UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

KASPERSKY LAB, INC.; and KASPERSKY LABS LIMITED,	)	
Plaintiffs,	)	
v.	)	Civ. No. 17-2697 (CKK)
U.S. DEPARTMENT OF HOMELAND SECURITY; and KIRSTJEN NIELSEN *Secretary of Homeland Security*	)	
Defendants.	)	

REPLY MEMORANDUM IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

REGULATIONS

INTRODUCTION

The government has shown that Kaspersky lacks standing because rescinding the BOD would not redress the legal or reputational harms alleged in the complaint. In particular, it has shown that vacating one allegedly harmful law only to leave a functionally identical one in place can never amount to a meaningful Article III remedy. Kaspersky does not seriously dispute the governing standing law, and it more or less concedes that, so long as the NDAA's government-wide ban is in place, lifting the BOD would in no way affect its inability to obtain a federal contract.

The company's primary response has been to hope the Court will accept its second lawsuit as a cure for the standing defects in the first. But this Court cannot simply assume the NDAA ban away based on a challenge to the statute in a separate action, which is still at the pleading stage. Nor can it accept Kaspersky's effort to make its asserted Article III injury appear redressable by recasting it in vague procedural terms. The only way Kaspersky can satisfy Article III is to identify a concrete harm that can be relieved by a judicial decree rescinding the BOD while the NDAA ban remains in place. Kaspersky has not made that showing. This case should be dismissed.

Kaspersky's claims fare no better on the merits. Kaspersky received notice and a meaningful opportunity to respond before the BOD affected its legal rights, and the government has shown that the administrative process satisfied, and in key ways exceeded the procedural protections afforded to contractors subject to debarment. Kaspersky's challenge rests on the unsupportable assumption that it was entitled to due process before DHS took action that was "injurious" to the company, regardless of whether such action deprived the company of a constitutionally protected interest. No court has accepted such an expansive theory of procedural due process.

Finally, the government has shown that the Secretary's determination as to whether a cyber threat is serious enough to warrant invocation of the BOD authority is committed to agency

discretion and outside the scope of Administrative Procedure Act (APA) review. Multiple plaintiffs have brought APA challenges seeking to enjoin agency decisions under the Federal Information Security Modernization Act of 2014 (FISMA) and its predecessor statute. Not one has prevailed, and every court to consider the issue has agreed that decisions under these statutes are committed to agency discretion and thus outside the scope of APA review. Kaspersky believes its APA claim should be more successful because it is the first to challenge an agency's FISMA decision on its merits. But the fact that Kaspersky's challenge goes *further* than those that have been uniformly rejected before it hardly supports the case for judicial review.

Even if APA review were appropriate, the unclassified record provides ample support for DHS's determination that Kaspersky software presents known and reasonably suspected risks to federal information and information systems. Kaspersky's main grievance — that DHS improperly relied on press reports in the unclassified portion of the administrative record — is foreclosed by D.C. Circuit precedent. But in any case, the record can be sustained on summary judgment with or without the press reports. The Acting Secretary's decision was informed by recommendations from DHS's top cybersecurity officials, including hundreds of pages of evidence and written analysis, aside from the press reports, that document the normal operation of antivirus software, which provides broad access to files and elevated privileges on the computers on which the software is installed; the rapidly evolving Russian cyber threat; the prospect of Russian agents or Kaspersky using antivirus software running on federal networks as a platform for malicious cyber operations; and the reasons why Kaspersky software poses an intolerably high risk of falling under Russian control. Those findings are uncontested at summary judgment. They are entitled to deference, and they easily satisfy the APA's requirement that DHS's action be supported by substantial evidence and demonstrate a rational connection to the underlying facts.

DISCUSSION

I. Kaspersky Lacks Standing To Challenge the BOD.

The standing analysis in this case is straightforward. Where two laws independently produce the same alleged harm, a judicial decree overturning just one does not satisfy the redressability requirement. Here, two laws — the BOD and the NDAA ban — independently prohibit federal agencies from using Kaspersky-branded software, and yet the relief requested in this action — both at the time the Complaint was filed and now at summary judgment — is addressed only to the BOD. Rescinding the BOD would leave the NDAA ban in place, which means federal agencies still would be required to stop using Kaspersky software and there would still be law on the books branding the company's products as a security risk. Due to the lingering presence of the NDAA ban, Kaspersky is left to argue that the NDAA ban and the BOD are "different," and that lifting the BOD would restore to Kaspersky its "right to sell to the government." Pls Opp 7. But that simplistic distinction, and the empty procedural right it supposedly protects, is insufficient to establish Article III standing.

A. Kaspersky's Purported Loss of Its "Right to Sell to the Government" Does Not Establish Article III Injury.

Kaspersky's brief in opposition has significantly narrowed the legal and factual issues in dispute. Kaspersky implicitly concedes that standing fails where undoing a challenged government action would not negate the alleged harm, either because a different government action produces the same harm or operates to ensure that third parties will have incentive to continue their harmful conduct. *See* Defs MSJ at 16-17; Defs PI Opp at 16-19 (collecting cases). And the company accepts the reality that lifting the BOD just months before an even broader prohibition takes effect would have no practical effect on its ability to obtain a government contract. *See* Schneider Decl., Dkt. 13-1; Defs MSJ at 18-20. Kaspersky is thus left to argue (1) that the Court should simply assume

that the NDAA ban is an unconstitutional bill of attainder because Kaspersky has challenged it in an entirely separate lawsuit; or (2) that, even though it is uncontested that the existence of the NDAA ban means that lifting the BOD would not affect Kaspersky's sales to the U.S government, the mere *ability to sell*, even if only for a matter of months, suffices to establish Article III injury. As discussed below, neither of these last-gasp attempts establishes standing.

i. The NDAA Ban Forecloses Any Effective Relief from the Alleged Injury.

