



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

JAN 09 2018

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

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

Dear Mr. Chairman and Mr. Vice Chairman:

This letter presents the views of the Department of Justice (the Department) on S. 1761, the "Intelligence Authorization Act for Fiscal Year 2018." As to the general desirability of the bill, we defer to other agencies. However, the legislation raises numerous constitutional and policy concerns, as we explain below.

I. Constitutional Concerns

A. Section 102(b)(3): National Security Information

In certain circumstances, section 102(b)(3) could interfere with the President's control of national security information. That provision states that "[t]he President shall not publicly disclose the classified Schedule of Authorizations or any portion of such Schedule," except in enumerated conditions.

We object to this provision in its current form and recommend modifying it to confirm the President's constitutional authority to decide when to declassify and publicize national security information. If this provision were enacted in its current form, we would treat it consistently with the President's prerogatives in this area. *See Dep't of Navy v. Egan*, 484 U.S. 518, 527 (1988). This intended treatment would accord with the long-established position of the Executive Branch that the President has the exclusive authority to control the dissemination of national security information.

B. Section 402: National Security Information

Section 402 could be read to interfere with the President's control of national security information. Section 402(a)(1) would direct the Director of National Intelligence to "sponsor a security clearance up to the top secret level for each eligible chief election official of a State or the District of Columbia, and up to one eligible designee of such an election official, at the time that he or she assumes such position." Section 402(b)(1) provides that the Director "shall share 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)."

If this provision were understood to require the Director of National Intelligence to grant access to classified information to the specified individuals or to share any such information with them, it would contravene the President's constitutional "authority to classify and control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to occupy a position in the Executive Branch that will give that person access to such information." *Dep't of Navy v. Egan*, 484 U.S. 518, 527 (1988). However, we do not read the requirement to "sponsor" a security clearance as a mandate to grant such a clearance or otherwise to restrict the President's authority to determine whether any particular individual "sponsor[ed]" under this provision should or should not be granted access to classified information. We similarly understand the direction in section 402(b)(1) to share "appropriate" information to recognize, consistent with the President's constitutional authority to control the dissemination of national security information, that the President may determine that any or all of the information described should not be shared.

C. Section 616(b): Open Law Enforcement Files

In certain circumstances, section 616 could undermine the confidentiality of open law enforcement files. Section 616 would require the Assistant Attorney General for the National Security Division to submit to the congressional intelligence committees regular reports regarding unauthorized disclosures of classified information. Section 616(b) provides that each report shall include, among other information, information "indicating whether an open criminal investigation related to the referral is active," and a "statement indicating whether the Department of Justice has been able to attribute the unauthorized disclosure to a particular entity or individual."

We object to this provision and recommend modifying it to confirm the President's constitutional authorities in this area. In particular, we recommend the removal of section 616(b)(4) (requiring that the report include a "statement indicating whether an open criminal investigation related to the referral is active") and section 616(b)(5) (requiring that the report include a "statement indicating whether any criminal charges have been filed related to the referral"). If the provision were enacted in its current form, we would treat this reporting

requirement consistently with the longstanding policy of the Executive Branch to protect open law enforcement files from any breach of confidentiality, except in extraordinary circumstances. *See, e.g., Congressional Requests for Information from Inspectors General Concerning Open Criminal Investigations*, 13 Op. O.L.C. 77, 77 (1989) (“[W]hen . . . Congress seeks to obtain from an IG confidential information about an open criminal investigation, established executive branch policy and practice, based on consideration of both Congress’ oversight authority and principles of executive privilege, require that the IG decline to provide the information, absent extraordinary circumstances.”); *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.”).

We also would construe this reporting requirement to be consistent with the President’s constitutional authority to control the dissemination of national security information. *See Dep’t of Navy v. Egan*, 484 U.S. 518, 527 (1988) (noting the President’s authority under the Constitution “to classify and control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to occupy a position in the Executive Branch that will give that person access to such information”).

II. Policy Concerns

Section 306: Supply Chain and Counterintelligence Risk Management Task Force

Section 306(a) provides

The Director of National Intelligence shall establish a Supply Chain and Counterintelligence Risk Management Task Force to standardize information sharing between the intelligence community and the acquisition community of the Government of the United States with respect to the supply chain and counterintelligence risks.

Section 306(b) sets forth the membership of the task force. Notably, the membership does not include the FBI or the Department of Homeland Security as a standing member.

The FBI is the Government’s lead agency in counterintelligence and plays a pivotal role in counter-proliferation. This includes the sequence of acquisition. We recommend amending section 306(b) to include the FBI as a standing member of the task force.

