UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

KASPERSKY LAB, INC., *et al*., Plaintiffs v. UNITED STATES DEPARTMENT OF HOMELAND SECURITY, *et al*., Defendants	Civil Action No. 17-2697 (CKK)
KASPERSKY LAB, INC., *et al*., Plaintiffs v. UNITED STATES OF AMERICA, Defendant	Civil Action No. 18-325 (CKK)

MEMORANDUM OPINION
(May 30, 2018)

The United States government's networks and computer systems are extremely important strategic national assets. Threats to these systems are constantly expanding and evolving. Their security depends on the government's ability to act swiftly against perceived threats and to take preventive action to minimize vulnerabilities. These defensive actions may very well have adverse consequences for some third-parties. But that does not make them unconstitutional.

Plaintiffs in the two lawsuits discussed in this Opinion represent Kaspersky Lab, a large multinational cybersecurity company headquartered in Russia. At least until 2017, Kaspersky Lab's cybersecurity products were used to defend the networks and computer systems of a number of United States federal government agencies. Amid growing concerns in early 2017 about malicious Russian cyber activity against the United States, government officials and members of Congress began asking questions, and voicing concerns, about the presence of these products on government systems. These concerns were based on the risk that the use of

Kaspersky Lab products to defend United States government computer systems could be exploited by Russia, either with or without Kaspersky Lab's consent, cooperation, or knowledge. The concerns were fueled, in very summary form, by some combination of the following facts: Kaspersky Lab products enjoy extremely broad access and elevated privileges within the computer systems on which they are installed; Kaspersky Lab is headquartered in Russia; Kaspersky Lab and its founder and Chief Executive Officer, Eugene Kaspersky, have close connections to the Russian government and intelligence services; Kaspersky Lab products cycle users' data to the company's servers that are based in (or accessible from) Russia; Kaspersky Lab is subject to Russian laws that allow the Russian government to request or compel assistance from Russian companies, and is also susceptible to non-legal forms of pressure from the Russian government.

The apparent national security risk presented by federal government agencies using Kaspersky Lab products eventually proved intolerable to both Executive Branch officials and Congress. On September 13, 2017, the Department of Homeland Security ("DHS") issued a Binding Operative Directive ("BOD 17-01") pursuant to the Federal Information Security Modernization Act of 2014 ("FISMA"), that required all federal departments and agencies to identify and, ninety days later, remove Kaspersky Lab products from their systems. That directive was soon effectively superseded when Congress passed the National Defense Authorization Act for Fiscal Year 2018 ("NDAA"), which contains a provision entitled "Prohibition on Use of Products and Services Developed or Provided by Kaspersky Lab." As its title suggests, that provision prohibits all elements of the federal government from using any Kaspersky Lab products or services.

Shortly after BOD 17-01 was finalized and the NDAA was signed into law, Kaspersky Lab filed a lawsuit (17-cv-2697) claiming that the BOD violated the Administrative Procedures Act ("APA") and the Due Process Clause of the Fifth Amendment to the United States Constitution (hereinafter the "BOD Lawsuit"). The BOD Lawsuit did not challenge the legality of the NDAA's prohibition on the use of Kaspersky Lab products. Months later, after this omission became a point of contention regarding Plaintiffs' standing in the BOD Lawsuit, Plaintiffs filed a second lawsuit (18-cv-325) claiming that the NDAA's prohibition was an unconstitutional bill of attainder (hereinafter the "NDAA Lawsuit").

These lawsuits are separate and distinct, but both are pending before this Court. The Court is issuing this Opinion in both lawsuits, because there are motions pending in each that present overlapping and interrelated issues. Those motions include: Defendant's [10] Motion to Dismiss the Complaint in the NDAA Lawsuit, Plaintiffs' [19] Motion for Summary Judgment in the BOD Lawsuit, and Defendants' [21] Motion to Dismiss or Alternatively for Summary Judgment in the BOD Lawsuit.

Having carefully reviewed the record, the pleadings,[1] and the relevant authorities, the Court GRANTS Defendant's Motion to Dismiss the NDAA Lawsuit. Plaintiffs have not plausibly alleged that the NDAA constitutes a bill of attainder. A bill of attainder is "a law that legislatively determines guilt and inflicts punishment upon an identifiable individual without

[1] The Court's consideration has focused on the following documents and their attachments in the NDAA Lawsuit:

- Def.'s Mem. in Supp. of Mot. to Dismiss, ECF No. 10-1 ("Def.'s Mem.");
- Pls.' Mem. in Opp'n to Def.'s Mot. to Dismiss, ECF No. 11 ("Pls.' Opp'n");
- Def.'s Reply Mem. in Supp. of Mot. to Dismiss; ECF No. 12 ("Def.'s Reply").

In an exercise of its discretion, the Court finds that holding oral argument in this action would not be of assistance in rendering a decision. *See* LCvR 7(f).

provision of the protections of a judicial trial." *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 468 (1977). The NDAA does not inflict "punishment" on Kaspersky Lab. It eliminates a perceived risk to the Nation's cybersecurity and, in so doing, has the secondary effect of foreclosing one small source of revenue for a large multinational corporation.

Having carefully reviewed the record, the pleadings,[2] and the relevant authorities, the Court also GRANTS Defendants' Motion to Dismiss the BOD Lawsuit for lack of standing. Plaintiffs allege that BOD 17-01 causes them harm by depriving them of the ability to sell to the United States federal government and by damaging their reputation. Even if the Court were to rule in Plaintiffs' favor in the BOD Lawsuit and order the rescission of BOD 17-01, these harms would continue. The NDAA would remain on the books, preventing any federal government agency from purchasing Kaspersky Lab products. It is true that the NDAA's prohibition does not become effective until October 1, 2018. However, government agencies have likely already removed all Kaspersky Lab products from their systems as a result of BOD 17-01 and they know that, regardless, all such products must be removed by the fast-approaching NDAA effective date. Under these circumstances, it is completely implausible that any government entity would purchase a Kaspersky Lab product before October 1st. Accordingly, the empty "right" to sell to

[2] The Court's consideration has focused on the following documents and their attachments in the BOD Lawsuit:

- Pls.' Mem. of Law in Supp. of Mot. for Summ. J., ECF No. 19-1 ("Pls.' Mem.");
- Defs.' Mem. in Opp'n to Pls.' Mot. for Summ. J. and in Support of Mot. to Dismiss or, in the Alternative, for Summ. J., ECF Nos. 20, 21-1 ("Defs.' Opp'n");
- Pls.' Reply in Supp. of Mot. for Summ. J. and in Opp'n to Defs.' Mot. to Dismiss or, in the Alternative, for Summ. J., ECF Nos. 22, 23 ("Pls.' Reply and Opp'n");
- Defs.' Reply in Supp. of Mot. to Dismiss or, in the Alternative, for Summ. J., ECF No. 24 ("Defs.' Reply").

In an exercise of its discretion, the Court finds that holding oral argument in this action would not be of assistance in rendering a decision. *See* LCvR 7(f).

the federal government for the short period before October 1st that Plaintiffs could stand to gain from success in the BOD Lawsuit lacks any concrete value. It is insufficient to confer standing. An order rescinding the BOD would also not redress the alleged harm to Plaintiffs' reputation as a cybersecurity business because, according to Plaintiffs themselves, the NDAA independently causes, at least, that same harm. Plaintiffs attempted to avoid this jurisdictional roadblock by filing a separate lawsuit challenging the NDAA, but even if the later-filed NDAA Lawsuit had any relevance to Plaintiffs' standing in the BOD Lawsuit, that relevance has been eliminated by its dismissal. Because the BOD Lawsuit is dismissed for lack of standing, the Court need not reach the parties' cross-motions for summary judgment.

I. BACKGROUND

A. The Threat of Russian Cyber-Attacks

An important context of Plaintiffs' lawsuits, which neither party appears to dispute, is that it is the assessment of the United States government that cyber-attacks, especially from Russia, present a potent threat to critical United States infrastructure. As described by then-Director of National Intelligence James R. Clapper in a statement to the Senate Armed Services Committee in 2015, "[p]olitically motivated cyber-attacks are now a growing reality, and foreign actors are reconnoitering and developing access to US critical infrastructure systems, which might be quickly exploited for disruption if an adversary's intent became hostile." AR0106. "[T]hose conducting cyber espionage are targeting US government, military, and commercial networks on a daily basis." *Id.* As current Director of National Intelligence Daniel R. Coats recently stated in a similar report, "Russia is a full-scope cyber actor that will remain a major threat to US Government, military, diplomatic, commercial, and critical infrastructure." AR0065. "Moscow has a highly advanced offensive cyber program, and in recent years, the

Kremlin has assumed a more aggressive cyber posture." *Id.* "This aggressiveness was evident in Russia's efforts to influence the 2016 US election." *Id.*

B. Kaspersky Lab and Eugene Kaspersky

Kaspersky Lab is a large cybersecurity company headquartered in Moscow. *See* Decl. of Angelo Gentile, BOD Lawsuit ECF No. 19-3 ("Gentile Decl."), ¶¶ 9-11. It sells products that are intended to protect its customers' computer systems against cyber-threats. *Id.* ¶ 9. The company was founded in 1997 by Eugene Kaspersky, who serves as the company's Chief Executive Officer. *Id.* ¶ 11. Kaspersky Lab is a multinational corporation present in countries throughout the world, but the particular Plaintiffs in the two lawsuits discussed in this Opinion are Kaspersky Lab, Inc., a Massachusetts corporation that acts as the North American headquarters for Kaspersky Lab, and Kaspersky Lab Limited, a U.K.-based holding company for Kaspersky Lab entities. *Id.* ¶¶ 4, 9-11.

It is important to note that Kaspersky Lab does not sell its products exclusively to the United States federal government. *Id.* ¶ 9. Far from it. To the contrary, "[o]ver 400 million users—from governments to private individuals, commercial enterprise to critical infrastructure owners and operators alike—utilize Kaspersky Lab technologies." *Id.* ¶ 9. Indeed, only a *tiny* fraction of Kaspersky Lab sales in the United States are to the federal government. *Id.* ¶ 15. "Active licenses held by federal agencies in September 2017 had a total value (to Kaspersky Lab, Inc. and the Company as a whole) of less than $54,000—approximately 0.03% of Kaspersky Lab, Inc.'s annual U.S. sales at the time." *Id.*

C. Early Concerns Voiced About Kaspersky Lab Products

Members of Congress and the Executive Branch began expressing concerns about the government's use of Kaspersky Lab products—and acting on those concerns—in, at least, early

2017. For example, during a March 2017 Senate hearing on Russian cyber activities, Senator Marco Rubio of Florida cited a "long history" of open-source reporting connecting Kaspersky Lab to Russian security services, and asked a panel of cybersecurity experts if they would feel comfortable using Kaspersky Lab products on their devices. Although one of those experts noted that "Kaspersky is not an arm of the Russian government," another responded "no, I wouldn't, and I wouldn't recommend that you do it either." *Disinformation: A Primer in Russian Active Measures and Influence Campaigns, Panel II Before the S. Select Comm. on Intelligence*, 115th Cong. 40 (Mar. 30, 2017). In April 2017, the Senate Select Committee on Intelligence asked the Director of National Intelligence and the Attorney General to investigate Kaspersky Lab's ties to the Russian government. *See Bolstering the Government's Cybersecurity: Assessing the Risks of Kaspersky Lab Products to the Federal Government Before the H. Comm. on Science, Space, and Technology*, 115th Cong. 33 (Oct. 25, 2017). That same month, two Congressmen introduced a bill describing Kaspersky Lab as "a company suspected of having ties with the Russian intelligence services and later caught up in a Russian espionage investigation." H.R. Con. Res. 47, 115th Cong. (2017). In May 2017, six United States intelligence directors, including the directors of the Central Intelligence Agency ("CIA") and the National Security Agency ("NSA"), told the Senate Select Committee on Intelligence that they would not be comfortable using Kaspersky Lab products on their computers. *See Hearing on Worldwide Threats Before the S. Select. Comm. on Intelligence*, 115th Cong. (May 11, 2017), https://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats-hearing-0. NSA Director Michael Rogers said that he was "personally involved" in monitoring the Kaspersky Lab issue, and then-CIA Director Michael Pompeo acknowledged that concerns about Kaspersky Lab products "ha[d] risen to the director" level at the CIA. *Id.*

Throughout the summer of 2017, lawmakers continued to raise concerns about the presence of Kaspersky Lab products on federal government systems in at least three other committee hearings in the House and the Senate. *See Bolstering the Government's Cybersecurity: Lessons Learned from Wannacry Before H. Comm. on Science, Space, and Technology*, 115th Cong. (June 15, 2017); *Russian Interference in the 2016 U.S. Elections Before S. Select Comm. on Intelligence*, 115th Cong. (June 21, 2017); *Help or Hindrance? A Review of SBA's Office of the Chief Information Officer Before the H. Comm. on Small Business*, 115th Cong. (July 12, 2017). In July 2017, Congressman Lamar Smith, Chairman of the House Science Committee, sent a letter to various federal agencies requesting information about their use of Kaspersky Lab software and expressing concern that the company's products were "susceptible to manipulation by the Russian government." AR0557-58. Also in July 2017, the General Services Administration ("GSA") removed Kaspersky Lab as a pre-approved vendor for contracts. AR0017.