Kaspersky contends standing is proper because rescinding the BOD would restore its "right" to submit bids for government contracts – even though that "right" disappears in October, when a more stringent prohibition kicks in; and even though, as the Schneider Declaration and common sense demonstrate, it is a virtual certainty that no agency would accept a bid from Kaspersky in the interim. Pls Opp 5-6. In other words, Kaspersky concedes that the most it can hope for in the way of relief is a narrow window, likely no more than several months, during which an agency *theoretically* could acquire and use Kaspersky software without breaking the law. *Id*. Whatever value Kaspersky attaches to the prospect of being legally permitted to sell software to the U.S. government during the brief period between the rescission of the BOD and the date the NDAA's ban kicks in, the incremental effect on the company is too "vague and unsubstantiated" to constitute a redressable Article III injury. *See McBryde v. Comm. to Review Circuit Council Conduct & Disability Orders of Judicial Conference of U.S.*, 264 F.3d 52, 57 (D.C. Cir. 2001).

Redressability depends on whether judicial intervention "will produce tangible, meaningful results in the real world," *Common Cause v. Dept. of Energy*, 702 F.2d 245, 254 (D.C. Cir. 1983), and must be "sufficient to take the suit out of the category of the hypothetical," *Sierra Club v. EPA*, 754 F.3d 995, 1001 (D.C. Cir. 2014). Kaspersky assumes, in conclusory fashion, that its purported attempt to recover a "legal right to sell" software to the government constitutes Article

III injury, despite the government's evidence (unrebutted by Kaspersky) that no government agency would purchase Kaspersky software while simultaneously working to remove any trace of the company's code from its networks before October 1. *See* Schneider Decl. ¶¶ 6-7. Of course, as the Supreme Court has held, a lost opportunity in the abstract, without the possibility of fulfilling the opportunity in any meaningful sense, cannot constitute a concrete and particularized Article III injury. *See Summers v. Earth Island Inst.*, 555 U.S. 488, 496 (2009)) ("[D]eprivation 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.").[1]

Kaspersky cannot avoid the redressability requirement by diminishing its Article III injury to the point of abstraction. Having conceded that no practical benefit can come from lifting the BOD, Kaspersky is left to allege the infringement of a bare procedural right, untethered from any concrete harm. But seeking relief from a procedural injury "does not — and cannot — eliminate" the requirement that a litigant identify a concrete injury in fact. *Fla. Audobon Soc'y v. Bentsen*, 94 F.3d 658, 664 (D.C. Cir. 1996). Unless the company can point to a "concrete interest" that will be affected by the deprivation, the case must be dismissed. *Summers*, 555 U.S. at 496.

The NDAA ban forecloses Kaspersky's standing no matter how the company frames its injury. If the "right to sell" has any concrete value — *i.e.*, if it encompasses not only the ability to bid for contracts, but also a presumption that the bids submitted will be considered on equal footing with those of other contractors — then the deprivation is not redressable, because no reasonable agency will consider a bid from Kaspersky if the NDAA ban is in place. On the other hand, if the "right

[1] This concept also is captured by the standing decisions involving injuries with multiple regulatory causes. *See, e.g.*, *Delta Const. Co. v. EPA*, 783 F.3d 1291, 1296 (D.C. Cir. 2015) (where two agencies issue "substantially identical" regulatory restrictions, vacating one agency's restrictions while leaving the other's in place would do nothing to redress the alleged harm).

to sell" is so nebulous that it can be restored by lifting the BOD even while the NDAA ban remains in place — *i.e.*, the temporary ability to bid for a contract Kaspersky has no reasonable possibility of being awarded — then the asserted right is too vague and insubstantial to constitute an injury-in-fact. In short, any injury allegedly caused by the BOD that is concrete enough to satisfy the injury-in-fact requirement will not be redressable, and any injury that can be redressed by lifting the BOD will necessarily fail the injury-in-fact requirement. In either case, Kaspersky lacks standing; the only question is whether it falters on injury or redressability grounds.[2]

ii. Kaspersky Cannot Cure This Deficiency by Challenging the NDAA Ban in A Separate Lawsuit.

Kaspersky's lawsuit challenging the NDAA ban does not cure the standing defect that existed when this action was filed. "[S]tanding is to be determined as of the *commencement* of suit," *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 570-72 n.5 (1992) (emphasis added), and "may not be established by a development that occurs after the commencement of the litigation," *Park v. Forest Serv. of the U.S.*, 205 F.3d 1034, 1037-38 (8th Cir. 2000). If Kaspersky's injury was not redressable when the company commenced this suit — after the NDAA ban was signed into law but before it was challenged in a separate action — then the case must be dismissed, regardless of any post-

[2] Kaspersky cites *ACORN v. United States*, 618 F.3d 125 (2d Cir. 2010) for the notion that restoring a "right" to bid for contracts satisfies Article III even if there is no realistic scenario in which such a bid would be accepted. *ACORN* says nothing of the sort. While it is true that the government unsuccessfully challenged the plaintiff's standing to sue DOD on the ground that the plaintiff had not and likely would not seek funding from DOD, the reason that challenge failed had nothing to do with the vindication of some sort of nominal legal right to receive federal funds. No argument to that effect was even raised, much less adopted by the court. Instead, just as the D.C. Circuit did in *Foretich v. United States*, 351 F.3d 1198 (D.C. Cir. 2003), the court held that the plaintiff had standing to seek relief from reputational injuries caused by a federal statute that singled the plaintiff out by name and cut off its right to receive federal funds. And it held that the plaintiff had standing to sue DOD, notwithstanding the remote possibility of it soliciting a contract from the agency, because DOD was "constrained to enforce the law" since the challenged provision happened to appear in a defense spending bill. *Id*. at 134.

filing steps the company took to cure the defect. There are no exceptions to this rule, and it applies with equal force where the post-filing development is a second lawsuit seeking relief which, had it been sought via amendment of the first suit, may have avoided the standing problem. *See Conservation Law Found. v. Pritzker*, 37 F. Supp. 3d 234, 243-44 (D.D.C. 2014).

