U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

SEP 17 2018

The Honorable Richard M. Burr
Chairman
The Honorable Mark Warner
Vice Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

This letter presents the views of the Department of Justice ("the Department") on S. 3153, the "Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018 and 2019." The Department of Justice looks forward to working with the Committees to address a number of constitutional and policy concerns, as explained below.

I. Constitutional Concerns

A. Restriction on Entering Into and Implementing Cybersecurity Executive Agreements

Section 701 would restrict the President's constitutional authority to enter into and implement an executive agreement with the Russian Federation relating to cybersecurity. The Department recommends that section 701 be deleted.

1. Section 701(b)(1) would provide that "[n]o amount may be expended by the Federal Government, other than the Department of Defense, to enter into or implement any bilateral agreement between the United States and the Russian Federation regarding cybersecurity, including the establishment or support of any cybersecurity unit, unless, at least 30 days prior to the conclusion of any such agreement, the Director of National Intelligence submits to the appropriate congressional committees a report on such agreement that includes the elements required by subsection (c)." Section 701(c) in turn would provide that the report "shall" include: "(1) The purpose of the agreement. (2) The nature of any intelligence to be shared pursuant to the agreement. (3) The expected value to national security resulting from the implementation of the agreement. (4) Such counterintelligence concerns associated with the agreement as the Director may have and such measures as the Director expects to be taken to mitigate such concerns."

In short, section 701(b)(1) would restrict the President from using non-Defense Department personnel and resources in the Executive Branch to "enter into" or to "implement" an executive agreement with the Russian Federation relating to cybersecurity. That restriction would interfere in multiple respects with the President's constitutional "authority to represent the United States and to pursue its interests outside the borders of the country," *The President's Compliance with the "Timely Notification" Requirement of Section 501(b) of the National Security Act*, 10 Op. O.L.C. 159, 160 (1986) ("*Timely Notification*"); *Am. Ins. Ass'n v. Garamendi*, 539 U.S. 396, 414–15 (2003), and with his constitutional authority as Commander in Chief.

First, "[t]he President's power over the conduct of diplomacy . . . includes exclusive authority to determine the individuals who will represent the United States in those diplomatic exchanges." *Unconstitutional Restrictions on Activities of the Office of Science and Technology Policy in Section 1340(a) of the Department of Defense and Full-Year Continuing Appropriations Act, 2011*, 35 Op. O.L.C. __, at *5 (Sept. 19, 2011) ("*OSTP*") (citations and internal quotation marks omitted). Congress thus may not limit the President to using personnel and resources from the Department of Defense to "enter into" an international agreement.

Second, the restriction on "enter[ing] into" a cybersecurity agreement with the Russian Federation is ambiguous as to its scope. If the act of "enter[ing] into" an international agreement were understood to encompass the acts of negotiating and finalizing the text of such an agreement, section 701(b)(1) would contravene the President's "exclusive constitutional authority to determine the time, scope, and objectives of international negotiations." *OSTP*, 35 Op. O.L.C. __, at *4. The President has the exclusive authority to negotiate and finalize such agreements as he sees fit, whether or not such an agreement is a sole executive agreement or would require the approval of the Senate (for treaties) or of Congress (for congressional-executive agreements). *See Acquisition of Naval and Air Bases in Exchange for Over-age Destroyers*, 39 Op. Att'y Gen. 484, 485–86 (1940).

Third, even if "enter into" were understood to refer solely to the act of causing an agreement in question to enter into force, Congress may not restrict the President's "enter[ing] into" or "implement[ing]" an executive agreement that constitutes the exercise of one of his exclusive Article II authorities. Restatement (Third) of the Foreign Relations Law of the United States, at 159, § 303(4) ("[T]he President, on his own authority, may make an international agreement dealing with any matter that falls within his independent powers under the Constitution."); *see, e.g.*, *United States v. Pink*, 315 U.S. 203, 229–30 (1942). Joint commitments to deploy government resources, military and otherwise, for the protection of cybersecurity would fall squarely within the President's exclusive authorities to command the armed forces and conduct foreign policy for the defense of the Nation. *See Placement of United States Armed Forces Under United Nations Operational or Tactical Control*, 20 Op. O.L.C. 182, 185 (1996); *Timely Notification*, 10 Op. O.L.C. at 159–60. The President also has exclusive