D. Communications Between Kaspersky Lab and DHS Prior to BOD 17-01

On July 18, 2017, amidst this growing consensus that the use of Kaspersky Lab products to defend federal systems posed national security risks, Eugene Kaspersky wrote then-Secretary of Homeland Security John F. Kelly a letter "offer[ing] any information or assistance we can provide with regard to any Department investigation regarding the company, its operations, or its products." AR0749. The letter generally extolled Kaspersky Lab's integrity and sought to assure Secretary Kelly that the company had no ties with the Russian government and has not, and would not, assist any government with cyber-espionage efforts. *Id.* Mr. Kaspersky offered to make himself available to DHS, the Senate Select Committee on Intelligence, or any other committees or agencies conducting any relevant investigations. *Id.*

DHS responded by letter on August 14, 2017, thanking Mr. Kaspersky for offering to provide information, stating that DHS looked forward to communicating with him further, and indicating that DHS "will be in touch again shortly." AR0940.

E. BOD 17-01

Much to Plaintiffs' dismay, the next they heard from DHS was on September 13, 2017, when, pursuant to her authority under FISMA, Acting DHS Secretary Elaine C. Duke issued BOD 17-01, entitled "Removal of Kaspersky-Branded Products." AR0633-35.

A very brief explanation of BODs generally is necessary here. Pursuant to FISMA, federal agencies are required, under the supervision of the Director of the Office of Management and Budget and the Secretary of Homeland Security, to establish and implement their own policies, principles, standards and guidelines on information security. 44 U.S.C. § 3554(b) ("Each agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency."). As particularly relevant to this case, FISMA provides that "[t]he Secretary, in consultation with the Director, shall administer the implementation of agency information security policies and practices for information systems," including by "developing and overseeing the implementation of binding operational directives to agencies." 44 U.S.C. § 3553(b)(2). A binding operational directive, or BOD, is "a compulsory direction to an agency that (A) is for purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk; (B) shall be in accordance with policies, principles, standards, and guidelines issued by the Director; and (C) may be revised or repealed by the Director if the direction issued on behalf of the Director is not in accordance with policies and principles

developed by the Director." *Id.* § 3552(b)(1). In other words, BODs are used to address suspected threats, vulnerabilities, or risks to federal information systems. In this way, the BOD is a tool that gives the DHS Secretary the ability to take swift action based on predictive judgments to address constantly evolving cyber-threats.

BOD 17-01 in particular required all federal departments and agencies to take three actions: (1) within 30 days of the issuance of the BOD (October 13, 2017), all agencies were required to identify the use or presence of Kaspersky-branded products on all federal information systems and report this information to DHS; (2) within 60 days (November 12, 2017), all agencies were required to develop and provide to DHS a plan for removing and discontinuing present and future use of all Kaspersky-branded products beginning 90 days after the issuance of the BOD; and (3) within 90 days (December 12, 2017), unless otherwise directed, all agencies were required to begin implementing their plan and provide DHS a status report on that implementation every 30 days thereafter until full removal and discontinuance of Kaspersky-branded products was achieved. AR0634-35. "Kaspersky-branded products" were defined as "information security products, solutions, and services supplied, directly or indirectly, by AO Kaspersky Lab or any of its predecessors, successors, parents, subsidiaries, or affiliates." AR0634. BOD 17-01 exempted from its scope "national security systems" and certain other systems operated by the Department of Defense and the intelligence community. AR0633.

The BOD itself stated that "DHS, in consultation with interagency partners, ha[d] determined that the risks presented by Kaspersky-branded products justif[ied] the issuance of" the BOD, AR0633, and a "Decision Memorandum" accompanying the BOD explained the reasoning underlying that determination. The Acting Secretary stated that she had issued the BOD because, based on the evidence presented to her by the Assistant Secretary for Cyber

Security and Communications, she had concluded that Kaspersky-branded products on federal information systems presented a known or reasonably suspected information security threat, vulnerability, and risk to federal information and information systems. AR0628-29. That conclusion was based primarily on the following factors: (1) Kaspersky-branded products were currently being used by federal agencies, and Kaspersky Lab intended to expand its sale of those products to federal agencies in the near future; (2) anti-virus products like Kaspersky Lab's enjoy broad access to files and elevated privileges on the systems on which they are used that can be exploited by malicious cyber-actors; (3) data of those using Kaspersky Lab products is transferred automatically from their computers to Kaspersky Lab servers (which are either located in Russia or accessible from Russia); (4) Russia has engaged in, and will likely continue to engage in, malicious cyber-activities against United States government information systems; (5) Kaspersky Lab and Kaspersky Lab officials have ties to the Russian government, and specifically to its intelligence services; and (6) Russian legal provisions allow Russian intelligence services to request or compel assistance from companies like Kaspersky Lab and to intercept communications transiting Russian networks. AR0629-30.

The BOD was not based on a determination that Kaspersky Lab was disloyal or guilty of any wrongdoing. Acting Secretary Duke explained that the "crux" of the threat addressed by the BOD was "the ability of the Russian government, whether acting on its own or through Kaspersky, to capitalize on access to federal information and information systems provided by Kaspersky-branded products." AR0629. "These risks," she noted, "exist regardless of whether Kaspersky-branded products already have been used by Kaspersky or the Russian Government for malicious purposes." *Id.* Her determination was supported by the unclassified information

presented to her, although she noted that she had reviewed classified information as well that provided further support for her action. AR0631.

BOD 17-01 was supported by a considerable administrative record. Most relevant for the purposes of this Opinion is a September 1, 2017, memorandum prepared for Acting Secretary Duke by the Assistant Secretary for Cyber Security and Communications, Jeanette Manfra, which outlined much of the publically available information underlying concerns about Kaspersky Lab products. AR0003-23. The memo stated that "DHS cybersecurity experts in the National Protection and Programs Directorate, in consultation with interagency partners, agree that Kaspersky-branded products present known or reasonably suspected information security risks to federal information and information systems." AR0004. More specifically, the memo stated that:

> BOD 17-01 is based on expert judgment about threats to U.S. national security. The danger stems in part from the inherent properties of anti-virus software, which operates with broad file access and elevated privileges. Such access and privileges can be exploited by a malicious cyber actor such as Russia, which has demonstrated the intent to target the U.S. government and the capability to exploit vulnerabilities in federal information systems. Kaspersky or the Russian government could use this software to engage in a wide range of malicious cyber activities against federal information and information systems, including exfiltrating files, modifying data, or installing malicious code, with potentially grave consequences for U.S. national security. These actions could take place because of a range of factors, including Russian laws that authorize the Russian Federal Security Service ("FSB") to compel Russian enterprises to assist the FSB in the execution of FSB duties, to second FSB agents to Russian enterprises (with the enterprise's consent), and to require Russian companies to include hardware or software needed by the FSB to engage in "operational/technical measures." Kaspersky also relies on the FSB for needed business licenses and certificates, and the FSB could condition the granting of such approvals on Kaspersky's cooperation. Finally, Russian law allows the FSB to intercept all communications transiting Russian telecommunications and Internet Service Provider networks, which presumably includes data transmissions between Kaspersky and its

> U.S. government customers. Because of these known or reasonably suspected risks to federal information and information systems, which directly implicate U.S. national security, this memorandum recommends that you exercise your authority to issue BOD 17-01.

Id. The Assistant Secretary's memo goes on to explain these concerns in far more detail than the Court will recount in this Opinion. However, certain of her findings warrant emphasis. First, according to a report prepared by the National Cybersecurity and Communications Integration Center ("NCCIC"), anti-virus products generally, and Kaspersky Lab products specifically, present unique security risks. AR0007. Because these products are intended to *defend* against cyber-threats, they require the highest level of privileges and access on the systems on which they are installed. *Id.* Those privileges may allow them to extract files and send them to company servers and may permit the interception of otherwise-encrypted communications. *Id.* Moreover, because these products are themselves supposed to defend the systems on which they are installed from malicious activities, they can be modified to intentionally *not* identify malicious files. *Id.* They can also be used to install malicious code under the guise of a security update, extract a file of interest under the pretext that it needs to be inspected for malware, or simply decline to install security updates that are needed. AR0008. In other words, if compromised, cybersecurity products like Kaspersky Lab's could end up being the proverbial fox guarding the hen house.

Also warranting brief mention here is the memorandum's analysis of Kaspersky Lab's ties to the Russian government and intelligence agencies (including Eugene Kaspersky's personal ties). These include, among other things, reports that Kaspersky Lab has certificates and licenses from the Federal Security Service ("FSB"), a Russian intelligence service, that suggest a close relationship between Kaspersky Lab and that organization, as well as reports that Eugene Kaspersky, who graduated from an institute that was sponsored by the KGB and

previously worked for the Russian Ministry of Defense, maintains close personal ties with Russian intelligence officers. AR0011-13. Other Kaspersky Lab leaders have similar pedigrees. AR0013.

In addition to citing the above facts as her basis for concern that Kaspersky Lab products posed a cybersecurity risk on federal systems, Acting Secretary Duke also explained her reasoning for using a BOD to address this risk as opposed to a "debarment" process under the Federal Acquisition Regulation ("FAR"). AR0631. She concluded that debarment would not be effective because "debarment would affect only future contracts for a finite period; it would not require federal agencies to remove products previously purchased and installed on federal networks, and thus would not address current information security risks to federal information systems." *Id.* Debarment also would allow third parties to continue selling Kaspersky Lab products to the federal government, and would allow agencies to continue contracts in existence at the time the contractor was debarred. *Id.* For those reasons, the Acting Secretary determined that debarment would not remove the threat DHS (and others) had identified because it would not completely remove Kaspersky Lab products from federal information systems. *Id.*[3]

The BOD established an administrative process for the submission and consideration of comments on the removal of Kaspersky-branded products before that removal took place 90 days thereafter. AR0630. On the same day that BOD 17-01 was issued, Acting Secretary Duke also sent Eugene Kaspersky a letter informing him of the BOD and providing him "an opportunity to provide [DHS] with any information that [he thought was] relevant to [her] ongoing

[3] Both the Acting Secretary's Decision Memorandum and the Assistant Secretary's memorandum addressed "contrary evidence" or arguments that Kaspersky Lab had publicly made regarding the integrity of its products, and explained why those arguments were not persuasive. AR0630; AR0019-23.

deliberations concerning [Kaspersky Lab's] products and services." AR0637-38. The letter informed Mr. Kaspersky that he could initiate a review by DHS by providing the Department with a written response to the BOD and supporting evidence. *Id.* DHS also published a notice in the Federal Register that explained the actions required by BOD 17-01, and gave any entity whose commercial interests were directly impacted by the BOD an opportunity to respond, provide additional information, and initiate a review by DHS. AR0639-46. Mr. Kaspersky and other entities that wanted to respond were given 45 days to do so, and informed that a decision by the Secretary regarding their responses would be communicated to them in 85 days. AR0639, 646.