It makes no difference, for the purposes of this analysis, that the two suits have been temporarily consolidated for briefing. Unless a court states that consolidation is "for all purposes," the two cases retain their separate identities, proceed in separate procedural postures, and result in separate judgments – a fact Kaspersky does not attempt to rebut. *U.S. ex rel. Hampton v. Columbia/HCA Healthcare Corp.*, 318 F.3d 214, 216 (D.C. Cir. 2003). Since the NDAA challenge was consolidated with this case "solely for the purpose of briefing an upcoming round of dispositive motions," Order (February 16, 2018), Dkt No. 17, the two actions have not merged, and the NDAA challenge remains, like any other post-filing development, irrelevant to Kaspersky's standing to challenge the BOD. *See Lujan*, 504 U.S. at 570-72 n.5. That conclusion is reinforced by the fact that the meritless bill of attainder lawsuit remains at the motion to dismiss stage, whereas Kaspersky asks this Court to decide the present case on the merits. While Kaspersky correctly observes that the government's redressability decisions often turn on the existence of an unchallenged law, it fails to recognize that, for the purposes of the standing analysis in this case, the NDAA ban *is* unchallenged in the present suit. The NDAA action did not exist when this suit was commenced, and Kaspersky has not amended its lawsuit to include a claim against the NDAA.

Kaspersky does not seriously contest any of these principles. Instead, it faults the government for "fail[ing] to cite to a single that holds parties must mount pre-enforcement challenges to any statutes that may in the future affect their rights in order to maintain standing." Pls' Opp 11. This argument misses the point. The government has never suggested that Kaspersky should have

brought a "pre-enforcement" challenge to the NDAA to avoid a "future [e]ffect" on its standing to challenge the BOD. The NDAA ban wiped out any prospect of effective relief in this case the moment it was signed into law, and the government's position has always been that the statute deprives Kaspersky of standing to raise a separate challenge to the BOD. *See* Defs PI Opp 15-19.

Even if the new lawsuit were relevant, the Court could not plausibly infer from the mere filing of a complaint that the NDAA ban is in jeopardy. While a court ordinarily can presume the plaintiff will prevail on the merits of its claim in assessing standing, no such presumption is afforded to claims in a separate lawsuit. *See US Ecology, Inc. v. U.S. Dep't of Interior*, 231 F.3d 20, 25-26 (D.C. Cir. 2000) ("The mere fact that appellant has brought [a separate suit about issues relevant to the redressability analysis] says nothing about the underlying merits of those claims nor the remedy to which [appellant] would be entitled should it prevail."). Without that presumption, the Court could only speculate as to whether Kaspersky's new suit supports a likelihood that the NDAA ban will be struck down, such that rescinding the BOD could actually stand a chance of redressing Kaspersky's asserted injury. And even assuming such speculation were appropriate, as the government has explained, Kaspersky's bill of attainder claim is transparently flawed, and the prospect of finding that Kaspersky is entitled to relief in that case is virtually non-existent.[3]

B. Kaspersky's Reputational Injury Is Neither Redressable Nor Traceable to the BOD.

The second component of Kaspersky's purported injury — the asserted damage to the company's reputation and attendant commercial harm — fails on both redressability and causation

[3] The redressability problems are self-evident when one considers how Kaspersky's entire argument depends on the order in which this Court decides the pending motions. Under Kaspersky's theory, if this Court decided the motion for summary judgment in the present case before the motion to dismiss in the related case, it would have to assume that the NDAA is invalid. And the Court would presumably have to make that assumption even if it would have dismissed the NDAA challenge had it first addressed defendant's motion to dismiss in that case. Standing cannot be based on such procedural gimmickry.

grounds. Even if the BOD were lifted, there still would be a law on the books that Congress passed due to the information-security risk posed by the company's products. And Kaspersky has not carried its burden of showing how invalidating one purportedly stigmatizing action by the Executive Branch only to leave a broader statute in place would provide meaningful relief. Similarly, Kaspersky cannot show that its purported reputational harm is fairly traceable to the BOD, as opposed to an "endless number of diverse factors potentially contributing" to a particular injury, "foreclose[ing] any reliable conclusion" that the injury is "fairly traceable" to the challenged action. *Winpisinger v. Watson*, 628 F.2d 133, 139 (D.C. Cir. 1980).

In response, Kaspersky lumps the government's various causation and redressability arguments together and refers the Court to the D.C. Circuit's decision in *Foretich,* which Kaspersky characterizes as a "seminal" reputational standing case that "unequivocally rejects [the government's] arguments." Pls Opp 8-9. Kaspersky contends that "there were several causes" to the reputational harm in *Foretich*, and that the plaintiff in *Foretich* overcame the "same redressability arguments" the government advances here. Pls' Opp. 8.

Kaspersky stretches the *Foretich* decision beyond its breaking point. The standing analysis in *Foretich* was clear-cut. Congress enacted a law "that effectively denounce[d] Dr. Foretich as a danger to his own daughter," 351 F.3d 1198, 1215 (D.C. Cir. 2003), and there was no serious doubt that the asserted reputational injuries "resulted directly" from that congressional action, *id*. at 1211, or that declaratory relief "would remove the imprimatur of government authority from an [a]ct that effectively denounces Dr. Foretich as a danger to his own daughter." *Id*. at 1215. And while there were other sources of reputational harm identified in *Foretich*, including publicity surrounding the custody dispute with the plaintiff's ex-wife, the court did not have to untangle the consequences of multiple, overlapping government actions in determining whether the legally relevant injury

could be fairly traced to the challenged statute. Thus, contrary to *Foretich*, where a judicial decision could remediate the "imprimatur of government authority" that caused the reputational injury, invalidating the BOD would leave the legislative imprimatur of the NDAA in place. *Id*.

