CISA: Hope for More Cybersecurity, Challenges in Implementation and Interpretation

By Matthew J. Gardner, Moshe B. Broder

Matthew J. Gardner

Moshe B. Broder

On December 18, 2015, after years of debate and numerous attempts, Congress enacted the Cybersecurity Information Sharing Act of 2015 (CISA, or Act). The Act was the product of more than a decade of effort and years of stalled legislative efforts in both the Senate and the House of Representatives. It was passed when it was inserted into the omnibus Consolidated Appropriations Act for 2016 as a title within "Division N" (the Cybersecurity Act of 2015) and with the passage of that bill, which funded the federal government for the remainder of the fiscal year, CISA became law.

The Act's passage is only the beginning of a new chapter. The government and the private sector will have to apply and interpret this important law, and in the coming months, several federal agencies will implement it through regulations and other actions. Although CISA may affect virtually every company and sector, government contractors in particular will face the challenge of grappling with the law and its implications, for a number of reasons. First, government contractors have been the target of cyber attacks and hacking attempts, and in order to strengthen their cybersecurity posture, they will want to take advantage of the information sharing and receiving provisions, as well as the network monitoring and defensive measure authorizations. Second, contractors may seek to voluntarily provide information to the federal government, and the federal government, for its part, will ask for cybersecurity information from contractors—though there are limitations on its ability to coerce a contractor into providing such information. Third, cybersecurity contractors will be retained to perform many of the technical tasks necessitated by CISA, including monitoring, automated sharing, removing private information, and operating defensive measures. Because contractors will need to comply with the Act to obtain the benefit of the statutorily provided protection from liability, it is imperative that these contractors, like all others, pay careful attention to CISA's requirements and the forthcoming regulatory guidelines.

Matthew J. Gardner is of counsel and Moshe B. Broder is an associate at Wiley Rein LLP. Mr. Gardner is a member of the firm's White Collar Defense and Cybersecurity practices, and Mr. Broder is a member of the firm's Government Contracts practice.[1]

Intro to CISA: Cybersecurity Information Sharing Gains Momentum

The public discussion regarding cybersecurity information-sharing legislation dates back more than fifteen years, yet the issues raised by the private sector have largely remained the same. The Clinton administration's January 2000 National Plan for Information Systems Protection was one of the first major initiatives. In this early effort, industry expressed concern that shared information would be disclosed by a Freedom of Information Act (FOIA) request.[2] Notwithstanding this concern, the National Plan promoted sector-specific Information Sharing and Analysis Centers (ISACs) in order to share and disseminate cybersecurity threat and vulnerability information within the private sector and between the private and public sectors.[3] Several years later and following the attacks on September 11, 2001, the Bush administration established the Department of Homeland Security (DHS) and published the February 2003 National Strategy to Secure Cyberspace.[4] The Strategy advocated for voluntary public-private information sharing and identified "real or perceived legal obstacles" that made some entities "hesitant to share information about cyber incidents with the government or with each other."[5] Cybersecurity information-sharing legislation advanced incrementally between 2003 and 2009,[6] at which time President Obama returned the focus to the issue with the May 2009 Cyberspace Policy Review[7] and The Comprehensive National Cybersecurity Initiative.[8] In those efforts, the Obama administration identified public-private cybersecurity information sharing as essential aspects of any cybersecurity legislation, but the private sector continued to voice concerns relating to antitrust law, disclosure of sensitive or proprietary data, release of information by FOIA requests and/or suits, and reputational harm.[9] President Obama also issued Executive Order 13636, which sought to encourage private sector participation in a voluntary cybersecurity information-sharing program.[10]

Around 2009, Congress began to debate cybersecurity information-sharing legislation and laid out the broad outline of what would ultimately develop into CISA.[11] From 2009 through 2015, lawmakers repeatedly

CISA

continued from page 1

attempted to enact this type of legislation. On each occasion, however, the efforts were met with significant opposition from lawmakers,[12] privacy and technology groups,[13] and even a veto threat from President Obama in response to a previous version's failure to adequately protect privacy or appropriately restrict government uses.[14] Years of national debate caused the proposed laws to evolve, and in 2015, the Senate and the House of Representatives advanced three versions of the bill,[15] before a final combined version was inserted in late-December 2015 into the Cybersecurity Act of 2015.

Several explanations may be offered for the successful passage of CISA following so many failed attempts.[16] Some assert foul play over the extremely short time during which CISA was up for debate, believing that its passage was due, in large part, to its insertion into the last-minute "must-pass" appropriations act.[17] From a policy perspective, while government officials have warned of a "cyber" or "digital" "Pearl Harbor" for nearly 15 years,[18] the rhetoric has increased in both volume and tone,[19] with officials cautioning about cyber attacks being responsible for the largest transfer of wealth in history[20] combined with a serious threat to the homeland.[21] Perhaps more importantly, the news cycle grew increasingly saturated with reports that resonated with the typical citizen: high profile data breaches and cyber intrusions, causing the theft of consumer credit card and social security numbers.

With that background, the Cybersecurity Act contains four titles:

- Cybersecurity Information Sharing (the focus of this article)
- National Cybersecurity Advancement (relating to other federal government efforts to improve federal network security)
- Federal Cybersecurity Workforce Assessment (requiring the assessment of federal government human resource capabilities and needs in cybersecurity)
- Other Cyber Matters (requiring a study on mobile device security, forming a strategy for international cyberspace policy, etc.)