F. Congressional Scrutiny of Kaspersky Lab Continues

In the meantime, Congress continued to deliberate about the risks presented by the reliance on Kaspersky Lab products to defend federal systems. In October 2017, the House Science Committee held investigative hearings on the federal government's use of Kaspersky Lab products, and the implementation of BOD 17-01. *See, e.g., Bolstering the Government's Cybersecurity: Assessing the Risks of Kaspersky Lab Products to the Federal Government Before the H. Comm. on Science, Space, and Technology*, 115th Cong. 33 (Oct. 25, 2017). The BOD itself was discussed, as were the major issues raised by DHS about Kaspersky Lab products in the BOD proceedings, including, among other things, Kaspersky Lab and Eugene Kaspersky's ties to Russia and their susceptibility to exploitation by the Russian government. On October 31, 2017, the House Science Committee issued a report about the risks presented by the presence of Kaspersky Lab products on federal government systems and concluded that "Congress must take aggressive actions to support and assure a fundamentally different approach to cybersecurity that addresses the magnitude and nature of growing threats." H.R. Rep. No.

115-376, at 4 (Oct. 31, 2017); *see also* Decl. of Ryan P. Fayhee, ECF No. 19-4 ("Fayhee Decl."), Ex. D (transcript from November 2017 House Subcommittee on Oversight hearing regarding the implementation of BOD 17-01).

G. Kaspersky Lab Responds to the BOD

Kaspersky submitted a lengthy response to BOD 17-01 on November 10, 2017. AR0647-745; *see also* AR0746-48 (granting Kaspersky Lab a one-week extension of time to submit their response). According to Plaintiffs, the submission "rebutted at length the legal arguments and factual allegations levied against Plaintiffs, corrected many misunderstandings apparently held by DHS and perpetuated by the cited news reports, and highlighted the deficiencies in the administrative process offered by DHS." Pls.' Mem. at 9. The submission argued, among other things, that Kaspersky Lab had no improper relationship with the Russian government; that there was no evidence that Kaspersky Lab had engaged in any wrongdoing or posed any more risk than similarly situated companies; that the BOD was based on uncorroborated and anonymous sources; that the administrative procedure surrounding the issuance of the BOD and for responding to the BOD was insufficient; and that the BOD violated Kaspersky Lab's equal protection and due process rights. *Id.* No other entity submitted a response to the BOD. AR0755.

On November 29, 2017, Kaspersky Lab officials and their counsel met with DHS officials to discuss BOD 17-01. *See* Fayhee Decl. ¶ 6. DHS officials had declined to meet with Kaspersky Lab until after their written response to the BOD was submitted. AR0746-68. At the November 29, 2017 meeting, "Plaintiffs responded to a number [of] questions from DHS attorneys regarding the Kaspersky Lab Submission." Fayhee Decl. ¶ 6. The meeting included a discussion of the company's submission and numerous related topics, including "Kaspersky's

corporate structure," "the alleged effects to the company's business," "the NDAA," "Kaspersky's intention not to target federal business," and "mitigation proposals." AR0755.

H. Final Decision on BOD 17-01

On December 6, 2017, Acting Secretary Duke issued a "Final Decision" on BOD 17-01. AR0934-37. She stated that the Department had "closely reviewed the Kaspersky Submission," "met with Kaspersky and its counsel," "identified additional statements made by Kaspersky from public sources, obtained information from agencies pursuant to the BOD 17-01 reporting requirements, and received a report on relevant provisions of Russian law prepared by Professor Peter Maggs of the University of Illinois College of Law, as well as a supplemental Assessment from the [NCCIC]." AR0935. Secretary Duke stated that "the information obtained by DHS since issuance of the BOD [did] not meaningfully impact, and indeed further support[ed], the information security and national security determination that [she] made in issuing the BOD." AR0934. Accordingly—relying on the reasons explained in the preceding DHS memoranda—the Acting Secretary stated that her determination that Kaspersky-branded products presented a known or reasonably suspected information security threat, vulnerability, or risk to federal information and information systems remained unchanged, and that she maintained BOD 17-01 without modification. AR0935. Acting Secretary Duke sent a letter to Mr. Kaspersky notifying him of her decision the day it was issued. AR0938.

The reasoning underlying the Final Decision was explained further in a memorandum from Assistant Secretary Manfra. AR0752-76. That memorandum indicated that fourteen federal government agencies had reported identifying Kaspersky-branded products on their information systems. AR0756. Some of those agencies had, on their own initiative, already removed those products prior to the 90-day deadline under BOD 17-01. *Id.* This was done of

the agencies' own accord, pursuant to their own agency risk management responsibilities under FISMA. *Id.* DHS did not advise those agencies to remove the products before the BOD's 90-day deadline. *Id.* All other agencies had submitted plans to remove Kaspersky Lab products, but had not yet implemented them. *Id.*

This memorandum also discussed the report on Russian law prepared by Professor Peter Maggs. AR0756; *see also* AR0777-821 (Report of Peter B. Maggs). Professor Maggs had prepared a report that, the memorandum indicated, supported DHS's view of Russian law and provided additional support for DHS's Russian law-related concerns (*i.e.*, that under Russian law, the FSB could use companies like Kaspersky Lab with or without their consent). *Id.* The memorandum also contained approximately 18 pages of detailed responses to the arguments in Kaspersky Lab's response to BOD 17-01, explaining why those arguments were not persuasive to DHS. AR0757-75. In conclusion, the Assistant Secretary stated that, "the totality of the administrative record," including Kaspersky Lab's submission, "presents a compelling picture of the various ways that the Russian Government, and particularly the FSB intelligence agency, can compel, request, and otherwise exploit the access provided by Kaspersky-branded products to the information and information systems of Kaspersky customers, including U.S. government customers." AR0775.

I. The National Defense Authorization Act for Fiscal Year 2018

Almost immediately after the BOD was finalized, it was effectively superseded by an act of Congress. On the heels of DHS's proceedings, Congress passed, and President Donald J. Trump signed into law, the NDAA. *See* PL 115-91, 2017 HR 2810, PL 115-91, December 12, 2017, 131 Stat 1283. In very summary terms, the NDAA is a law that authorizes appropriations and sets policies for Department of Defense programs and activities.

The relevant portion of the NDAA for the purposes of this Opinion is Section 1634. Section 1634 falls within Subtitle C of the Act, entitled "Cyberspace-Related Matters." Section 1634(c) requires the Secretary of Defense, in consultation with other agencies, to conduct a review of procedures for removing suspect products and services from federal information technology networks and to submit a report to Congress on the same. Section 1634(a) focuses on Kaspersky Lab products. It states that "[n]o department, agency, organization, or other element of the Federal Government may use, whether directly or through work with or on behalf of another department, agency, organization, or element of the Federal Government, any hardware, software, or services developed or provided, in whole or in part, by—(1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership." *Id*. § 1634(a). Section 1634(b) sets October 1, 2018, as the effective date for the prohibition. *Id*. § 1634(b).

This prohibition is broader in scope than BOD 17-01 in two ways. First, it applies to all Kaspersky Lab products (hardware, software, and services), whereas the BOD only applied to a smaller subset of "Kaspersky-branded products." Second, unlike BOD 17-01, the NDAA does not have any carve outs or exceptions for national security systems or other systems used by the Department of Defense or the intelligence community.

As initially introduced, the NDAA did not contain a provision regarding Kaspersky Lab products. An amendment to the Act adding a prohibition on the use of Kaspersky Lab products was first introduced by Senator Jeanne Shaheen of New Hampshire. A Senate Armed Services Committee executive summary described the amendment as a response to "reports that the

Moscow-based company might be vulnerable to Russian government influence." NDAA FY 2018, U.S. Senate Armed Services Committee, at 10, https://www.armed-services.senate.gov/imo/media/doc/FY18%20NDAA%20Summary6.pdf. Senator Shaheen's proposed prohibition appears to have attracted bipartisan support in Congress and grown broader before it was eventually passed into law as Section 1634.

Plaintiffs' lawsuits cite certain statements Senator Shaheen made to the public regarding the proposed prohibition and Kaspersky Lab generally around the time that the amendment was introduced and adopted. On September 4, 2017, the *New York Times* published an editorial authored by Senator Shaheen, in which she asserted that the use of Kaspersky Lab products by federal agencies created a "threat" of Russian cyber-interference, and that she was proposing an amendment to bar federal government use of those products "to close this alarming national security vulnerability." *See* Compl., Ex. C, NDAA ECF No. 1-3. In addition, in a September 18, 2017, press release, issued after an amendment to the NDAA barring the use of Kaspersky Lab products passed in the Senate, Senator Shaheen stated that "[t]he case against Kaspersky Lab is overwhelming." *See* Compl., Ex. E, NDAA ECF No. 1-5. She continued:

> The strong ties between Kaspersky Lab and the Kremlin are alarming and well-documented. I'm very pleased that the Senate has acted in a bipartisan way on my amendment that removes a real vulnerability to our national security. I applaud the Trump administration for heeding my call to remove Kaspersky Lab software from all federal computers. It's important that this prohibition also be a part of statute and be expanded to the entire federal government, as my amendment would do. Considering the

> strong bipartisan, bicameral support for this proposal, I'm optimistic this will soon be signed into law.

J. Plaintiffs' Lawsuits and Procedural History

Plaintiffs Kaspersky Lab Inc. and Kaspersky Labs Limited have filed two related but separate lawsuits. One, the BOD Lawsuit, was filed on December 18, 2017, shortly after the BOD was finalized and the NDAA was signed into law. *See* Compl., BOD ECF No. 1. Plaintiffs allege in that suit that the BOD and the Final Decision confirming the BOD violate the APA and Plaintiffs' Fifth Amendment right to due process. *Id*. ¶¶ 1, 20. The lawsuit does not challenge the NDAA.

On January 17, 2018, Plaintiffs filed an Application for Preliminary Injunction in the BOD Lawsuit. *See* Pls.' App. for Preliminary Injunction, BOD ECF No. 10. Upon receipt of that Application, the Court immediately held a teleconference on the record with the parties to set a briefing schedule. Defendants then filed an opposition to that Application wherein they argued, in part, that Plaintiffs lacked standing. *See* Defs.' Mem. in Opp'n to Pls.' App. for Prelim. Inj., BOD ECF No. 13, at 14-27. Because the BOD Lawsuit left the NDAA's complete prohibition of Kaspersky Lab products unchallenged, Defendants argued that even if Plaintiffs were successful in obtaining the rescission of BOD 17-01, their alleged harms would not be redressed. *Id.*

In an apparent effort to rebut this argument, on the same day that Plaintiffs filed their reply in support of their Application for Preliminary Injunction in the BOD Lawsuit, they also filed the NDAA Lawsuit. *See* Compl., NDAA ECF No. 1. That suit claims that Sections 1634(a) and (b) of the NDAA constitute an unconstitutional bill of attainder. *Id.* ¶ 4.

After these filings, the Court issued a Minute Order giving Defendants in the BOD Lawsuit an opportunity to file a sur-reply addressing the legal relevance of the newly-filed

NDAA lawsuit to Plaintiffs' request for a preliminary injunction in the BOD Lawsuit. *See* Feb. 13, 2018 Min. Order. The Court also gave Plaintiffs an opportunity to withdraw their preliminary injunction application in lieu of pursuing an expedited summary judgment briefing schedule.[4] *Id.* Plaintiffs subsequently did withdraw their application. *See* Pls.' Notice of Withdrawal, BOD ECF No. 16. The Court then consolidated the BOD Lawsuit and the NDAA Lawsuit "solely for the purpose of briefing an upcoming round of dispositive motions," including cross-motions for summary judgment and a motion to dismiss in the BOD Lawsuit and a motion to dismiss in the NDAA Lawsuit." *See* Feb. 16, 2018 Order, BOD ECF No. 17, NDAA ECF No. 7. Those motions have now been fully briefed and are ripe for resolution.

