to Congress without interference from the DNI.

Unnecessarily restrictive language was added to the provision facilitating direct whistleblower communications with Congress. The Intelligence Community Whistleblower Protection Act created a process for whistleblowers to communicate with the "intelligence committees," whereas the bill appears to limit such communication to the Chairman and Vice Chairman, or certain nonpartisan staff. To the extent the bill creates new limitations on efforts by whistleblowers to convey concerns to members of Congress, the language in the bill should be modified or clarified.

The bill includes a fifth whistleblower provision I proposed that protects whistleblowers whose security clearances are revoked or who face an adverse access determination by requiring that the government demonstrate by clear and convincing evidence that the agency would have made the same security clearance or access determination in the absence of the whistleblower's disclosure.

It also includes my provision requiring a report on the threat posed by the proliferation of commercial spyware as well as U.S. government efforts to counter that threat.

Finally, I am pleased that the Classified Annex requires a report with information that Senator Heinrich and I have been seeking related to collection conducted pursuant to Executive Order 12333.

RON WYDEN.

○