Here, by contrast, the court has no way of determining whether the BOD plays a meaningful part in the causal story. *See Travis v. U.S. Dep't of Health & Human Servs*, 2005 WL 589025, at *3 (D.D.C. Mar. 10, 2005) (denying standing where it was not clear if challenged action was a "deciding factor – or even a significant factor" in causing the harm). By the time DHS issued the BOD, six intelligence chiefs had publicly expressed concerns about the company's software, multiple congressional committees were investigating the company's connections to the Kremlin, GSA had started removal of Kaspersky from its schedules, a major national retailer had announced its decision to remove Kaspersky products from its stores, and Congress was poised to enact a government-wide ban. Kaspersky's failure to account for these actions makes it impossible to identify the *legally relevant* injury – that is, the harm to the company's reputation and revenue stream resulting from the BOD, above and beyond the reputational harm resulting from other governmental actions targeting the firm. And Kaspersky has made that task even more difficult by challenging the NDAA ban in a separate action, based in part on "profound reputational injuries" the company claims to have suffered solely as a result of the statute.

Kaspersky's justiciability problems are in a league of their own. They cannot seriously be likened to those confronted by the court in *Foretich*, where the only government action linked to the alleged reputational harm was the one the plaintiff was challenging. Indeed, where two government actions produce the same stigmatizing harm, courts have found that a challenge to just one does not satisfy the redressability requirement. *See Paracha v. Obama*, 194 F. Supp. 3d 7, 10 (D.D.C. 2016) (Guantanamo detainee lacked standing to challenge federal statutes forbidding his

relocation and labeling him a terrorist where he could not show that "the alleged harm to his reputation . . . is caused by the challenged statutes, rather than by the underlying facts of his detention or the Executive Branch's designation of petitioner as an enemy combatant"); *cf. Lebron v. Rumsfeld*, 670 F.3d 540, 562 (4th Cir. 2012) ("It 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"). This is especially true where, as here, limitations on judicial review make it impossible for a court to pass judgment on the merits of the underlying findings. *See McBryde*, 264 F.3d at 57.

II. DHS Is Entitled to Summary Judgment on Kaspersky's Due Process Claim.

A. Assuming It Was Entitled To It, Kaspersky Received Adequate Pre-Deprivation Process.

The crux of Kaspersky's due process claim is its contention that DHS should have notified the company sooner, before taking action that Kaspersky describes as an "immediate debarment" of Kaspersky from government business. MSJ 1. The premise of this argument is Kaspersky's assertion that it was effectively excluded from federal business "*upon the issuance* of the BOD." Compl. ¶ 9. As a result, the company asserts, any process that came after issuance of the BOD is constitutionally deficient. Kaspersky says a "meaningful" process would have mirrored the pre-deprivation procedures used for the debarment of federal contractors. MSJ at 32.

Kaspersky continues to labor under the false impression that the BOD effected an immediate debarment. Contrary to the company's assertions, the BOD did *not* require immediate removal of its products from federal networks. Instead, it began a 90-day fact-finding process that would eventually culminate in a requirement to *begin* removal, but *only if* agencies were not "directed otherwise by DHS in light of new information." AR 635. During this 90-day period, agencies reported to DHS with information about the Kaspersky products on their systems, and Kaspersky

came forward with detailed written arguments opposing DHS's intended action. No directive to begin removing Kaspersky products took effect until the information-gathering stage was over and the Acting Secretary had an opportunity to reach a final decision based on all the evidence.

Kaspersky brushes off the BOD's "unless directed otherwise" proviso as "superfluous," reasoning that "DHS was free to change direction with or without this proviso." Pls Opp 13-14. DHS did not include the proviso merely to preserve the *power* to modify the BOD. Rather, it included the proviso, together with similar language in other BOD documents, to make clear from the outset that the Secretary's final decision hinged on the outcome of the administrative review. In addition to the "unless directed otherwise" proviso in the BOD, AR 635, the Decision to issue the BOD stated that DHS "reserves the right to modify or terminate the BOD based on new information provided during the administrative process." AR 630. DHS also published a Federal Register Notice detailing the administrative process available to Kaspersky and any other directly impacted parties, and, in a letter to Eugene Kaspersky, DHS highlighted Kaspersky's ability to address the grounds for the decision as "an important element" of the Secretary's decision on whether to modify or terminate the requirement to start removal on day 90, AR 637.

By the time the Acting Secretary determined that the BOD should be maintained without modification and agencies were required to begin removal, Kaspersky had received all the standard features of pre-deprivation process: notice of the action being considered, a thorough explanation of the unclassified reasons for considering it, and an opportunity to oppose the action before the agency reached a final decision. The BOD procedures provided — if not in form, then certainly in substance — the same basic protections afforded to federal contractors subject to debarment, *see* 48 C.F.R. § 9.406-3(d), protections which Kaspersky itself concedes are constitutionally adequate. *See* Pls Opp 18 (describing the core elements of the debarment process as (1) the reasons for the

proposed debarment, (2) notice of the opportunity to submit information in opposition, (3) notice of the procedures that will govern the agency's decision-making process, and (4) the effects of proposed and actual debarment); *cf. Liberte Capital Grp., LLC v. Capwill*, 421 F.3d 377, 384 (6th Cir. 2005) (courts "must look at the actual substance, not the name or form, of the procedure to see if the claimants' interests were adequately safeguarded").