II. LEGAL STANDARDS

A. Motion to Dismiss for Lack of Jurisdiction

When a motion to dismiss a complaint under Federal Rule of Civil Procedure 12(b)(1) is filed, a federal court is required to ensure that it has "the 'statutory or constitutional power to adjudicate [the] case[.]'" *Morrow v. United States*, 723 F. Supp. 2d 71, 77 (D.D.C. 2010) (emphasis omitted) (quoting *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 89 (1998)). "Federal courts are courts of limited jurisdiction" and can adjudicate only those cases or controversies entrusted to them by the Constitution or an act of Congress. *Kokkonen v.*

[4] As the Court discussed with the parties, there is a troubling trend in APA cases whereby plaintiffs are routinely filing preliminary injunction motions simply to "jump the queue" and have the Court consider the merits of their claims immediately. There are certainly instances where such motions are necessary and appropriate to prevent an impending injury, but increasingly these "emergency" motions are being filed simply because the plaintiff is aggrieved by an agency decision and wants the Court to focus its attention on its claims immediately, at the expense of the claims of other litigants. This practice is strongly discouraged. *See Am. Bioscience, Inc. v. Thompson*, 269 F.3d 1077, 1084 n.8 (D.C. Cir. 2001) (warning against the use of preliminary injunction motions in APA cases); *Emily's List v. Fed. Election Comm'n*, 362 F. Supp. 2d 43, 53 (D.D.C.), *aff'd*, 170 F. App'x 719 (D.C. Cir. 2005) ("the preliminary injunction stage is not the appropriate time to consider the merits of Plaintiff's substantive APA claims.").

Guardian Life Ins. Co. of Am., 511 U.S. 375, 377 (1994). In determining whether there is jurisdiction on a motion to dismiss, the Court may "consider the complaint supplemented by undisputed facts evidenced in the record, or the complaint supplemented by undisputed facts plus the court's resolution of disputed facts." *Coal. for Underground Expansion v. Mineta*, 333 F.3d 193, 198 (D.C. Cir. 2003) (citations omitted). "Although a court must accept as true all factual allegations contained in the complaint when reviewing a motion to dismiss pursuant to Rule 12(b)(1)," the factual allegations in the complaint "will bear closer scrutiny in resolving a 12(b)(1) motion than in resolving a 12(b)(6) motion for failure to state a claim." *Wright v. Foreign Serv. Grievance Bd.*, 503 F. Supp. 2d 163, 170 (D.D.C. 2007) (citations omitted).

B. Motion to Dismiss for Failure to State a Claim

Under Rule 12(b)(6), a party may move to dismiss a pleading on the grounds that it "fail[s] to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). "[A] complaint [does not] suffice if it tenders 'naked assertion[s]' devoid of 'further factual enhancement.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 557 (2007)). Rather, a complaint must contain sufficient factual allegations that, if accepted as true, "state a claim to relief that is plausible on its face." *Twombly*, 550 U.S. at 570. "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678. "In determining whether a complaint fails to state a claim, [the Court] may consider only the facts alleged in the complaint, any documents either attached to or incorporated in the complaint and matters of which [the Court] may take judicial notice," such as facts in the public record. *E.E.O.C. v. St. Francis Xavier Parochial Sch.*, 117 F.3d 621, 624 (D.C. Cir. 1997).[5]

[5] The Court has taken judicial notice of all of the public records discussed in this Opinion.

III. DISCUSSION

The Court's Opinion will be divided into two parts. The first part addresses Defendant's motion to dismiss the NDAA Lawsuit on the grounds that Sections 1634(a) and (b) of the NDAA do not constitute legislative punishment, and therefore are not a bill of attainder. The second part of the Court's Opinion addresses Defendants' motion to dismiss the BOD Lawsuit on the grounds that Plaintiffs lack standing to challenge BOD 17-01. Defendants argue that the harms that this agency action allegedly causes Plaintiffs are independently caused by the NDAA, which will remain "on the books" even if the BOD is rescinded, rendering the outcome of the BOD Lawsuit meaningless. The Court agrees with Defendants and will dismiss both lawsuits. It accordingly need not reach the parties' cross-motions for summary judgment in the BOD Lawsuit.

A. The NDAA Lawsuit

Plaintiffs claim that Sections 1634(a) and (b) of the NDAA constitute a bill of attainder in violation of Section 9 of Article I of the United States Constitution. That Section states that "[n]o Bill of Attainder or ex post facto Law shall be passed." U.S. Const. art. I, § 9, cl. 3 (the "Bill of Attainder Clause"). A bill of attainder is "a law that legislatively determines guilt and inflicts punishment upon an identifiable individual without provision of the protections of a judicial trial." *Nixon*, 433 U.S. at 468. "Under the now prevailing case law, a law is prohibited under the bill of attainder clause 'if it (1) applies with specificity, and (2) imposes punishment.'" *Foretich v. United States*, 351 F.3d 1198, 1217 (D.C. Cir. 2003) (quoting *BellSouth Corp. v. F.C.C.*, 162 F.3d 678, 683 (D.C. Cir. 1998) ("*BellSouth II*")); *see also United States v. Brown*, 381 U.S. 437, 447 (1965) (explaining that the Bill of Attainder Clause bars "legislative punishment, of any form or severity, of specifically designated persons or groups"). "Both

'specificity' and 'punishment' must be shown before a law is condemned as a bill of attainder." *Foretich*, 351 F.3d at 1217. Defendant appears to concede the specificity element—the heart of the parties' dispute is about punishment.

1. Specificity

The first requirement of any bill of attainder is that it be specific. That is, the law must apply with specificity to only a designated person or group. "The element of specificity may be satisfied if the statute singles out a person or class by name or applies to 'easily ascertainable members of a group.'" *Hettinga v. United States*, 677 F.3d 471, 477 (D.C. Cir. 2012) (quoting *Foretich,* 351 F.3d at 1217).

Defendant does not contend in its Motion to Dismiss that Sections 1634(a) and (b) lack the requisite specificity. *See* Def.'s Mem. at 11 ("Even assuming Kaspersky can demonstrate that Section 1634 satisfies the specificity requirement . . . "). Accordingly, for the purposes of this Opinion, the Court will assume that the specificity requirement is satisfied. Given that the NDAA expressly singles out Kaspersky Lab by name, this assumption appears to be a sound one.

2. Punishment

Specificity alone, however, "does not render a statute an unconstitutional bill of attainder." *Foretich*, 351 F.3d at 1217. The law must also inflict "punishment." *Id.* Many laws apply with specificity. It is the inflicting of "punishment" that is the "principal touchstone" of a bill of attainder. *Id.* at 1218.

"In deciding whether a statute inflicts forbidden punishment," the Supreme Court has "recognized three necessary inquiries: (1) whether the challenged statute falls within the historical meaning of legislative punishment [the "Historical Test"]; (2) whether the statute, 'viewed in terms of the type and severity of burdens imposed, reasonably can be said to further

nonpunitive legislative purposes' [the "Functional Test"]; and (3) whether the legislative record 'evinces a congressional intent to punish' [the "Motivational Test"]." *Selective Serv. Sys. v. Minnesota Pub. Interest Research Grp.*, 468 U.S. 841, 852 (1984) (quoting *Nixon*, 433 U.S. at 473, 475-76, 478). These three tests are each "independent—though not necessarily decisive—indicator[s] of punitiveness." *Foretich*, 351 F.3d at 1218. They "are considered independently, and are weighed together to resolve a bill of attainder claim." *Patchak v. Jewell*, 828 F.3d 995, 1006 (D.C. Cir. 2016). That being said, the D.C. Circuit has noted on multiple occasions that the Functional Test is the most important of the three, *see, e.g.*, *BellSouth II*, 162 F.3d at 684, and indeed that "compelling proof" under this test may even "be determinative," *Foretich*, 351 F.3d at 1218.

All three tests lead to the same conclusion in this case: the challenged provisions of the NDAA are not punishment. Sections 1634(a) and (b) of the NDAA do not fall within the historical meaning of legislative punishment and reasonably further the nonpunitive legislative purpose of safeguarding the Nation's infrastructure from the risk of Russian cyber-attacks. Moreover, there is nothing in the record that indicates a congressional intent to punish Kaspersky Lab.

a. The Historical Test

First, the NDAA does not qualify as a bill of attainder under the Historical Test. The Historical Test asks if the challenged legislation constitutes one of a "checklist of deprivations and disabilities" that have been historically associated with bills of attainder. *Foretich*, 351 F.3d at 1218. This checklist includes death, "imprisonment, banishment, . . . the punitive confiscation of property by the sovereign," and "legislative enactment[s] barring designated individuals or groups from participation in specified employments or vocations." *Nixon,* 433 U.S. at 474. These "deprivations and disabilities" have been said to be "so disproportionately severe and so

inappropriate to nonpunitive ends that they unquestionably have been held to fall within the proscription of Art. I, s 9." *Id.* at 473.

Little need be said about most of these historical forms of legislative punishment. Sections 1634(a) and (b) of the NDAA bar federal government agencies from using the products of a particular cybersecurity vendor. They do not order anyone's execution, imprisonment, or banishment, nor do they confiscate anyone's property. Plaintiffs do not seem to seriously contend otherwise.[6]

Instead, Plaintiffs' principal argument with respect to the Historical Test is that the NDAA "falls within the scope of the historic work and employment bans." Pls.' Opp'n at 8. This argument is untenable.

There is no doubt that legislation barring specific individuals or groups of individuals from certain types of employment, or preventing them from pursuing certain vocations, constitutes "punishment" as that term has been historically understood. In fact, "the [Supreme] Court's four major decisions invalidating statutes on Bill of Attainder Clause grounds have all involved legislation preventing specific classes of persons from pursuing certain occupations." *BellSouth Corp. v. F.C.C.*, 144 F.3d 58, 64 (D.C. Cir. 1998) ("*BellSouth I*"). These decisions (hereinafter, the "Employment Ban Cases") include *United States v. Brown*, 381 U.S. 437 (1965), in which the Supreme Court invalidated a law that made it a crime for a member of the

[6] In a footnote, Plaintiffs make a cursory argument that the NDAA is a "punitive confiscation of property" because it will "diminish the value of the corporation" "if sold to a new owner." Pls.' Opp'n at 11 n.6. As an initial matter, Plaintiffs have no property interest in discretionary contracts that they may or may not have received from the federal government in the future. Regardless, the Court rejects the notion that any attenuated effect on a hypothetical future sale of Plaintiffs' corporation is the type of punitive "confiscation of property by the sovereign" that has historically been associated with bills of attainder. Plaintiffs cite nothing in support of that argument.

Communist Party to serve as an officer of a labor union, *United States v. Lovett*, 328 U.S. 303 (1946), in which the Court invalidated a law that prohibited payment of salary to three named federal employees who were members of the Communist Party, and *Cummings v. Missouri*, 71 U.S. 277 (1866) and *Ex parte Garland*, 71 U.S. 333 (1866), in which the Court struck down laws effectively preventing individuals who sympathized with the rebellion against the Union from engaging in certain professions.

The NDAA, however, is nothing like the legislation in these Employment Ban Cases. Sections 1634(a) and (b) of the NDAA have nothing to do with anyone's employment. They do not bar any individual from pursuing their livelihood or from engaging in any vocation. In fact, unlike the legislation in the Employment Ban Cases, these sections of the NDAA do not apply to any "flesh-and-blood" individuals at all. They apply to the products of a multinational corporation. Even assuming that the Bill of Attainder Clause applies to corporations in the abstract,[7] the fact that the legislation at issue here targets the products of a multinational corporation, instead of an individual, certainly distinguishes it from the "historic work and employment bans." *See BellSouth II*, 162 F.3d at 684 ("[I]t is obvious that there are differences between a corporation and an individual under the law," and "[t]hus, any analogy between prior cases that have involved individuals and this case, which involves a corporation, must necessarily take into account this difference."); *ACORN v. United States*, 618 F.3d 125, 137 (2d Cir. 2010) ("'[T]here may well be actions that would be considered punitive if taken against an individual, but not if taken against a corporation.'") (quoting *Consol. Edison Co. of New York*,

[7] *BellSouth I*, 144 F.3d at 63 ("We assume, as do the parties, that the Bill of Attainder Clause protects corporations as well as individuals."); *Consol. Edison Co. of New York v. Pataki*, 292 F.3d 338, 346-49 (2d Cir. 2002) (holding that the Bill of Attainder Clause applies to legislation that targets corporations as well as natural persons).