Section 402: Information Sharing with State Election Officials

Section 402 of this bill would require the Director of National Intelligence to sponsor high-level security clearances for State officials and their designees and to provide “appropriate” classified information to cleared State officials. Even read narrowly (as described *supra* page 2, in our discussion of constitutional issues), this provision’s guidance to the Executive Branch runs contrary to the Government’s long-standing opposition to legislative or judicial involvement in the granting of security clearances, for example, to private parties in litigation, including the dissemination of classified information to parties or to their counsel in discovery. This provision would undermine the Government’s longstanding opposition to granting security clearances to private parties in litigation and to any subsequent dissemination of classified information to parties or their counsel in discovery. Our ability to rely upon this principle has been essential to our defense of, *inter alia*, cases seeking to challenge the Government’s authorities under the Foreign Intelligence Surveillance Act and the USA FREEDOM Act, the Government’s designations of foreign terrorist organizations, and the protection of aviation safety through the Terrorist Screening Database and no-fly list.

Significantly, section 402 does not appear to provide any discretion to the Executive Branch about the identity of those for whom security clearance is to be sponsored. Rather, it would permit the State officials — selected by operation of State law — to themselves designate an additional person to be sponsored. In contrast, the only statute employing parallel language to mandate that an Executive Branch official “sponsor” security clearances, 46 U.S.C.A. § 70107A, provides substantial latitude to the Executive Branch to “identify key individuals” for such clearances, and applies to individuals actively engaging in primarily law enforcement and security activities.

Further, section 402 does not appear to reflect that Executive Order 13526 governs the process of providing national security information to individuals. Thus, section 402 suggests that the Legislative Branch — and, potentially, the Judicial Branch — may adopt their own supplemental procedures governing how national security information is disseminated to State officials or private individuals. Legislation in this area should reflect that the dissemination of classified information is to be in accordance with established Executive Branch procedures such as Executive Order 13526.

Further, based upon our experience litigating classified national security issues, we believe that section 402 does not reflect an appreciation of the significant risks to national security that the broader distribution of classified information creates. As courts have recognized, it is an essential principle of protecting classified information that the risk of disclosure, both inadvertent and deliberate, rises when even one more person — regardless of who that person may be — is provided access to it. Here, section 402 would encourage the distribution of classified information to a large number of individuals whose jobs may not routinely involve the handling of law enforcement or national security information, who may not

be routinely provided with the security necessary to protect such information, and who may not be individuals best positioned to act upon the information (raising the possibility that State law may obligate them to encourage others to act). These elements magnify the risk of disclosure.

Significantly, the type of information that the drafters of section 402 anticipate sharing is likely to be information about the intentions and activities of significant national adversaries, including sophisticated foreign intelligence entities. Executive Branch information about their activities is likely to originate from some of the most sensitive and sophisticated intelligence sources and methods. Sharing this information, even with adequate safeguards, carries a risk of damage to those sources and methods. Moreover, information of these types of activities by foreign adversaries may be of such a nature that disseminating even our knowledge of the information, *e.g.*, a particular activity or plan, may be sufficient to reveal classified information about the nature and identity of a source or method that it is essential to protect. These issues will make it difficult for the Executive Branch to carry out the apparent purpose of the legislation while adequately protecting national security.

Section 504: Working Group to Evaluate Program Standards and Develop Strategy

Section 504 would require the Director of Intelligence and Counterintelligence of the Department of Energy to establish a working group to study technology platforms and standards developed to isolate and defend the most critical industrial control systems (as defined in section 502(4)(B)) from security vulnerabilities and exploits, and to develop a cyber-informed engineering strategy to accomplish this. Section 504(b) sets forth the membership of the working group. The membership does not include the FBI. We recommend amending section 504(b) to include a cleared representative of the FBI in the membership of the task force.

Section 507: Exemption from Disclosure of Shared Energy Infrastructure Information

Section 507(2) of the bill provides that

information shared by or with the Federal Government or a State, tribal, or local government under this title shall be . . . exempt from disclosure under any provision Federal, State, tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring the disclosure of information or records.

This appears to be an attempt to create an Exemption 3 statute under the Freedom of Information Act (FOIA), *see* 5 U.S.C. § 552(b)(3), for shared energy infrastructure information. While section 507(2) expressly references the FOIA, it does not cite specifically 5 U.S.C. § 552(b)(3)(B) of the Act. Because section 507(2) does not include an express reference to 5 U.S.C. § 552(b)(3)(B), the Intelligence Authorization Act for Fiscal Year 2018 would not qualify

as an Exemption 3 statute under the FOIA, and could not be used as a basis to withhold records responsive to a FOIA request.