Article II powers over the control and dissemination of national security information, including information relating to cybersecurity. *Dep't of the Navy v. Egan*, 484 U.S. 518, 527 (1988); *see Whistleblower Protections for Classified Disclosures*, 22 Op. O.L.C. 92, 97 (1998) ("[S]ince the Washington Administration, Presidents and their senior advisers have repeatedly concluded that our constitutional system grants the executive branch authority to control the disposition of secret information."). Thus, if funding for cybersecurity were available in accounts other than those of the Department of Defense, the President would not require congressional authorization to use those funds to enter into or implement most cybersecurity agreements with the Russian Federation, nor could Congress restrict the President in doing so.

Congress accordingly may not require the Director of National Intelligence to report to Congress on the nature of these agreements as a precondition to entering into or implementing them, much less require the President to wait thirty days after the Director makes the report. Furthermore, certain of the information to be included in the report, such as "[t]he nature of any intelligence to be shared pursuant to the agreement" (section 701(c)(2)), would be "information bearing on national security," access to which is controlled by the President "as head of the Executive Branch and as Commander in Chief." *Egan*, 484 U.S. at 527. Congress may not mandate the disclosure of such information.

2. Section 701(b)(2) would additionally require that any cybersecurity agreement negotiated with Russia using Department of Defense funds be conducted in accordance with provisions of the National Defense Authorization Acts for Fiscal Year 2017 and 2018 that purport to prohibit the use of Fiscal Year 2017 and Fiscal Year 2018 funds "for any bilateral military-to-military cooperation between the Governments of the United States and the Russian Federation" until the Secretary of Defense certifies to Congress, among other things, that "the Russian Federation has ceased its occupation of Ukrainian territory and its aggressive activities that threaten the sovereignty and territorial integrity of Ukraine and members of the North Atlantic Treaty Organization." The Secretary may waive the certification requirement only if he notifies Congress that the waiver is in the national security interest of the United States, describes the national security interest covered by the waiver, and explains to Congress why he could not make the required certifications.

By restricting military-to-military contact or cooperation, including during wartime, these provisions that section 701(b)(2) would incorporate by reference infringe upon the President's constitutional authorities to command the armed forces and conduct diplomacy. *See* Statement on Signing the National Defense Authorization Act for Fiscal Year 2018, Daily Comp. Pres. Doc. No. DCPD201700906, at 2 (Dec. 12, 2017) (objecting to section 1231 of the National Defense Authorization Act for Fiscal Year 2018, which imposed one of the restrictions incorporated into section 701(b)(2), and stating that the Administration would treat this and other provisions "consistent with the President's exclusive constitutional authorities as Commander in Chief and as the sole representative of the Nation in foreign affairs"). The President's exclusive

constitutional authorities cannot be conditioned upon certifications or waivers made by subordinate Executive Branch officials. *See Over-age Destroyers*, 39 Op. Att'y Gen. at 590. And even assuming that the President could direct the exercise of the certification and waiver authorities by the Secretary of Defense, the conditions on exercise of those authorities would still unduly constrain the President's discretion. *See U.N. Tactical Control*, 20 Op. O.L.C. at 185–86 ("It might be argued that [a provision denying the use of appropriated funds to place U.S. armed forces under U.N. tactical control] does not impose a significant constraint on the President's constitutional authority because it grants the President the authority to waive the prohibition whenever he deems it in the 'national security interest' of the United States to do so . . . . Congress cannot, however, burden or infringe the President's exercise of a core constitutional power by attaching conditions precedent to the exercise of that power.").

3. Finally, "[t]hat Congress has chosen to invade the President's authority indirectly, through a condition on an appropriation, rather than through a direct mandate, is immaterial. Broad as Congress's spending power undoubtedly is, it is clear that Congress may not deploy it to accomplish unconstitutional ends." *U.N. Tactical Control*, 20 Op. O.L.C. at 186–87. For the reasons set forth, the funding restrictions in section 701 would be unconstitutional in most applications. The Department therefore recommends that section 701 be deleted.