292 F.3d at 354). This distinction is an important one, because "[w]hen the [Supreme] Court extended 'punishment' to include employment bars, it did so because it was concerned that the government had imposed restrictions that violated the fundamental guarantees of political and religious freedom." *BellSouth II*, 162 F.3d at 686. That concern simply is not implicated here. A statute that does not apply to any individual but instead deprives a large multinational corporation of one of its many sources of revenue does not threaten anyone's personal rights or freedoms.

Moreover, even if there could be a case where depriving a corporation of a source of revenue had such a profound impact on its business that the deprivation effectively rose to the level of a work or employment ban, this is not that case. The effect on Kaspersky Lab of losing the United States federal government as a customer does not begin to compare to the effect of historically recognized "employment bans" on the targeted individuals. Those historically recognized bans have completely prevented individuals from being employed in certain positions or pursuing certain types of vocations. Kaspersky Lab is not prevented from operating as a cybersecurity business.[8] It is prevented from seeking discretionary contracts from the United States federal government. The company may still operate and derive revenue throughout the world, including in the United States, by selling its products to individuals, private companies, and other governments.

This is no meaningless concession. Kaspersky Lab concedes that sales to the United States federal government make up a *tiny* fraction of the company's overall business. In Kaspersky Lab's own words, "[o]ver 400 million users—from governments to private

[8] The Court rejects Plaintiffs' attempt to characterize their "vocation" as "direct and indirect federal government contracting." Pls.' Opp'n at 10. That is not a vocation.

individuals, commercial enterprise to critical infrastructure owners and operators alike—utilize Kaspersky Lab technologies." Gentile Decl. ¶ 9. "Active licenses held by federal agencies in September 2017 had a total value (to Kaspersky Lab, Inc. and the Company as a whole) of less than $54,000—approximately 0.03% of Kaspersky Lab, Inc.'s annual U.S. sales at the time." *Id.* There is simply no plausible way that the NDAA's prohibition on the federal government's use of Kaspersky Lab products—depriving that corporation of less than one percent of its revenue from sales in one country within which it operates—can be compared to the individual employment bans that have been struck down by the Supreme Court.

The D.C. Circuit has rejected the argument that regulations limiting the types of business which a company may engage in, or the products it may sell, thereby depriving that company of some revenue, are akin to a historical employment ban. In *BellSouth I*, the D.C. Circuit held that a line-of-business restriction "imposing structural separations on corporations seeking to engage in specific types of commercial activity" was not the same as "traditional employment debarments." 144 F.3d at 64-65. That court explained that such a restriction could not be fairly compared to employment bans because it left its subjects "free to pursue their" business goals, simply subject to requirements that, despite being "hardly costless," did not "remotely approach the disabilities that have traditionally marked forbidden attainders." *Id.* at 65; *see also Navegar, Inc. v. United States*, 192 F.3d 1050, 1066-67 (D.C. Cir. 1999) (holding that law preventing a company from selling particular products was not equivalent to historical employment bans). Plaintiffs here too are free to pursue their business goals. Their products simply will not be used by the federal government of the United States. While not costless, this restriction does not approach the degree of disability historically associated with bills of attainder.

Perhaps the weakness of Plaintiffs' argument on this point is best indicated by the caselaw that they are able to marshal in its support. Plaintiffs cite three out-of-circuit district court opinions, one of which is unpublished. These authorities are of course not binding and, in any event, do not discuss Plaintiffs' argument in depth. More importantly, all three opinions are clearly distinguishable. In all of them, unlike in this case, the legislation challenged had the effect of shutting down the businesses of, and/or laying off or terminating, actual "flesh-and-blood" people. In *Florida Youth Conservation Corps., Inc. v. Stutler*, No. 4:06CV275-RH/WCS, 2006 WL 1835967, at *1 (N.D. Fla. June 30, 2006), the court held (in an unpublished opinion at the preliminary injunction stage with six sentences addressing the bill of attainder issue) that a law barring a not-for-profit corporation from state contracting was "very much akin to the enactments that prompted the framers to include in the Constitution a prohibition on bills of attainder." That ruling, however, was in part based on the court's finding that the effect of the law "would be to put plaintiff out of business, or at least to put plaintiff out of the business in which it has been engaged to date." *Id.* In *Planned Parenthood of Central North Carolina v. Cansler*, 877 F. Supp. 2d 310, 324 (M.D.N.C. 2012), the court held (relying primarily on *Florida Youth Conservation Corps.*) that a law that prevented Planned Parenthood from any opportunity to apply for or receive government grants or contracts was "analogous to legislation that prohibits a person or entity from engaging in certain employment, which courts have historically found to be associated with punishment." That ruling, however, came after the court had determined in a previous opinion that the law at issue would require plaintiff to "close facilities" and "lay-off employees." *Planned Parenthood of Cent. N. Carolina v. Cansler*, 804 F. Supp. 2d 482, 498 (M.D.N.C. 2011). Finally, in *Mendelsohn v. Meese*, 695 F. Supp. 1474, 1486-89 (S.D.N.Y. 1988), the court held that the Anti-Terrorism Act was akin to historical forms of

punishment, but it did so because the law penalized a group of "employees"—i.e., flesh-and-blood people—"by closing their offices and effectively terminating their activities in the United States." In sum, even if the Court found the analysis in these non-binding district court opinions persuasive, they nevertheless would not prove Plaintiffs' point because, in each of them, individual people were prevented from pursuing their employment. They do not stand for the proposition that depriving a large multinational corporation like Kaspersky Lab of one tiny source of revenue is a historically recognized form of legislative punishment.

Finally, another reason that the challenged provisions of the NDAA are unlike the legislation in the Employment Ban Cases is that they do not brand Kaspersky Lab as disloyal, or express any determination that Kaspersky Lab is guilty of any wrongdoing. The decisions of the Supreme Court that have determined that employment bans are legislative punishment have done so "where the employment bans were imposed as a brand of disloyalty." *Foretich*, 351 F.3d at 1217. And, more generally, "[a] familiar theme in the[ ] classic examples of punishment is the initial determination by the legislature of 'guilt.'" *ACORN*, 618 F.3d at 136. The NDAA lacks these characteristics. As Plaintiffs repeatedly emphasize, the law appears to have nothing to do with any finding that Kaspersky Lab has done anything wrong or disloyal. Instead, it is premised on the determination that the use of that company's products to defend federal government networks and computer systems presents a national security vulnerability because they could be used (whether with or without Kaspersky Lab's knowledge or consent) by the Russian government. The law does not assume any guilt, disloyalty, or wrongdoing on the part of Kaspersky Lab.[9]

[9] Plaintiffs attempt to demonstrate that the law brands them as disloyal by pointing to Senator Jeanne Shaheen's public statements. The Court is not convinced. As discussed further

In sum, the Court finds that Plaintiffs have not plausibly alleged that the challenged provisions of the NDAA are legislative punishment under the Historical Test. Plaintiffs, perhaps foreseeing this result, have argued that the Court should nonetheless consider that the NDAA is not entirely incongruous with historical notions of punishment when weighing all three punishment tests together. Pls.' Opp'n at 8. The Court does consider the results of all three tests in their totality, but this does not help Plaintiffs. The next two tests clearly weigh against them.

b. The Functional Test

"[W]here an enactment falls outside the historical definition of punishment, therefore failing to satisfy the first test, the legislation may still be a bill of attainder under the functional test if no legitimate nonpunitive purpose appears." *Foretich*, 351 F.3d at 1218. The Court accordingly moves on to the Functional Test.[10]

The principal question under the Functional Test is "whether the law under challenge, viewed in terms of the type and severity of burdens imposed, reasonably can be said to further nonpunitive legislative purposes." *Nixon*, 433 U.S. at 475-76. "Under this functional test, the nonpunitive aims must be 'sufficiently clear and convincing' before a court will uphold a

---

below in the Court's analysis of the Motivational Test, the thrust of Senator Shaheen's statements demonstrates a purpose of preventing Russia from exploiting Kaspersky Lab products, not of punishing Kaspersky Lab for being disloyal. To the extent one could interpret some aspects of Senator Shaheen's statements differently, one-off statements by a single Senator to the media do not control the meaning or effect of a statute.

[10] Plaintiffs cite a Second Circuit opinion, *Consol. Edison Co. of New York v. Pataki*, 292 F.3d 338 (2d Cir. 2002), for the proposition that a statute that imposes a burden that falls within the historical meaning of legislative punishment is "per se" a bill of attainder. *See* Pls.' Opp'n at 8. This would appear to conflict with the statement of the D.C. Circuit that "'[e]ven measures historically associated with punishment—such as permanent exclusion from an occupation—have been otherwise regarded when the nonpunitive aims of an apparently prophylactic measure have seemed sufficiently clear and convincing.'" *BellSouth I*, 144 F.3d at 65 (quoting Laurence H. Tribe, *American Constitutional Law*, § 10–5, at 655 (2d ed.1988)). The Court notes this apparent discrepancy but need not resolve it because it finds that Sections 1634(a) and (b) do not fall within any historic meaning of legislative punishment.

disputed statute against a bill of attainder challenge." *Foretich*, 351 F.3d at 1221. "Courts have conducted this inquiry by examining both the purported ends of contested legislation and the means employed to achieve those ends." *Id.* The D.C. Circuit has emphasized that there must be "a rational connection between the burden imposed and nonpunitive purposes of the legislation." *Id.* "In other words, the means employed by the statute must be rationally designed to meet its legitimate nonpunitive goals." *Patchak*, 828 F.3d at 1006. "[T]here must be a nexus between the legislative means and legitimate nonpunitive ends." *Foretich*, 351 F.3d at 1221. "[W]here there exists a significant imbalance between the magnitude of the burden imposed and a purported nonpunitive purpose, the statute cannot reasonably be said to further nonpunitive purposes." *Id.*

Sections 1634(a) and (b) of the NDAA do not constitute legislative punishment under the Functional Test. These provisions of the NDAA serve a legitimate and eminently reasonable nonpunitive function: protecting the United States government's information systems from the threat of Russian cyber-intrusion. This is a prospective, risk-prevention function that is distinct from punishment.

Moreover, the challenged provisions of the NDAA are rationally related to this nonpunitive goal—that is, there is a nexus between the means Congress used and the nonpunitive end it sought to achieve.[11] As discussed in more detail above, Congress was presented with at

[11] Plaintiffs argue that the D.C. Circuit in *Foretich* instructed courts to consider "whether there is a 'coherent and reasonable nexus between the burden imposed and the benefit to be gained'" as part of the Historical Test. Pls.' Opp'n at 12-13. The Court actually understands the *Foretich* opinion to mean that this consideration is, under modern precedent, considered as part of the "Functional Test." *Foretich*, 351 F.3d at 1219 ("These early decisions foreshadowed the development of the functional test and reinforce the necessity of a coherent and reasonable nexus between the burden imposed and the benefit to be gained."). The Court has considered this factor, but has addressed it as part of its Functional Test analysis.

least the following set of facts: Russia had committed, and will likely continue to commit, malicious cyber-activities against the United States; the United States' federal government computer systems relied on Kaspersky Lab products to protect them from malicious cyber-activity; those products can be misused to exploit or harm the systems on which they are installed; Kaspersky Lab is headquartered in Russia and subject to Russian laws; and both Kaspersky Lab and its founder and CEO have connections to the Russian government and intelligence services.