Section 602: Responsibilities for Security Clearance Suitability and Fitness

Section 602 would assign certain responsibilities for suitability and security clearance functions to a "Suitability Executive Agent," "Credentialing Executive Agent," and "Security Executive Agent," each of whom would also serve on an interagency "Security, Suitability, and Credentialing Council." Section 602 would also require that the Director of the Office of Personnel Management (OPM) serve as both the Suitability Executive Agent and the Credentialing Executive Agent, and that the Director of National Intelligence serve as the Security Executive Agent. In our view, specifying that only the Director of OPM and the Director of National Intelligence may serve in those roles raises serious policy concerns. We recognize that the bill attempts to mirror existing executive orders, but imposing similar requirements by statute would deprive the President of future flexibility to assign and manage administrative responsibilities in these sensitive areas. *Cf. Dep't of Navy v. 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 deleting section 602 in its entirety. Alternatively, we recommend amending subsections (b)(1), (c)(1), and (d)(1) by inserting before the final period " , unless otherwise determined by the President." For similar reasons, we also recommend including the same clause as lead-ins to subsections (a)(2)(A) and (a)(3), so that the President would have express authority to alter the membership of the Council and its assigned duties.

In addition, in section 602(b)(2)(F), we recommend amending "Shall, pursuant to section 1104 of title 5, United States Code, prescribe performance" to state the following: "To prescribe, pursuant to section 1104 of title 5, United States Code, performance". This alteration would make the provision grammatically correct and would conform paragraph (F) to paragraphs (A)-(E).

Section 604: Reports on the Vulnerability Equities Policy and Process of the Federal Government

Section 604 of the bill would require the head of each element of the intelligence community to submit a report to the intelligence committees detailing the process and criteria the head uses for determining whether to submit a vulnerability for review under the vulnerability equities policy and process of the Federal Government. This provision would impose an unnecessary burden on the intelligence community and duplicate the process and criteria already set forth in the Vulnerability Equities Process (VEP) charter and policy followed by the intelligence community and other VEP members. The VEP charter was recently approved and released publicly, which will result in further transparency and clarity of both the process and the

criteria considered. Requiring each member of the intelligence community to submit its own report on the process and criteria would duplicate the governing policy itself.

We also recommend reconciling the reporting requirements in section 604 with any other reporting requirements in the VEP policy (or in other proposed legislation) in order to avoid the duplication of effort. Further, although we favor and, in fact, have promulgated and publicly released an unclassified VEP *policy*, we believe that policy makers must be very cautious in crafting the scope and classification of annual reporting requirements about the *day-to-day activities* of the VEP. Transparency regarding, *e.g.*, the overall number of vulnerabilities submitted, disseminated, and restricted by the VEP is an appropriate goal. However, it would be harmful to set forth additional or granular detail — whether in isolation or in the aggregate — that could educate an adversary about, *e.g.*, the number, nature and existence of restricted vulnerabilities, or methods and capabilities of our intelligence and law enforcement agencies. Although we support reporting on the overall, aggregate number of vulnerabilities submitted, disseminated, and restricted by the VEP, we would object to any unclassified or public reporting of, *e.g.*, the number of vulnerabilities involving or disclosed to a particular vendor. Moreover, publicly highlighting which vulnerabilities have been patched or mitigated by a vendor (and which have not) could educate our adversaries and malicious cyber actors about a particular attack vector to exploit. We believe it critical to protect unsophisticated citizens from victimization resulting from criminal cyber intrusions and attacks. Highlighting vulnerabilities that have not been subject to meaningful mitigation or patching by a vendor could result in this kind of victimization.

Section 606: Report on Cyber Attacks by Foreign Governments against United States Election Infrastructure

Section 606 would require the Under Secretary of Homeland Security for Intelligence and Analysis to submit to the intelligence committees a report on cyber attacks by foreign governments on United States election infrastructure related to the 2016 presidential election and/or anticipated in the future. We understand that the Department of Homeland Security (DHS) believes this provision raises significant concerns and should be stricken. DHS works with non-Federal entities on a voluntary basis, and there are no Federal requirements to report incidents to DHS. Legislation forcing DHS to violate the trust-based relationships it has developed with affected entities would signal that DHS could not keep its commitments to protect sensitive identifying information and would damage more than DHS's future work on elections. It would undermine the trust that DHS has been working to establish with all critical infrastructure entities, and discourage current and would-be partners from reporting incidents and working with DHS in the future. The loss of voluntary cyber incident reporting would compromise DHS's ability to receive early warning of emerging cyber incidents, alert government and private sector partners, and develop effective countermeasures. At a minimum, we recommend amending section 606 to (1) exempt reporting that might compromise the integrity of any potential or ongoing Federal criminal investigation; and (2) protect sensitive

identifying information that could damage DHS's efforts to increase voluntary cyber incident reporting.

Section 607: Report on Collection and Assessments Related to Russian Efforts to Interfere in United States Elections

Section 607 would require the Director of National Intelligence to submit to the intelligence committees a report on United States intelligence collection and assessments related to efforts by the Government of Russia to interfere with the 2016 United States presidential election. We recommend amending section 607 to exempt reporting that might compromise the integrity of any potential or ongoing Federal criminal investigation.