If anything, Kaspersky would have been worse off under the debarment procedures, because a "proposed debarment" results in a contractor's immediate exclusion from federal business pending a final decision from the debarment officer, *id.* § 9.405, whereas issuing the BOD had no such preclusive effect.[4] While federal agencies were required, upon issuance of the BOD, to identify Kaspersky products on their systems and develop plans for removal, it was clear from the outset that the requirement to implement those plans was subject to the outcome of DHS's review process. Kaspersky has yet to come to terms with this distinction, and although the company acknowledges that proposed debarment effects an immediate deprivation, Pls Opp 18, it insists the BOD process is still worse, offering only the bald assertion that "the BOD debarment was effective and immediate at the time the BOD was issued in September," *id.*[5] That statement is false, belied both by the terms of the administrative process and the way it was applied to Kaspersky in practice.

[4] Indeed, the FAR procedures for suspension of a federal contractor appear to bypass pre-deprivation process altogether, affording "the contractor . . . an opportunity, *following the imposition of suspension*, to submit, in person, in writing, or through a representative, information and argument in opposition to the suspension." 48 C.F.R. § 9.407-3(b)(1) (emphasis added).

[5] Kaspersky notes that the BOD goes further than debarment by requiring removal of software already running on federal networks, in addition to discontinuing use of Kaspersky products in the future. Pls Opp 18-19. For one thing, this distinction goes to the consequences of the two administrative actions, rather than the procedural safeguards afforded to aggrieved parties. For another, it highlights one of the central reasons for DHS's conclusion that the federal debarment process would not have served the Department's operational objectives in this case. *See* AR 5-6.

Kaspersky nevertheless insists that it was entitled to notice before DHS issued the BOD because the "BOD decision was final at the time of its issuance" and because "Kaspersky suffered injury" before the Acting Secretary made a final decision in December 2017. Pls Opp 12-13. Even assuming these claims are true, however, not every governmental action that detrimentally affects a private party amounts to a constitutional deprivation, and the Fifth Amendment's due process protections are not implicated anytime an agency takes action that can be characterized as "final" or "injurious." Pls Opp at 12. Due process is required only where "government action . . . affects a citizen's legal rights." *Town of Castle Rock, Colo. v. Gonzales*, 545 U.S. 748, 750 (2005). It does not apply to "action that is directed against a third party and affects the citizen only incidentally," *id*, or to action that affects "reputation alone," apart from the alteration of legal status or the deprivation of some more tangible interest, *Paul v. Davis*, 424 U.S. 693, 701 (1976).

Under these settled principles, Kaspersky had no right to administrative process before the Acting Secretary published her determination that Kaspersky's products present a security risk. That determination, together with the Acting Secretary's direction to agencies to identify and take steps to prepare for the removal of Kaspersky products, were lawful exercises of the agency's BOD authority that had no direct effect on Kaspersky's legal rights. *See, e.g.*, *Legal Tender Cases*, 79 U.S. 457, 551 (1870) (due process refers to "a direct appropriation, and not to consequential injuries resulting from the exercise of lawful power"). Kaspersky's contention that the Acting Secretary, in issuing the BOD, made findings that damaged the company's reputation does nothing to advance its claim, because reputational injury, standing alone, is not sufficient to invoke due process protections. *See Paul*, 424 U.S. at 701; *Advanced Mgmt Tech., Inc. v. FAA*, 211 F.3d 633, 637 (D.C. Cir. 2000) (agency's harmful characterizations of company's conduct during bidding process were not sufficient, standing alone, to trigger due process protections). Initial

determinations of this kind are a common feature of informal adjudication, and courts routinely uphold them without suggesting that they should be preceded by administrative process.[6] Indeed, the federal debarment procedures, Kaspersky's own benchmark for adequate administrative process, presuppose that agencies will make an adverse initial determination before any process is afforded. 48 C.F.R. § 9.406-3(d).

Similarly, Kaspersky tries to make the case that the BOD deprived it of due process by causing federal agencies to begin removing Kaspersky software before the 90-day mark. This argument mistakes voluntary risk-management decisions by third-party agencies for legal compulsion by DHS. The agencies that removed Kaspersky software before the 90-day mark did so on their own initiative, consistent with their own statutory obligations to address security risks, and without any direction from DHS. Those independent risk-management decisions, which could have resulted from a combination of any of the executive and legislative actions described above, did not amount to a constitutional deprivation of Kaspersky's rights by DHS. The "complete debarment" Kaspersky repeatedly refers to was not enacted by the provisional order; the requirement to remove and discontinue use came only after DHS made the final decision to maintain the removal requirement without modification. Because *that* action forms the basis for Kaspersky's alleged constitutional injury, *see* Compl. ¶ 34, it is the process surrounding that action that governs Kaspersky's due process claim. *See O'Bannon v. Town Court Nursing Ctr.*, 447 U.S. 773, 789 (1980) (due process "does not apply to the indirect adverse effects of government action").[7]

---

[6] *See, e.g.*, *Gargiulo v. Dep't of Homeland Sec.*, 727 F.3d 1181, 1182 (Fed. Cir. 2013) (describing procedures for revocation of security clearances); *Seraji v. Gowadia*, No. 8:16-cv-01637, 2017 WL 2628545 at *1-2 (C.D. Cal. April 27, 2017) (describing procedures for denial of Transportation Worker Identification Credential).

[7] There is no tension between the position that third-party agencies acted on their own initiative in removing Kaspersky software before the 90-day mark and the position that the NDAA ban

In addition to its pre-deprivation arguments, Kaspersky tries at every turn to portray the administrative process as a sham. Kaspersky contends, for example, that the "30-60-90 day structure was always an implementation phase and never an administrative review period," and it insists that there was never any "genuine prospect of reversal." Pls Opp 13-14. To the extent Kaspersky is suggesting there was something unfair or prejudicial about the structure or operation of the review process, it has yet to identify what that something is. DHS made it clear from the outset that it would carefully consider opposing evidence and reserve its right to modify the BOD pending the outcome of the administrative review, and every step the agency took during that review process — providing the company with a detailed, 20-plus page internal memorandum, with 47 exhibits; explaining the unclassified rationale for issuing the BOD, AR 3-625; allowing it 52 days to submit a response, along with any mitigation proposals; and providing it with an additional 25-page memorandum explaining the final decision to maintain the BOD without modification, AR 752-776 — bore out the agency's intentions.