It is not Plaintiffs' or this Court's role to determine *de novo* what precise actions should have been taken in light of this information to protect the nation's cyber-security. That function was reserved for the political branches. It is sufficient for this Court to say that it was rational for Congress to conclude on the basis of this information that barring the federal government's use of Kaspersky Lab products would help prevent further Russian cyber-attacks. *See Patchak*, 828 F.3d at 1006 ("[T]he means employed by the statute must be rationally designed to meet its legitimate nonpunitive goals."). In other words, this is not a case where Congress barred Plaintiff from an activity based on characteristics (*e.g.*, holding an unpopular political view) that had no rational connection with its suitability for that activity. Such a disconnect, which could suggest a punitive purpose, is absent here. Information suggesting that a company's products could be used by a foreign power known to be regularly attempting cyber-attacks on the United States rationally bears on that company's suitability to provide cyber-security products to the federal government. *See Flemming*, 363 U.S. at 614 ("Where the source of legislative concern can be thought to be the activity or status from which the individual is barred, the disqualification is not punishment even though it may bear harshly upon one affected. The contrary is the case where the statute in question is evidently aimed at the person or class of

persons disqualified."); *Siegel v. Lyng*, 851 F.2d 412, 418 (D.C. Cir. 1988) (finding that bar from employment in agricultural industry was not punishment because it was based on "legitimate justifications"—connection to an entity that had previously violated agricultural laws).

Congress' non-punitive purpose was also not out of balance with the burden that the NDAA places on Kaspersky Lab. "[M]erely because a regulation is burdensome does not mean that it constitutes punishment." *Navegar*, 192 F.3d at 1067. The Court must ask whether that burden, however great, is *out of balance* with the purpose of the regulation. Here, that is clearly not the case. On the one side of the scale in this case is Congress' goal of securing our Nation's networks and computer systems from malicious cyber-threats. The importance of this goal in today's world can hardly be overstated.

On the other side of the scale is the burden to Kaspersky Lab which, while real, is exaggerated by Plaintiffs. The NDAA deprives Kaspersky Lab of one of its revenue streams. But, as discussed above, that revenue stream represents a tiny portion of the company's overall business. And, although the prohibition also may have a negative effect on Kaspersky Lab's reputation in the cybersecurity field, that reputational harm is not as great as Plaintiffs suggest. Plaintiffs compare this case to *Foretich*, but the comparison is a stretch. The reputational burden the D.C. Circuit addressed in *Foretich* derived from Congress having effectively labeled a particular individual as a child molester who had sexually abused his own daughter. *See Foretich*, 351 F.3d at 1223. The Act "memorialize[d] a judgment by the United States Congress that [the plaintiff] was guilty of horrific crimes." *Id.*

The reputational burden in this case is not as severe. Through the NDAA, Congress has effectively declared that the use of Kaspersky Lab products by federal government agencies presents a security risk because those products could be used—whether with or without

Kaspersky Lab's knowledge or consent—by the Russian government. This understandably will affect Kaspersky Lab's reputation as a cybersecurity business, but it does not, as Plaintiffs repeatedly argue, label them as disloyal or adjudge them guilty of any "horrific crime." In sum, even considering the reduction in revenue and harm to reputation Plaintiffs allegedly suffered, this is not a case where "[a] grave imbalance or disproportion between the burden and the purported nonpunitive purpose suggests punitiveness." *Id.* at 1222. The burdens placed on Kaspersky Lab by the challenged provisions of the NDAA, although perhaps not trivial in absolute terms, are not out of balance with Congress' goal of protecting the Nation's cyber-security.

Plaintiffs argue that various aspects of Sections 1634(a) and (b) reveal that its actual function is punitive. First, Plaintiffs argue that the punitive nature of the NDAA is demonstrated by the fact that it singles out Kaspersky Lab and no other cybersecurity vendors. Indeed, Plaintiffs at times go so far as to imply that the law is *inherently* a bill of attainder because it is not one of general applicability. *See, e.g.*, Pls.' Opp'n at 22-23. This argument is not persuasive. It is true that the specificity of a law is one factor that the Court may consider when determining whether a law is punitive. *See Foretich*, 351 F.3d at 1222. However, it is also true that specificity alone is not sufficient to establish that a law has a punitive function. *See Nixon*, 433 U.S. at 470-71 (rejecting notion that a law was a bill of attainder simply because it "impose[d] undesired consequences on an individual or on a class that is not defined at a proper level of generality" because this notion, if accepted, would "cripple the very process of legislating, for any individual or group that is made the subject of adverse legislation [could] complain that the lawmakers could and should have defined the relevant affected class at a greater level of generality."); *ACORN*, 618 F.3d at 138-39 (explaining that specificity is relevant to assessing an

alleged punitive purpose but "does not create a presumption of unconstitutionality"). Where a law targets a particular individual (or corporation) because there is a legitimate nonpunitive reason to take such targeted action, specificity is not improper and does not evince punishment. *See Nixon*, 433 U.S. at 472 (holding that law was not objectionable solely because it singled out President Richard Nixon, because Congress had reason to conclude that action against President Nixon specifically "demanded immediate attention"); *SeaRiver Mar. Fin. Holdings, Inc. v. Mineta*, 309 F.3d 662, 676 (9th Cir. 2002) (holding that focus on removing a particular tank vessel from the Prince William Sound did not evince a punitive purpose because it was reasonable to conclude that prompt action with respect to that vessel in particular was necessary).

That was the case here. Grappling with a real-time need to take action to protect the government's networks and computer systems from cyber-attacks, Congress opted to pass a law of general applicability that ordered the review of procedures for removing suspect products and services from federal systems going forward (Section 1634(c)), and also immediately took action to stem a perceived risk caused by the government's use of one company's products in particular based on facts already known (Sections 1634(a) and (b)). There was nothing improper about this course of action. The record indicates that no other cybersecurity vendor had the same set of characteristics that had caused concerns about Kaspersky Lab. AR770. It was therefore reasonable for Congress to act only with respect to that company.

Plaintiffs also argue that Sections 1634(a) and (b) of the NDAA do not have a legitimate nonpunitive function because Congress could have employed less burdensome alternatives and because the statute lacks "safeguards" for Kaspersky Lab's rights. Plaintiffs' considerable reliance on these points is misplaced. These are merely factors the Court may consider when determining whether a law had a nonpunitive purpose. They are not requirements. Neither the

Supreme Court nor the D.C. Circuit has held that the Court may invalidate a law with a clear nonpunitive purpose that is rationally designed to further that purpose simply because it lacks "safeguards" for a class that is burdened by the law. Nor have those courts held that it is necessary, or appropriate, for the Court to apply a "least restrictive means test" to laws challenged as bills of attainder.

Additionally, the principal "less burdensome alternative" proffered by Plaintiffs—"refer[ing] the matter to the executive branch to consider" proceedings to debar Kaspersky Lab under the FAR, Pls.' Opp'n at 29—would not have accomplished Congress' nonpunitive goal. Debarment would have only applied to future transactions between Kaspersky Lab and the government—it would not have required federal agencies to remove Kaspersky Lab products they had previously purchased and installed. AR0631. Nor would debarment have prohibited third parties from selling Kaspersky Lab products to federal agencies. *Id.* Accordingly, debarment would not have prevented agencies from *using* Kaspersky Lab products.

To the extent Plaintiffs argue that the prohibition could have been limited to only Kaspersky Lab *software* (not hardware or services), or should have provided Kaspersky Lab a means to "extricate itself from the ban," Pls.' Opp'n at 27, the Court is not convinced that these characteristics of the NDAA cast any doubt on its nonpunitive function. Considering the extensive record regarding Kaspersky Lab that was before Congress, it was reasonable for Congress to conclude that a broad and permanent ban was necessary to prevent the sort of cyber-attacks about which Congress was concerned. Plaintiffs believe that the law could have been designed better but, as already stated, it is not the Court's role to review *de novo* the technical decisions Congress makes to protect the Nation's cyber-security. It is enough that a "rational and fairminded Congress" could have determined that the approaches urged by Plaintiffs would

not have accomplished its nonpunitive goals. *Nixon*, 433 U.S. at 483. The Court easily concludes that that is the case here.

For the foregoing reasons, Sections 1634(a) and (b) of the NDAA have a clear nonpunitive function. The means Congress employed to accomplish that function are rational, and the burdens imposed by the NDAA are not out of balance with the importance of its nonpunitive goal. Therefore, the Functional Test shows that the law does not constitute punishment.

c. The Motivational Test

"The final test of legislative punishment is 'strictly a motivational one: inquiring whether the legislative record evinces a congressional intent to punish.'" *Foretich*, 351 F.3d at 1225 (quoting *Nixon*, 433 U.S. at 478). "Under this prong, a court must inspect legislation for a congressional purpose to 'encroach[ ] on the judicial function of punishing an individual for blameworthy offenses.'" *Id.* (quoting *Nixon*, 433 U.S. at 479). "Courts conduct this inquiry by reference to legislative history, the context or timing of the legislation, or specific aspects of the text or structure of the disputed legislation." *Id.*

The Motivational Test "by itself is not determinative in the absence of 'unmistakable evidence of punitive intent.'" *Id.* (quoting *Selective Serv. Sys*., 468 U.S. at 856 n.15). The Court approaches the Motivational Test with caution, because "[j]udicial inquiries into Congressional motives are at best a hazardous matter." *Flemming*, 363 U.S. at 617. When a law is claimed to impose legislative punishment on the basis of such an inquiry, "only the clearest proof could suffice to establish the unconstitutionality of [the] statute." *Id.*; *see also ACORN*, 618 F.3d at 141 ("The legislative record by itself is insufficient evidence for classifying a statute as a bill of attainder unless the record reflects overwhelmingly a clear legislative intent to punish.").

Presumably in light of this daunting standard, Plaintiffs disavow any argument that Sections 1634(a) and (b) of the NDAA constitute a bill of attainder on the basis of the Motivational Test alone. *See* Pls.' Opp'n at 30 ("Plaintiffs are not challenging the constitutionality of the NDAA on 'this prong itself.'"). They contend only that this test "bolsters" their showing that the NDAA is punishment. *Id.* Even this modest claim, however, is wrong. The Motivational Test does not "bolster" Plaintiffs' argument. If anything, it weakens it.

Plaintiffs' primary argument under the Motivational Test is that the record related to Congress' decision to prohibit the use of Kaspersky Lab products is "silent." Pls.' Opp'n at 3. There are two major flaws with this argument. The first is that, even if it was accurate, it would *defeat* Plaintiffs' claim. Statutes are presumed constitutional. *See Flemming*, 363 U.S. at 617 ("[T]he presumption of constitutionality with which this enactment, like any other, comes to us forbids us lightly to choose that reading of the statute's setting which will invalidate it over that which will save it."). It is Plaintiffs' burden under the Motivational Test to demonstrate that Congress was motivated to punish Kaspersky Lab. *See BellSouth I*, 144 F.3d at 67 (finding that law was not punishment under the Motivational Test where plaintiff had not "come forward" and "provided" any evidence on Congress' purpose). If the record was in fact "silent," Plaintiffs could not do so. *See SeaRiver*, 309 F.3d at 677 ("The congressional silence surrounding § 2737 impedes SeaRiver in successfully carrying its burden on this factor."). Congress' silence, even when coupled with an awareness that its actions will harm a particular individual or company, is not sufficient to demonstrate punitive intent. *See Patchak*, 828 F.3d at 1007 ("While it may be true that Mr. Patchak was adversely affected as a result of the legislation, the record does not show that Congress acted with any punitive or retaliatory intent."); *SeaRiver*, 309 F.3d at 674

("Although Congress was aware when it passed § 2737 that it would impose a cost on SeaRiver, this awareness does not translate into a suggestion that Congress's intent was to punish").