Section 608: Assessment of Foreign Intelligence Threats to Federal Elections

Section 608 would require the Director of National Intelligence, in consultation with various Government officials and not later than 180 days before any regularly scheduled Federal election, to submit to the intelligence committees and to congressional leadership a report on the security vulnerabilities of State election systems and an assessment of foreign intelligence threats to that election. We recommend amending section 608 to exempt reporting that might compromise the integrity of any potential or ongoing Federal criminal investigation.

Section 609: Strategy for Countering Russian Cyber Threat to United States Elections

Section 609 of the bill would require the Director of National Intelligence, in consultation with various Government officials to "develop a whole-of-government strategy for countering the threat of Russian cyber attacks and attempted cyber attacks against electoral systems and processes in the United States." We recommend amending section 609 to exempt reporting that might compromise the integrity of any potential or ongoing Federal criminal investigation. Additionally, the list of officials to be consulted includes the Director of the Federal Bureau of Investigation. We recommend that the list include the Attorney General.

Section 612: Assessment of Russian Money Laundering Threat

Section 612 of the bill would require the Director of National Intelligence, in coordination with the Secretary of the Treasury, to submit to the intelligence committees an all-source assessment of the threat to the United States posed by Russian money laundering. We support the fundamental objective of section 612. We recommend a number of definitional and linguistic suggestions to improve the provision.

First, there are several agencies — beyond the Department of the Treasury — likely to have information useful to the Director of National Intelligence in preparing the assessment. We recommend amending section 612 to require that the Director of National Intelligence coordinate

or consult with additional agencies, *e.g.*, the Department of Justice and the Department of Homeland Security, when carrying out the assessment.

Second, section 612(b)(1) would require that the assessment address “[m]oney laundering in the Russian Federation, global nodes of money laundering used by Russian and associated entities, and the entry points of money laundering by Russian and associated entities into the United States.” Other subsections also refer to Russian money laundering, but the concept is not defined. We believe that it may be helpful to define Russian money laundering for purposes of the assessment, perhaps in section 612(a).

Third, section 612(b)(2) would require that the assessment include information on the “[v]ulnerabilities to money laundering in the United States financial and legal system, including specific sectors, and ways in which Russian money laundering has exploited those vulnerabilities.” This phrasing suggests that the assessment would have to include *all* such vulnerabilities — not just those vulnerabilities exploited by Russian money launderers. It might be helpful to clarify this language to reflect that the assessment cover only the latter.

Fourth, section 612(b)(3) would require that the assessment include information about “[a]ny connections between Russian oligarchs and elements of Russian organized crime involved in money laundering and the Government of Russia.” The editing of this language leaves unclear to which “connections” the drafters intend to refer: Should the assessment address connections between oligarchs and organized crime, or connections between oligarchs and organized crime, on one hand, and the Russian government on the other? We recommend clarifying the language. We also recommend including in section 612 a definition of “oligarch.”

Sec. 616: Semiannual report on Intelligence Community Referrals to the Justice Department Regarding Unauthorized Disclosure of Classified Information

Section 616 would require the Department of Justice to submit semiannual reports to the intelligence committees on referrals it receives from members of the intelligence community concerning the unauthorized disclosure of classified information. It would require the reports to reflect the progress of investigations and decisions on whether or not to file charges.

We understand the intelligence committees’ interest in the handling of these cases. The Department of Justice takes the investigation and prosecution of these disclosures very seriously. However, reporting the progress of investigations and decisions on whether to prosecute would interfere with prosecutorial discretion and could severely impede and interfere with ongoing counterintelligence investigations. We strongly recommend amending this provision to limit reporting to relevant convictions only.

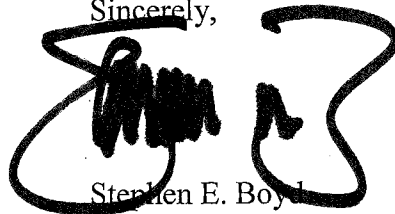
The Honorable Richard M. Burr
The Honorable Mark Warner
Page 10

Section 618: Biennial Report on Foreign Investment Risks

Section 618 would require the Director of National Intelligence to establish an interagency working group to prepare a biennial report on foreign investment risks and to submit the report to the intelligence committees. This proposal might duplicate efforts already undertaken by the Committee on Foreign Investment in the United States (CFIUS). Further, section 618 does not reference the FBI. However, historically the FBI has assisted CFIUS in gathering identical information. To the extent that the FBI might be expected to support preparation of the newly contemplated report, this could strain resources.

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,

A handwritten signature in black ink, appearing to read "Stephen E. Boyd", is written over a large, stylized, handwritten "S" that serves as a background for the signature.

Stephen E. Boyd
Assistant Attorney General