On the other hand, to the extent Kaspersky is suggesting that the redress process was mere window-dressing — that DHS designed redress procedures, delayed a final decision pending Kaspersky's response, and reviewed and responded to Kaspersky's opposition purely to create the appearance of fair process — the argument is foreclosed by the well-established principle that agency action is entitled to a presumption of validity. The United States is not in the business of establishing sham procedures, and federal agencies are entitled to a presumption that their actions are valid and taken in good faith. *AT&T Corp. v. FCC*, 220 F.3d 607, 616 (D.C. Cir. 2000). That

realistically foreclosed the possibility of agencies doing business with Kaspersky in the months before its effective date. In the first instance, agencies understood that they were not required to begin removal until the 90-day mark, and even then only if DHS decided not to modify the BOD. In the second instance, Congress required agencies to cease using Kaspersky products by a date certain, and the prohibition is not contingent on the outcome of a review process.

is no less true when an agency adjudicates the outcome of an administrative challenge to its own proposed action. *See Withrow v. Larkin*, 421 U.S. 35, 56-57 (1975). Indeed, agencies routinely serve such dual roles without unconstitutionally pre-judging outcomes. *Id*. Were it otherwise, scores of unquestionably lawful agency actions would be subject to constitutional challenge.

Kaspersky's remaining arguments can be dismissed in short order. The company complains that it did not receive a copy of the internal memorandum supporting the issuance of the BOD until two weeks after the BOD was issued. Pls Opp 16-17. However, it neglects to mention that DHS's rationale was outlined in a memorandum sent to Kaspersky, with the BOD, on the day the BOD was issued (September 13, 2017), AR 637-38, 628-32, 754; that the company's response time began running not from the date the BOD was issued but rather the date the administrative process was published in the Federal Register (September 19, 2017), AR 639; and that, upon request, DHS granted an extension of the company's response time, AR 746-47, allowing for a total of 52 days (more than three weeks longer than the standard response period provided for during the debarment process). In the same vein, without explanation or response to the government's arguments, Kaspersky complains that DHS introduced "new" material into the record after it submitted its response. But until Kaspersky offers authority for the suggestion that the Fifth Amendment is implicated by a supplemental report building on information provided at an earlier stage of the administrative process, or explains why the company was entitled to respond to *all* of the unclassified information the Acting Secretary was considering (rather than the 21-page memorandum it received at the beginning of the administrative process, with supporting exhibits including a technical assessment from the DHS's experts), this argument should be rejected. *See* Defs MSJ 35-36.

B. Kaspersky Was Not Entitled to Notice Prior to DHS's Provisional Action.

As the government has explained, the pre-deprivation process afforded to Kaspersky was comparable to, and in some respects greater than, what Kaspersky refers to as the "well-established" and "constitutionally adequate" debarment procedures, and any differences between the two procedures are not of constitutional dimension. But even if the court were to conclude that the BOD's review process somehow falls short of the federal debarment procedure, it would not follow that the review process violates due process. As the government has shown, when properly balanced, the government's interest in responding nimbly to imminent, potentially catastrophic cyber threats is entitled to significant weight, and the process Kaspersky received was more than sufficient to satisfy the Constitution. Kaspersky has no reasonable basis for demanding administrative review prior to the issuance of the BOD, and it has not carried its burden of establishing that additional process would reduce the risk of erroneous deprivation.

Kaspersky repeats its contention that "nothing in the administrative record . . . indicates urgency," adding that the "only significant recent development was intense political pressure following Russia's apparent interference in the 2016 presidential election . . . ." Pls' Opp 19. This argument puts Kaspersky at odds with the Director of National Intelligence (DNI), who recently described the threat from Russia as particularly "severe" and unlikely to abate." AR 65. The record shows that nation states with highly sophisticated cyber programs are targeting U.S. networks on a "daily basis," AR 106, and it was the Acting Secretary's judgment that the prospect of a foreign adversary gaining access to U.S. federal networks demanded immediate attention. Indeed, Congress made a similar judgment when it granted the Secretary broad authority to take protective measures in this area, and the absence of any requirement in the BOD authority for the procedural participation of affected entities is a testament to Congress's desire for swift, unencumbered action.

Further, while Kaspersky repeatedly contends that the debarment process would have adequately safeguarded its liberty interests, it never once responds to the government's explanation as to why debarment would not have addressed the security risks posed by Kaspersky software. As DHS has explained from the outset, "a debarment would affect only future contracts" and "would not require federal agencies to remove products previously purchased and installed." AR 6. Further, because debarment prohibits only the debarred company from contracting with the U.S. government, debarring Kaspersky would not have prohibited third parties (e.g., resellers) from selling Kaspersky products to federal agencies. *Id*.

Kaspersky's demand for additional process is therefore unwarranted in light of its limited "probable value" and the burdens it would impose on the government in the cybersecurity area. *Mathews v. Eldrige*, 424 U.S. 319. 335 (1976). The process Kaspersky received was more than enough to satisfy the constitutional standard. DHS gave Kaspersky notice of its intended action and an opportunity to introduce information in response. In the meantime, agencies were able to take certain preliminary steps that would allow them to act swiftly at day 90 if not directed otherwise. This process strikes an appropriate balance between Kaspersky's interest in receiving information about the decision and having an opportunity to respond, and the Department's interest in acting promptly and effectively in response to emerging cyber threats.