B. National Security Information

Certain provisions of the bill would intrude on the President's constitutional prerogative to control the dissemination of "information bearing on national security." *Dep't of the Navy v. Egan*, 484 U.S. 518, 527 (1988). This prerogative includes determining when to withhold and when to disclose such information, as well as to whom. *See Access to Classified Information*, 20 Op. O.L.C. 402, 404 (1996) ("[A] congressional enactment would be unconstitutional if it were interpreted to divest the President of his control over national security information in the Executive Branch" (internal quotation marks omitted)).

The Department therefore recommends the following changes to the bill:

- Section 102(b)(3), restricting the circumstances under which the President may publicly disclose the classified Schedules of Authorization accompanying the Act, should be deleted.

- Section 310(a), providing that "[a]n officer of an element of the intelligence community who has been nominated by the President for a position that requires the advice and consent of the Senate may not make a classification decision with respect to information related to that officer," and section 310(b)(1), providing that "the classification decision with respect to information relating to the officer [nominated for

the position requiring Senate confirmation] shall be made by the Director of National Intelligence," should be deleted.

- Section 310(b)(2), providing that the classification decision with respect to information related to an officer nominated for the position of Director of National Intelligence "shall be made by the Principal Deputy Director of National Intelligence," should be deleted or made optional by changing "shall" to "may."

- Section 505(a)(1), providing that "the Director of National Intelligence shall support the Under Secretary of Homeland Security for Intelligence and Analysis . . . in sponsoring a security clearance up to the top secret level for each eligible chief election official of a State or the District of Columbia, and additional designees of such election official, at the time that such election official assumes such position," should be made optional by changing "shall" to "may."

- Section 505(b)(1), providing that "[t]he Director of National Intelligence shall assist the Under Secretary of Homeland Security for Intelligence and Analysis with sharing any appropriate classified information related to threats to election systems and to the integrity of the election process with chief election officials and such designees who have received a security clearance under subsection (a)," should be made optional by changing "shall" to "may."

C. Law Enforcement Information

Section 718 would require officials in the Executive Branch to report to Congress on the progress of investigations of the unauthorized disclosure of classified information. The information contained in investigative files are protected by the law enforcement component of executive privilege. *See Prosecution for Contempt of Congress of an Executive Branch Official Who Has Asserted a Claim of Executive Privilege*, 8 Op. O.L.C. 101, 117 (1984) ("Since the early part of the 19th century, Presidents have steadfastly protected the confidentiality and integrity of investigative files from untimely, inappropriate, or uncontrollable access by the other branches, particularly the legislature."); *Assertion of Executive Privilege in Response to Congressional Demands for Law Enforcement Files*, 6 Op. O.L.C. 31, 32–33 (1982) (same concerning civil law enforcement files of the Environmental Protection Agency). The Department would advise the President to treat the reporting requirements in section 718 in a manner consistent with his constitutional authority to maintain the confidentiality of information whose disclosure could risk compromising an investigation or otherwise threaten the integrity of the law enforcement process.

D. Legislative Recommendations

Section 712(b) would provide that the Secretary of Homeland Security "shall" submit a report to Congress "on the authorities of the Under Secretary" of Homeland Security for Intelligence and Analysis. Section 712(c)(1)(B) would provide that this report "shall include" the "legal and policy changes necessary to effectively coordinate, organize, and lead intelligence activities of the Department of Homeland Security." To avoid intruding on the President's authority to "recommend to [Congress's] consideration such Measures as he shall judge necessary and expedient," U.S. Const. art. II, § 3, the Department recommends inserting "if any" after "legal and policy changes."

II. Policy Concerns

Section 306: Supply Chain and Counterintelligence Risk Management Task Force

Section 306 of the bill would direct the Director of National Intelligence to "establish a Supply Chain and Counterintelligence Risk Management Task Force to standardize information sharing between the intelligence community and the acquisition community . . . with respect to counterintelligence risks." Section 306(b) sets forth the participants in the task force; however, the listing does not include the FBI. The FBI should be a member of any task force charged with preparing a report on the "identification of supply chain and counterintelligence risks."