The second problem with Plaintiffs' "silence" argument is that it is incorrect as a matter of fact. As the Court described at length in the Background section of this Opinion, the NDAA was passed after months of congressional inquiries into the risk of Russian cyber-attacks created by the federal government's use of Kaspersky Lab products. The Court will not repeat that entire history here, but notes that concerns were raised at various committee hearings, and six United States intelligence directors, including the directors of the CIA and the NSA, told the Senate Select Committee on Intelligence that they would not be comfortable using Kaspersky Lab products on their computers. In addition, a Senate Armed Services Committee report discussing the prohibition on Kaspersky Lab products stated that the prohibition was a response to "reports that the Moscow-based company might be vulnerable to Russian government influence." NDAA FY 2018, U.S. Senate Armed Services Committee, at 10, https://www.armed-services.senate.gov/imo/media/doc/FY18%20NDAA%20Summary6.pdf. Although drawing conclusions about Congress' motivation is a "hazardous" endeavor, *Flemming*, 363 U.S. at 617, as a whole, this record suggests a motivation to take preventive action to eliminate a risk of Russian cyber-attacks, not to punish Kaspersky Lab.[12]

Plaintiffs argue that certain statements Senator Jeanne Shaheen made to the media show that Congress was motivated to punish. As described above, Senator Shaheen stated in a press

[12] Plaintiffs argue that most of this history should be ignored because it is not formal legislative history addressing the exact amendment to the NDAA that resulted in the prohibition at issue. Plaintiffs take far too narrow a view of the types of material that the Court may consider when assessing Congress' motivation under the Motivational Test. As the D.C. Circuit has held, courts may consider "the context or timing of the legislation." *Foretich*, 351 F.3d at 1225. This congressional activity provides helpful context that informs the Court's understanding of Congress' motivation.

release that "[t]he case against Kaspersky Lab is overwhelming." *See* Compl., Ex. E, NDAA ECF No. 1-5. She elaborated that:

> The strong ties between Kaspersky Lab and the Kremlin are alarming and well-documented. I'm very pleased that the Senate has acted in a bipartisan way on my amendment that removes a real vulnerability to our national security. I applaud the Trump administration for heeding my call to remove Kaspersky Lab software from all federal computers. It's important that this prohibition also be a part of statute and be expanded to the entire federal government, as my amendment would do. Considering the strong bipartisan, bicameral support for this proposal, I'm optimistic this will soon be signed into law.

Id. Additionally, in an editorial authored for the *New York Times*, Senator Shaheen wrote that the presence of Kaspersky Lab products on federal systems created a "threat" of Russian cyber-interference, and that she was proposing to bar federal government use of those products "to close this alarming national security vulnerability." *See* Compl., Ex. C, NDAA ECF No. 1-3.

These statements do not indicate that Congress' motivation was to punish Kaspersky Lab. As an initial matter, the overall emphasis of Senator Shaheen's statements was not that Congress should punish Kaspersky Lab for anything, but instead that the use of Kaspersky Lab products to defend federal government systems created a risk of Russian cyber-interference, and that action needed to be taken swiftly to address this vulnerability. It was the "case" for such action, according to Senator Shaheen, that was "overwhelming."

Additionally, even if these statements could be interpreted as indicating that Senator Shaheen was motivated to punish Kaspersky Lab—and the Court does not interpret them that way—isolated statements of one legislator are not sufficient under the Motivational Test to demonstrate a punitive motivation. "'Several isolated statements' are not sufficient to evince punitive intent." *BellSouth II*, 162 F.3d at 690 (quoting *Selective Serv. Sys.*, 468 U.S. at 856

n.15); *Navegar*, 192 F.3d at 1067 (holding that "isolated statements are not sufficient to show a punitive intent"); *ACORN*, 618 F.3d at 142 (holding that "smattering" of legislators' opinions regarding plaintiff's guilt of fraud was insufficient to demonstrate motivation to punish). In other words, even if *Senator Shaheen's* intention in passing the NDAA's prohibition on Kaspersky Lab products was to punish that company, as opposed to merely limit the risk of future Russian cyber-attacks, that intention of a sole senator is not sufficient to demonstrate that Congress as a whole was motivated to punish.

Also relevant to the Court's Motivational Test inquiry is that the NDAA was passed on the heels of actions by the Executive Branch addressing similar concerns about Kaspersky Lab products. Most importantly, Congress was considering the NDAA's prohibition on Kaspersky Lab products at the same time that DHS was in the midst of its BOD 17-01 proceedings. Congress even held hearings about those proceedings. By statute, BODs are used "for purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk"—not to impose punishment based on any wrongdoing. 44 U.S.C. § 3552(b)(1). The purpose of BOD 17-01 in particular was to stem the risk of Russian cyber-attacks, and DHS made clear that the action was not based on any assumption that Kaspersky Lab had done, or would do, anything wrong or worthy of punishment. AR0629. It is reasonable to assume that Congress had a similar motivation when, after overseeing the implementation of BOD 17-01, it passed a prohibition very similar to that BOD just days after it was finalized.

Additionally, "specific aspects of the text or structure" of Section 1634, such as the provision's placement within the NDAA, indicate Congress' nonpunitive motivation. *See Foretich*, 351 F.3d at 1225; *see also BellSouth I*, 144 F.3d at 66 (noting that a claim of punitive

purpose can be undermined by a provision's placement within an Act). Section 1634 falls under a subtitle of the NDAA entitled "Cyberspace-Related Matters." This section of the NDAA does not dole out punishments. It provides authorizations, sets policies, and requires reporting on various cyber-security issues. Section 1634(c), which follows immediately after the challenged sections, is one example: it requires agencies to conduct reviews of their procedures for removing suspect products or services from the information technology networks of the federal government. That the prohibition on Kaspersky Lab products falls within this section of the NDAA indicates that Congress viewed it as a similar cyber-security measure, not punishment.

The text and effect of the statutory sections themselves also indicate Congress' nonpunitive motivation. The statute does not prohibit *purchases* from Kaspersky Lab, but instead the *use* of Kaspersky Lab products. This required the government to undergo a time-intensive and costly process of identifying and discontinuing the "use" of Kaspersky Lab products throughout the government. If Congress' purpose was simply to punish Kaspersky Lab for something, it could have accomplished that goal in a far easier and cheaper manner by simply barring any future purchases from that company. The fact that it declined that option and instead ordered that all "use" of Kaspersky Lab products be halted, and incurred the considerable cost to do so,[13] suggests that the function of the law was to protect against prospective Russian cyber-threats, not to punish Kaspersky Lab.

In sum, it was Plaintiffs' burden to plausibly allege facts that would suggest that Sections 1634(a) and (b) were punishment under the Motivational Test. Their inability to do so defeats their claim. In addition, the record—including congressional activity, administrative activity,

[13] The Government also points out that if Congress had intended to punish Kaspersky Lab, it might have required the company to bear the cost of removing its own products, but Congress opted not to do so.

and the nature of the statute itself—affirmatively indicates a *nonpunitive* motivation. Accordingly, the Court concludes that Plaintiffs cannot plausibly establish that the challenged provisions constitute legislative punishment under the Motivational Test.

* * *

Weighing all three tests for punishment together, the Court concludes that Sections 1634(a) and (b) of the NDAA clearly do not inflict punishment on Plaintiffs. The law does not impose any form of historically recognized legislative punishment. It has an obvious and eminently reasonable nonpunitive purpose and, although the law has negative effects on Plaintiffs, those effects are not out of balance with the goal of protecting the Nation's cyber-security. Finally, there is no evidence that Congress acted with any motivation to punish Plaintiffs.

The Court emphasizes that "[i]n order to decide whether a statute impermissibly inflicts punishment, [the Court] consider[s] each case in 'its own highly particularized context.'" *Patchak*, 828 F.3d at 1006 (quoting *Selective Serv. Sys.*, 468 U.S. at 852); *see also Flemming*, 363 U.S. at 616 ("[E]ach case [ ] turn[s] on its own highly particularized context."). The context of this case—Congress' real-time attempt to address cutting edge and constantly evolving cyber-threats to some of our Nation's most sensitive strategic assets—is extremely unique. Viewed in this unique context, for the reasons explained above, the challenged provisions of the NDAA cannot plausibly be said to be a bill of attainder. Plaintiffs' NDAA Lawsuit will accordingly be dismissed.

B. The BOD Lawsuit

Plaintiffs' BOD Lawsuit will also dismissed, but for a different reason. Article III of the Constitution limits the jurisdiction of this Court to the adjudication of "Cases" and

"Controversies." U.S. Const., Art. III, § 2. "In an attempt to give meaning to Article III's case-or-controversy requirement, the courts have developed a series of principles termed 'justiciability doctrines,' among which [is] standing." *Nat'l Treasury Emps. Union v. United States*, 101 F.3d 1423, 1427 (D.C. Cir. 1996) (citing *Allen v. Wright*, 468 U.S. 737, 750 (1984)). Standing requires, in essence, that a plaintiff have "a personal stake in the outcome of the controversy . . . ." *Warth v. Seldin*, 422 U.S. 490, 498 (1975). The familiar requirements of Article III standing are:

> (1) that the plaintiff have suffered an "injury in fact"—an invasion of a judicially cognizable interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) that there be a causal connection between the injury and the conduct complained of—the injury must be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court; and (3) that it be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.

Bennett v. Spear, 520 U.S. 154, 167 (1997) (citing *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992)); *see also Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016).

Plaintiffs cannot satisfy these requirements in the BOD Lawsuit. Plaintiffs assert that they have standing to challenge BOD 17-01 because it causes them two types of injury: it prevents them from selling to the United States federal government, and it damages their reputation. To establish standing in the BOD Lawsuit, Plaintiffs must show "'that it [is] likely, as opposed to merely speculative, that the[se] injur[ies] will be redressed by a favorable decision'" in that suit. *Chamber of Commerce of U.S. v. E.P.A.*, 642 F.3d 192, 200 (D.C. Cir. 2011) (quoting *Bennett*, 520 U.S. at 167). Plaintiffs cannot make that showing. After BOD 17-01 was finalized, Congress separately passed an even broader prohibition on Kaspersky Lab products: Sections 1634(a) and (b) of the NDAA. Regardless of the outcome of the BOD

Lawsuit, those provisions of the NDAA will be the law. Sections 1634(a) and (b) of that law cause, *at least*, the same alleged harms as BOD 17-01. Therefore, even if Plaintiffs were successful and the Court were to order the rescission of the BOD, their harms would not be redressed. The Court has no jurisdiction to proceed to the merits of a lawsuit where its ultimate decision will have no real effect.

The NDAA has never been challenged as part of the BOD Lawsuit. Plaintiffs did eventually file a separate lawsuit challenging the NDAA (the NDAA Lawsuit, discussed above), but the two suits have always been, and remain, separate and distinct. The filing of a separate lawsuit challenging the NDAA did not have any effect on the Court's consideration of standing in the BOD Lawsuit, given that standing is determined at the time of the commencement of suit, and the NDAA Lawsuit was filed after the BOD suit. *See Lujan*, 504 U.S. at 571 n.5 ("standing is to be determined as of the commencement of suit"). Regardless, even assuming that the NDAA Lawsuit was relevant in any way to Plaintiffs' standing in the BOD Lawsuit, the NDAA Lawsuit has been dismissed. Accordingly, the Court assesses Plaintiffs' standing in the BOD Lawsuit assuming that, regardless of the outcome of that suit, the NDAA will remain in place.

It is a well-established principle that a plaintiff cannot demonstrate redressability when its lawsuit challenges only one of two government actions that both independently produce the same alleged harm. *See Delta Const. Co. v. E.P.A.*, 783 F.3d 1291, 1296 (D.C. Cir. 2015) (holding that petitioners did not have standing to challenge Environmental Protection Agency standards that allegedly raised the price of vehicles due to lack of redressability because the National Highway Traffic Safety Administration had promulgated substantially identical standards that were not challenged in the lawsuit, and therefore "even were we to vacate the EPA standards, the NHTSA standards would still increase the price of vehicles"); *Texas v. E.P.A.*, 726 F.3d 180, 198

(D.C. Cir. 2013) (dismissing challenge to administrative rules for lack of standing because vacating those rules "would not redress the State petitioners' injury," which was separately caused by a statute); *Renal Physicians Ass'n v. U.S. Dep't of Health & Human Servs.*, 489 F.3d 1267, 1277 (D.C. Cir. 2007) (finding that plaintiff challenging a regulatory safe harbor had not satisfied the redressability prong because "[e]ven if a court invalidated the safe harbor, dialysis facilities would remain obligated under the Stark Law to pay no more than fair market value for medical director services").