III. The United States Is Entitled to Summary Judgment on Kaspersky's APA Claim.

Kaspersky's APA claim fails at the threshold. The APA precludes judicial review where "agency action is committed to agency discretion by law," 5 U.S.C. § 701(a)(2), as FISMA does by giving the DHS Secretary unreviewable discretion to identify and eliminate threats. But even if APA review were appropriate, the decision to issue the BOD would easily withstand it: there is substantial evidence to support the Acting Secretary's finding that Kaspersky software presents a

known or reasonably suspected threat, vulnerability, or risk to federal information and information systems, and the rational connection between that finding and the removal directive is plain.

APA review is precluded under 5 U.S.C. § 701(a)(2) when a "statute is drawn so that a court would have no meaningful standard against which to judge the agency's exercise of discretion." *Heckler v. Chaney*, 470 U.S. 821, 830 (1985). In making this assessment, the D.C. Circuit considers three principal factors: (i) "the language and structure of the statute that supplies the applicable legal standards for reviewing that action," (ii) "Congress's intent to commit the matter fully to agency discretion as evidenced by . . . the statutory scheme," and (iii) "the nature of the administrative action at issue." *Watervale Marine Co. v. U.S. Dep't of Homeland Sec.*, 55 F. Supp. 3d 124, 137-38 (D.D.C. 2014). As the government explained at length in its opening brief, all three factors compel the conclusion that APA review is foreclosed.

Kaspersky provides only cursory treatment of the first factor (the second factor in Kaspersky's brief), asserting, without explanation or analysis, that "FISMA provides meaningful standards that qualify DHS' discretion in issuing BODs," and that "it is within the court's purview to interpret these qualifications based on their plain meaning or comparative legal concepts." Pls' Opp 24. But there is no legal test for what constitutes "a known or reasonably suspected information security threat, vulnerability, or risk," and no legal standard for determining whether a particular directive to "safeguard" goes too far or not far enough. *Id*. Any effort to interpret these provisions would be further complicated by the extraordinary degree of deference afforded to the Secretary not only to make judgments about cyber threats that may warrant invocation of the BOD authority, but also to use a variety of other measures to enforce compliance with cybersecurity policies. *See Watervale Marine Co.*, 55 F. Supp. 3d at 143-44; 44 U.S.C. § 3553(b) (listing the BOD as one of multiple tools available to the Secretary to address cyber threats to federal agencies).

With respect to the second factor (Kaspersky's third), Kaspersky ignores the government's arguments about the overall structure of FISMA and brushes off the FISMA-related APA decisions as inapposite to the BOD authority. The courts have unanimously concluded that the choices an agency makes in carrying out its obligations under FISMA are not susceptible to APA review. And while these decisions turned on different provisions of FISMA (or its similar predecessor statute, the Federal Information Security Management Act of 2002 (FISMA 2002)), their rationale speaks to the statute as a whole, and applies with even stronger force to the Secretary's authority to issue directives. This court has recognized, for instance, that FISMA "is a peculiarly hortatory statute directed to federal executives to protect federal information technology for the benefit of the federal government." *Welborn v. IRS*, 218 F. Supp. 3d 64, 81 (D.D.C. 2016) *appeal dismissed*, 2017 WL 2373044 (D.C. Cir. Apr. 18, 2017). It also has found Congress's deferential approach reflected generally in the statutory scheme, in which "[t]here is no private right of action" and "each agency head is delegated full discretion in determining how to achieve its goals, which removes it from APA review." *Id*; *see also In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig.* ("*OPM Litigation*"), 266 F. Supp. 3d 1, 44 (D.D.C. 2017) ("The Court holds that OPM's actions in carrying out the statute's requirements is committed to the agency's discretion, and not subject to judicial review under the APA."). And the D.C. Circuit has recognized the absence in the statute of any "role for the judicial branch," noting that it is "far from certain that courts would ever be able to review the choices an agency makes in carrying out its FISMA obligations." *Cobell v. Kempthorne*, 455 F.3d 301, 314 (D.C. Cir. 2006).

As for the third factor (Kaspersky's first), Kaspersky does not dispute that the initial determination as to whether the known facts and intelligence about a particular cybersecurity threat warrant government-wide action involves the review and analysis of sensitive and often classified

intelligence, coupled with the understanding and analysis of an ever-evolving cybersecurity environment. Nor does Kaspersky dispute that the information and analysis underlying these decisions tends to be expert-driven and highly technical. *See, e.g.*, *Huls Am., Inc. v. Browner*, 83 F.3d 445, 452 (D.C. Cir. 1996). Instead, Kaspersky reiterates its argument that the BOD is presumptively reviewable because it "effectuated a debarment." Pls Opp 24. Kaspersky's focus on the consequences of the BOD, rather than the nature of DHS's action, ignores controlling precedent and turns the reviewability analysis on its head. The question is whether there is a "meaningful standard against which to judge the agency's exercise of discretion," *Heckler*, 470 U.S. at 830, not whether the adverse effects of the challenged action resemble those of other agency actions subject to APA review. While such adverse effects may entitle a company to certain *procedural* protections, they do not expand the judicially-settled scope of the APA or subject an otherwise unreviewable action to legal challenge.

Even if the court were to conclude that the decision is reviewable, the APA claim still fails on the merits. An agency decision should be upheld unless it is (as relevant here) "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2). The Court's review under this standard is narrow and highly deferential, and the Court does not substitute its judgment for that of the agency. *See Citizens to Preserve Overton Park*, 401 U.S. at 416. Notwithstanding the deference accorded agency decisions that, like this one, directly implicate national security, Kaspersky claims that the BOD should be overturned as arbitrary and capricious because DHS relied, in part, on media reports in building the evidentiary record.