Section 501: Report on Cyber Attacks by Foreign Governments against United States Election Infrastructure

Section 501(b) of the bill provides:

> Not later than 60 days after the date of the enactment of this Act, the Under Secretary of Homeland Security for Intelligence and Analysis shall submit to congressional leadership and the appropriate congressional committees a report on cyber attacks and attempted cyber attacks by foreign governments on United States election infrastructure in States and localities in connection with the Presidential election in the United States and such cyber attacks (or attempted cyber attacks) as the Under Secretary anticipates against such infrastructure.

The FBI and the Department of Homeland Security's Office of Intelligence and Analysis have lead roles in reporting threats to and cyber attacks against election infrastructure. Additionally, the Department of Homeland Security has the lead role in reporting on steps being taken to harden infrastructure and abate existing vulnerabilities. Therefore, we believe that the DHS Under Secretary for Intelligence & Analysis and the Director of the FBI should prepare the report jointly.

Sections 504 and 506: Election Matters

With regard to election-related matters, some of the new structures and requirements that the bill would establish are duplicative. We recommend reducing this duplication because competing structures and officials could generate confusion.

Section 504 would require the Director of National Intelligence, in coordination with the Secretaries of Defense, Homeland Security, State, and Treasury, and the directors of the FBI and the CIA, to develop a whole-of-government strategy for countering the threat of Russian cyber attacks against Federal, State, and local election systems, voter registration databases, voter tabulation equipment, and the like. Portions of this provision duplicate reporting requirements already existing for the annual report required by section 501 of the 2017 Intelligence Authorization Act and by section 1239A of the 2018 National Defense Authorization Act. Section 501 of the Intelligence Act requires the establishment of a committee and the production of an annual report on efforts to counter active measures by the Russian Federation to exert covert influence within the United States and abroad. Section 1239A of the Defense Act requires the development of a comprehensive strategy to counter the threat of malign influence by the Russian Federation.

Section 506 of the bill would require the Director of National Intelligence to designate a counter-intelligence officer from the National Counterintelligence and Security Center to "lead manage, and coordinate" counterintelligence matters relating to election security. This would include risks posed by interference from foreign powers to the supply chain, voting systems and software, voter registration databases, and critical infrastructure related to elections. Section 501 of the 2017 Intelligence Act already mandates a committee, and section 1239A of the 2018 Defense Act requires a comprehensive strategy. Moreover, the National Security Council staff, the Director of National Intelligence, the FBI, and the Department of Homeland Security already are leading several task forces and lines of effort to counter foreign influence operations. The designation of an additional official to lead another discrete effort related to election security might result in a duplicative coordination mechanism within the Executive Branch that could confuse, rather than clarify, lines of responsibility on this matter.

Additionally, as to section 504, we note that the scope of the strategy is unclear. The bill does not define "electoral process," "electoral systems," "cyber-attack," or "attempted cyber-attack." We believe that the section 504 does not clearly define roles of the Departments of State and Treasury.

Section 505: Information Sharing with State Election Officials

Section 505 of the bill provides for security clearances for and sharing Federal information with State election officials. Section 505(a)(2) would direct the Director of National Intelligence to provide interim clearances to election officials. The Department of Homeland Security already carries out this activity. In order to avoid confusion and duplication of effort, the Department of Homeland Security should be the entity responsible for this activity.

Section 505(b)(2) would require the Under Secretary of Homeland Security for Intelligence and Analysis to coordinate with the Director of National Intelligence when sharing information. We believe that section 505 also should require the Under Secretary to coordinate with the FBI before briefing state election officials on "classified information related to threats to elections systems and to the integrity of the election process."

Finally, the Department of Homeland Security's National Cybersecurity and Communications Integration Center shares classified threat information with Federal and non-Federal entities. Therefore, we recommend deleting from section 505 "Under Secretary of Intelligence and Analysis" and inserting instead "Secretary of Homeland Security".