This principle applies with full force in this case. Sections 1634(a) and (b) of the NDAA are not challenged in the BOD Lawsuit and cause both of the injuries Plaintiffs claim to suffer as a result of BOD 17-01.

First, like BOD 17-01, the NDAA prevents Plaintiffs from selling to the United States federal government. The NDAA requires that all federal agencies stop using all Kaspersky Lab products and services. In fact, the prohibition in the NDAA is broader than the prohibition in BOD 17-01, because it includes *all* Kaspersky Lab products and services (not just "Kaspersky-branded" products), and because it does not exempt any national security systems. The fact that the NDAA's prohibition does not technically become effective until October 1, 2018, does not change this analysis. There is no redressability unless a decision in Plaintiffs' favor would "produce tangible, meaningful results in the real world." *Common Cause v. Dep't of Energy*, 702 F.2d 245, 254 (D.C. Cir. 1983). No meaningful results would be produced by lifting BOD 17-01's prohibition on Kaspersky Lab products for the few months before the NDAA's prohibition goes into effect. Under the NDAA, federal agencies must have identified and halted the use of all Kaspersky Lab products by October 1, 2018. This is not contingent on the outcome of any review process. It is a date certain by which all use must stop. Under these

circumstances, it is highly implausible that, upon learning that BOD 17-01 was rescinded, any federal government agency would purchase a Kaspersky Lab product, obtain the necessary approval to use that product, install it, and begin using it, only to have to remove it again by October 1, 2018. To do so would not only defy common sense, it would also likely violate each federal agency's obligations under FISMA to reduce the risks to their information systems in a cost-effective manner.

Defendants have provided the Court with a declaration from the Acting Federal Chief Information Security Officer at the OMB, Grant Schneider, attesting to these points. Mr. Schneider's job is to oversee the development of government-wide cybersecurity policy and Federal civilian agency implementation of cybersecurity laws and policies. *See* Decl. of Grant Schneider, BOD ECF No. 13-1, ¶ 1. In his declaration, he states that "federal agencies are widely aware of the NDAA prohibition" and that "even if BOD 17-01 were rescinded before October 1, 2018, no federal agency would be likely to procure, test and install Kaspersky products, and then remove them, all before the October 1st NDAA effective date." *Id.* ¶ 5. He explains that "each federal agency makes its own independent IT acquisition decisions as long as the agency complies with applicable law and executive branch policy," and the personnel involved in those decisions "are acutely aware of the need to avoid use of IT products that increase risks to their information and information systems." *Id.* ¶ 6. In particular, agencies are aware of their obligations under FISMA to reduce risks to their information systems in a cost-effective manner, and are separately required under Executive Order and OMB policy to implement information security and cybersecurity risk management plans and measures. *Id.*

"Rescinding the BOD would not eliminate the security concerns underlying the decision to issue the directive in the first place," Mr. Schneider attests, which had been raised by other

lawmakers and intelligence officials, and which are also memorialized by the NDAA. *Id.* ¶ 7. Even if the BOD were rescinded, these agencies would still have to confront these concerns. They would have to determine that using Kaspersky Lab software in the months before the NDAA officially takes effect is an acceptable risk to their networks, and that purchasing those products, acquiring the necessary authorizations to use them and taking the time and resources to test, install, and deploy them—only to then immediately remove them prior to October 1, 2018—would be cost-effective and not wasteful. *Id.* ¶¶ 7-10. Mr. Schneider finds it "highly unlikely" that any agency's Chief Information Officer would make these determinations and choose to use Kaspersky Lab products between now and October 1, 2018, if the BOD was rescinded. *Id.* ¶ 7. In fact, according to Mr. Schneider, purchasing these products could open an agency up to investigation for wasteful procurement. *Id.* ¶¶ 8, 11.

Plaintiffs do not seriously attempt to dispute these points. Instead, Plaintiffs respond to Defendants' standing argument by attempting to recast their alleged injury as being deprived of the "*right* to sell to the government" until October 1, 2018. Pls.' Reply and Opp'n at 5 (emphasis in original). Regardless of whether any United States government agency would purchase their products, Plaintiffs argue, they stand to win back this "right to sell."

This asserted "right" is worthless. To "sell" requires another to "buy." Because no government agency would buy Plaintiffs' product in the period before October 1, 2018, Plaintiffs' theoretical "right" to sell has no value at all in the real world. The asserted deprivation of this empty procedural right would not affect any substantive or concrete interest of the Plaintiffs, and therefore is not sufficient to confer standing. *See Summers v. Earth Island Inst.*, 555 U.S. 488, 496-97 (2009) (rejecting standing based on a "procedural injury, namely, that [respondents] have been denied the ability to file comments on some Forest Service

actions," because "deprivation of a procedural right without some concrete interest that is affected by the deprivation—a procedural right *in vacuo*—is insufficient to create Article III standing"); *Sierra Club v. E.P.A.*, 754 F.3d 995, 1002 (D.C. Cir. 2014) ("[B]ecause Petitioners have failed to establish that they will likely suffer a substantive injury, their claimed procedural injury—being denied the right to comment on the Memorandum—necessarily fails.").

Second, the NDAA will continue to cause the same (or worse) harm to Plaintiffs' reputation as does BOD 17-01, even if the latter is rescinded. Even assuming that Plaintiffs can demonstrate that BOD 17-01 caused the reputational harms they allege, there are "circumstances in which governmental action is a substantial contributing factor in bringing about a specific harm, but the undoing of the governmental action will not undo the harm, because the new status quo is held in place by other forces." *Renal Physicians Ass'n*, 489 F.3d at 1278. That is the case here. The NDAA would preserve the new *status quo* with respect to Plaintiffs' reputation even if BOD 17-01 was rescinded. As Plaintiffs concede, it is their burden to show that "rescission likely would redress the discrete harm stemming from the BOD's labelling of Plaintiffs' products as 'information security risks' to federal government information systems.'" Pls.' Reply and Opp'n at 10. Plaintiffs cannot make this showing. As has been discussed already at length, BOD 17-01 and Sections 1634(a) and (b) of the NDAA are roughly equivalent prohibitions on Kaspersky Lab products, based on approximately the same concerns about the company. For this reason, Plaintiffs allege that the NDAA, like BOD 17-01, causes them "profound reputational injuries." Compl., NDAA ECF No. 1, ¶ 45. If anything, the effect of the NDAA on Plaintiffs' reputation would be greater than the effect of the BOD, because the NDAA codifies the prohibition against Plaintiffs' products into law and is broader than BOD 17-01 (covering all Kaspersky Lab products and services and all federal information systems).

Whatever harm was caused by the BOD labelling Plaintiffs' products as risks would not be redressed if the BOD was rescinded, because the NDAA would remain in place, continuing to label Plaintiffs' products in exactly the same way. And to the extent there is some distinct incremental harm that the existence of the BOD could be said to have on Plaintiffs' reputation above and beyond the existence of the NDAA, and therefore could be at stake in this lawsuit, that theoretical harm is simply "too vague and unsubstantiated" to support standing. *McBryde v. Comm. to Review Circuit Council Conduct & Disability Orders of Judicial Conference of the United States*, 264 F.3d 52, 57 (D.C. Cir. 2001) (in discussing standing and mootness based on incremental effect on reputation of a particular government action, noting that "[a]t some point . . . claims of reputational injury can be too vague and unsubstantiated to preserve a case from mootness"); *see also Lebron v. Rumsfeld*, 670 F.3d 540, 562 (4th Cir. 2012) (where plaintiff sought order enjoining the government from designating him as an enemy combatant, ruling that plaintiff did not have standing based on reputational injury because "[i]t is hard to imagine what 'incremental' harm it does to Padilla's reputation to add the label of 'enemy combatant' to the fact of his convictions and the conduct that led to them").

Plaintiffs argue that their standing is established by the D.C. Circuit's opinion in *Foretich*. The Court disagrees. The *Foretich* court did find that a plaintiff had standing based on an injury to his reputation. Moreover, that court did hold that the plaintiff had standing despite the fact that his reputation was harmed by the challenged law as well as other factors (e.g., publicity surrounding an underlying custody dispute and allegations in that dispute). *Foretich*, 351 F.3d at 1216. However, in *Foretich*, there was only one government determination that harmed plaintiff's reputation. Plaintiff's "reputational harms resulted directly" from a law that "embodie[d] a congressional determination that he engaged in criminal acts of child abuse from

which his daughter needed protection." *Id.* at 1211. The D.C. Circuit found that declaring that law unconstitutional would have redressed plaintiff's reputational harm because it would have "remove[d] the imprimatur of government authority from" that determination. *Id.* at 1215.

This simply is not the case here. In this case, there are multiple government determinations about Kaspersky Lab at issue—most importantly BOD 17-01 and the NDAA, but also apparent determinations by intelligence chiefs and the GSA—that make the same finding about Kaspersky Lab products that allegedly harms Plaintiffs' reputation. Accordingly, ordering the rescission of BOD 17-01 would not "remove the imprimatur of government authority" from the determination that Kaspersky Lab products present a risk to federal government networks. The *Foretich* court was not presented with these facts. *See Paracha v. Obama*, 194 F. Supp. 3d 7, 10-11 (D.D.C. 2016) *aff'd sub nom. Paracha v. Trump*, 697 F. App'x 703 (D.C. Cir. 2017) (finding no causation or redressability in case where petitioner challenged statutes labelling him a terrorist because, unlike in *Foretich*, petitioner presented no evidence that his reputational injury "derive[d] directly" from the challenged statutes, given that "petitioner [would] remain designated as an enemy combatant and will continue to be detained as such even if the Court rules in his favor").

In short, it is simply not plausible, let alone likely, that a favorable decision in the BOD Lawsuit ordering the rescission of that agency action on APA and procedural grounds would have any meaningful effect on Plaintiffs' reputation, where the same determinations about Kaspersky Lab products expressed by the BOD are codified in the NDAA and have also been expressed by numerous other government actors.

The Court also notes that, for many of the same reasons discussed above with respect to the redressability element, Plaintiffs also cannot demonstrate the causation requirement of

standing with respect to their alleged reputational harm. "Courts are powerless to confer standing when the causal link is too tenuous." *Winpisinger v. Watson*, 628 F.2d 133, 139 (D.C. Cir. 1980). As discussed above, BOD 17-01 is but one of a number of congressional and Executive Branch actions that would presumably have the same type of alleged effects on Kaspersky Lab's reputation. Prior to the issuance of BOD 17-01, various congressional committees were investigating the company, six intelligence directors had told the Senate Select Committee on Intelligence that they would not be comfortable using Kaspersky Lab products on their computers, and the GSA had removed the company as a vendor. All of these acts presumably had negative impacts on Plaintiffs' reputation. Plaintiffs cannot demonstrate that the BOD, and not these other acts, caused their reputational injury.

IV. CONCLUSION

For the reasons set out above, the Court will dismiss both Plaintiffs' NDAA Lawsuit and their BOD Lawsuit. The NDAA Lawsuit is dismissed for failure to state a claim, because Plaintiffs have not plausibly alleged that Sections 1634(a) and (b) of the NDAA constitute a bill of attainder. The BOD Lawsuit is dismissed for lack of standing because, even if Plaintiffs were to succeed in that lawsuit and the Court were to order the rescission of BOD 17-01, none of Plaintiffs' alleged harms would be redressed. They would continue in full force as a result of the NDAA. Because the BOD Lawsuit is dismissed for lack of standing, the Court need not reach the parties' cross-motions for summary judgment. Appropriate Orders accompany this Memorandum Opinion in each lawsuit.

/s/
COLLEEN KOLLAR-KOTELLY
United States District Judge