First, as the government has explained, it was entirely appropriate for DHS to rely on news reports, among other materials and evidence, to justify its decision to issue the BOD. The D.C. Circuit repeatedly has "approved the use of such materials as part of the unclassified record" in

national security cases. *Zevallos v. Obama*, 793 F.3d 106, 113 (D.C. Cir. 2015); *see, e.g.*, *People's Mojahedin Org. of Iran v. U.S. Dep't of State*, 182 F.3d 17, 19 (D.C. Cir. 1999) (noting that "nothing in [AEDPA] restricts [the Department of State] from acting on the basis of third hand accounts, press stories, material on the Internet[,] or other hearsay regarding the organization's activities"); *Holy Land Found. For Relief and Dev. v. Ashcroft*, 333 F.3d 156, 162 (D.C. Cir.) ("It is clear that the government may decide to designate an entity based on a broad range of evidence, including intelligence data and hearsay declarations"). As these decisions recognize, "[t]here are good reasons" to permit agencies to rely on these materials in national security matters, particularly where the challenged action is "based in part on classified information." *Zevallos*, 793 F.3d at 113 (explaining that various legal, diplomatic, and logistical obstacles "may limit what [an agency] or its agents can say publicly").

Kaspersky contends that relying on press reports was procedurally improper here because none of the D.C. Circuit's rationales for permitting agencies to rely on them is applicable here. Pls Opp 26-27 (listing rationales). As an initial matter, this argument reads *Zevallos* far too narrowly. In identifying some of the "good reasons" for permitting agencies to rely on press reports, the *Zevallos* court did not purport to create a hard-and-fast test or to constrain the scope of the court's previous decisions recognizing agencies' authority to rely on a broad range of evidence in support of its decisions. *See, e.g.*, *Holy Land*, 333 F.3d at 162.

In any event, the *Zevallos* court's primary rationale for permitting agencies to rely on media reports — protecting classified information — applies with equal force here. As the government has made clear from the outset, the Acting Secretary considered both classified and unclassified information in deciding whether to issue the BOD. As is the case with any agency action based in part on classified information, media reports and other public source information allowed DHS to

make the administrative record as robust as possible without compromising sensitive national security information. Kaspersky's suggestion that DHS's reliance on those reports was a "self-serving" "substitute for genuine . . . agency fact-finding" is wrong on two levels: first, as a matter of law, because reliance on media reports is a permissible means of "fact-finding," without regard to whether the agency can corroborate them, *Zevallos*, 793 F.3d at 113; and second, as a matter of fact, because it would be inappropriate to assume that reliance on media reports is "self-serving" where, as here, the agency's decision is based in part on classified information.

Further, in contending that the administrative record "consists almost entirely of unsubstantiated media reports and allegations against the Company," Pls Opp 25 Kaspersky distorts the record and ignores the crux of DHS's concerns that led to issuance of the BOD. As discussed above, the media reports that DHS cites go to the issue of ties between Kaspersky and the Russian Government. But those ties form only one part, and not a necessary part, of DHS's rationale for issuing the BOD. The Secretary's Decision Memo accompanying the issuance of the BOD cites multiple grounds underpinning the Secretary's decision. And the record is clear that the decision stands even if the ties between Kaspersky and the Russian government do not exist. AR 19 ("This Russian threat presents information security risks regardless of whether or not Kaspersky provides assistance to the FSB or another Russian government agency.").

Key aspects of the BOD's rationale do not rely on media reports.[8] In arriving at these conclusions, DHS relied on key pieces of evidence — not media reports — that Kaspersky

[8] These include: "that anti-virus products and solutions, including Kaspersky-branded products, have broad access to files and elevated privileges on the computers on which the software is installed"; "that customers who participate in the Kaspersky Security Network permit a wide range of sensitive data to be automatically transferred from user computers to Kaspersky servers"; and "that Russian law permits Russian governmental entities to request or compel assistance by Russian companies, including Kaspersky, and to intercept communications transiting Russian telecommunications and Internet Service Provider networks." AR 629.

repeatedly discounts. These include two detailed technical assessments by DHS experts. AR 25-32, 822-832. Kaspersky's main response to these reports is that they were prepared internally, Pls Opp 28, but Kaspersky fails to cite any authority for the dubious proposition that an agency cannot rely on its internal experts in reaching a determination. The record evidence also includes public statements by Kaspersky (AR 7, 9), statements of various U.S. officials (AR 16-17), reports from government agencies (AR 10), a detailed analysis of the End User License Agreements for Kaspersky products (AR 761-762), and an analysis of Russian law from publicly available sources (AR 14-15), later supplemented by a report from a leading professor in the field (AR 777-821).

Apart from DHS's reliance on press reports, the opposition brief says virtually nothing about the strength of the agency's evidence or the reasonableness of the underlying decision. Kaspersky makes it clear that it disagrees with the Acting Secretary's determination, and it alludes to certain objections it raised in its administrative response to DHS. But an agency's determination and explanation are not arbitrary or capricious simply because the plaintiff, or even the court, disagrees with its conclusion. And Kaspersky's passing reference to factual objections it raised during the administrative process is not sufficient to carry its burden on summary judgment. The Supreme Court has emphasized that "[m]atters intimately related to foreign policy and national security are rarely proper subjects for judicial intervention." *Haig v. Agee,* 453 U.S. 280, 292 (1981). This case is not the rare exception. Congress entrusted the security of the government's information systems to the Secretary, and this Court should decline Kaspersky's invitation to second-guess her determination that Kaspersky's software poses an unacceptable risk to the nation's security.

CONCLUSION

The Court should dismiss this lawsuit for lack of jurisdiction or, alternatively, deny Kaspersky's motion for summary judgment and grant the government's cross-motion.

Dated: April 16, 2018

Respectfully submitted,

CHAD A. READLER
Acting Assistant Attorney General

ERIC R. WOMACK
DIANE KELLEHER
Assistant Branch Directors
Civil Division

/s/ Samuel M. Singer
SAMUEL M SINGER (D.C. Bar 1014022)
Trial Attorney
United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave, NW
Washington, D.C. 20530
Telephone: (202) 616-8014