Section 605: Security Executive Agent

Section 605 would assign certain responsibilities for security clearance functions to a "Security Executive Agent." It would also require that the Director of National Intelligence serve as the Security Executive Agent. We recognize that the bill attempts to mirror existing executive orders, but imposing similar requirements by statute raises serious policy concerns because it would deprive the President of future flexibility to assign and manage administrative responsibilities in these sensitive areas. *Cf. Egan*, 484 U.S. 518, 527 (1988) (noting the President's exclusive constitutional authority "to classify and control access to information bearing on national security"). Thus, we recommend amending subsection (a) by inserting before the final period ", unless otherwise determined by the President."

Section 703: Russian Threat Finance

Some of the reports that title VII of the bill (particularly section 703) would require may duplicate the existing requirement to develop a national strategy for combating terrorist and other illicit financing that already is set forth in title II, subtitle C., part 1 of the "Countering America's Adversaries Through Sanctions Act," P.L. No. 115-44, 131 Stat. 886, 934 *et seq.* (2017). The Department of the Treasury is in the process of updating the national money laundering and terrorist financing risk assessments and developing a proliferation risk assessment for weapons of mass destruction, as part of that illicit finance strategy. This proliferation risk assessment reaches beyond Russia and addresses the threats more generally.

Section 718: Seminannual Reports on Investigations of Unauthorized Disclosures of Classified Information

Section 718 of the bill would create new section of the National Security Act of 1947 and would provide:

> Not less frequently than once every 6 months, the Assistant Attorney General for National Security of the Department of Justice, in consultation with the Director of the Federal Bureau of Investigation, shall submit to the congressional intelligence committees, the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the House of Representatives a report on the status of each referral made to the Department of Justice from any element of the intelligence community regarding an unauthorized disclosure of classified information made during the most recent 365-day period or any referral that has not yet been closed, regardless of the date the referral was made.

We oppose section 718 and the proposed reporting requirements for unauthorized disclosures.

We are concerned that the information required to be reported necessarily would reveal information about ongoing criminal investigations. Specifically, the provision would require reporting on active investigations and whether there had been attribution. Disclosure of this information would damage ongoing investigations.

Further, the existence of a referral would confirm that the information in an article is actual intelligence community information. Many referrals contain specific compartmentalized information requiring special authorizations for anyone reading the information. For all of these reasons, these referrals are very sensitive.

Additionally, statistics about "open investigations" tend to be misleading since investigators sometimes open multiple investigations based on a single referral, or a single investigation based upon multiple referrals (and we sometimes consolidate investigations over their course). We note that we typically reveal only the total number of unauthorized disclosure referrals we receive annually, without further information. Moreover, the provision would apply both to "formal" and "informal" inquiries. If required to brief all investigative activity, regardless of investigative stage, the Assistant Attorney General and the Director of the FBI would need to expend the same resources reporting each lead of little or no ultimate value as it would spend reporting fully predicated and Department-authorized investigations.

Additionally, section 718 would create a new section 1105(a)(4) of the National Security Act of 1947. This proposed new provision would define an "unauthorized public disclosure of classified information." We recommend amending this definition so that it aligns more closely with Intelligence Community Directive 701. *See* https://www.dni.gov/files/documents/ICD/10-3-17_Atch1_ICD-701-Unauthorized-Disclosures_17-00047_U_SIGNED.pdf.

Finally, the intended meaning of a "substantiated" unauthorized disclosure is unclear and it is unclear whether the provision would require reporting investigations to determine whether an unauthorized disclosure had occurred at all.

Section 721: Vulnerability Equities Process

Section 721(c) of the bill would require the Director of National Intelligence to submit to the Congress an annual report containing data relating to "the interagency review of vulnerabilities, pursuant to the Vulnerabilities Equities Policy and Process document or any successor document." We note that some of the information that section 721 would require to be included in that report already is included in the annual VEP report.

Thank you for the opportunity to present our views. We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,

Prim Escalona

Prim F. Escalona
Principal Deputy Assistant Attorney General