Very broadly speaking, the first title, Cybersecurity Information Sharing, provides authorization for private entities to do the following: monitor their (or their customers') information systems for "cybersecurity purposes," operate defensive measures for cybersecurity purposes on their (or their customers') networks to protect their "rights or property," and voluntarily share and receive certain information. By doing so in accordance with the Act, these private entities may receive protection from liability for monitoring or sharing or receiving information. The federal government may receive and share cybersecurity information and use it for limited purposes.

Definitional Ambiguities

"Cybersecurity Purpose." Much hinges on the scope and interpretation of this definition. For "cybersecurity purposes," a private entity is authorized to monitor certain networks;[22] operate "defensive measures";[23] and share with, or receive from, any other nonfederal entity or the federal government a cyber threat indicator or defensive measure.[24] By so doing, a private entity may receive protection from FOIA suits and disclosures,[25] antitrust laws,[26] most state prosecutions,[27] state regulatory enforcement actions,[28] and waiver of privilege, including trade secret protection.[29] Similarly, the federal government may disclose, retain, or use cyber-threat indicators or defensive measures for only five purposes: "cybersecurity purpose" is the first on the list.[30]

CISA defines "cybersecurity purpose" as "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability."[31] This definition needs to be broken down into its elements. "Information" and "information system" are familiar terms with relatively little ambiguity.[32] Information that may be protected must be "stored on," "processed by," or "transiting" an information system. This seemingly broad phrase does not have any readily apparent legislative parallels, and its use can be traced back to a 2012 precursor bill to CISA.[33] Critically, information and information systems may be protected from a "cybersecurity threat" or "security vulnerability."[34]

Some legislators considered the meaning of "cybersecurity purpose" to be "one of the *main limitations* on the ability of private and governmental entities to use cyber threat indicators and defensive measures."[35] Many previously applicable legal limitations on different kinds of information sharing were more restrictive; for example, laws permitting communication service providers to disclose or access information in response to government compulsion, with consent, or to ensure the provision of their service or to protect the rights or property of the provider.[36] These prior restrictions were perceived as an impediment to private entities voluntarily disclosing certain cybersecurity information with each other or with the government.[37] As a result, regardless of the precise definition of "cybersecurity purpose," the standard is seemingly broader than that which previously governed private entities seeking to voluntarily share information.

The definition of "cybersecurity threat" is where it gets less clear.

"Cybersecurity Threat." The Act defines a "cybersecurity threat" as "an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system."[38]

The Senate Report accompanying the Senate's version

of CISA, submitted by Senator Richard Burr, clearly appreciated the potential for this definition to be construed broadly. It specifically stated that the Senate Select Committee on Intelligence (SSCI) intended the definition of "cybersecurity threat" to "include activities that may have unauthorized and negative results, but to exclude authorized activities, such as extensive use of bandwidth that may incidentally cause adverse effects."[39] Yet this example requires further analysis—the difference between unauthorized or negative results and extensive use of bandwidth with only *incidental* adverse effects may be a matter of subjective intent or extent of the activity, neither of which is immediately known to an entity perceiving itself to be under attack.

Two examples illustrate this problem: legitimate heavy bandwidth users and unknowing attackers (e.g., computers controlled by a botnet[40]) can both use heavy bandwidth to overwhelm a particular information system. First, a distributed denial-of-service (DDoS)[41] attack can cause unauthorized and negative results, and thus clearly qualifies as a "cybersecurity threat." But what about a large media company whose employees are all constantly engaged in streaming high-definition video? While the company may have no intent to cause adverse effects, to the company's Internet service provider (ISP) or other Internet information provider,[42] the *aggregate* intensity of the company's network activity could appear malicious.[43] And the fact that unusual network activity appears to have the potential to harm the network may be itself sufficient to be considered a "cybersecurity threat." This is because the Act does not require actual damage to an information system in order for an action to be considered a "cybersecurity threat." Rather, a threat is defined as an action that "*may* result in an unauthorized *effort*." In other words, not only is actual damage not required, but an actual effort is also not required—all that is required is an action that *may result* in an unauthorized effort. Indeed, Senator Ron Wyden criticized this seemingly broad language and advocated for a more restrictive standard, such as an action that would be "reasonably likely" to harm an information system.[44] As Senator Wyden observed, some may argue that this definition could include otherwise innocuous activity; persistent and excessive streaming could potentially qualify as an action that may result in an unauthorized effort to impact the availability of an information system.

Second, some entities or individuals will unwittingly become a "cybersecurity threat" when their systems become compromised by botnets and flood other information systems with excessive commands. The target of such an attack will observe the malicious activity transiting the network and may conclude that it is facing a "cybersecurity threat" that "may result in an unauthorized effort" to compromise the availability and integrity of its information systems—notwithstanding that the attack appears to have originated from an entity or individual whose system owners have no ill intent. The absence of ill intent may not be ascertainable by the target, and it would monitor the network traffic in accordance with CISA's provisions. In so doing, it might acquire a large amount of legitimate network traffic or information about the legitimate actors coming from the infected systems. And if it operates defensive measures against all network traffic coming from an infected system, the owner of the host system may experience serious problems on its otherwise legitimate network traffic. The net result is that the victimized computer and network owners may be subject to monitoring or defensive measures.

Further, a "cybersecurity threat" excludes any action protected by the First Amendment. But the precise contours of that exception are difficult to predict because constitutional analysis is fact-specific; moreover, there is limited precedent analyzing whether computer code can receive First Amendment protection. Conceptually, it can be protected, though the scope of that protection depends on factors including whether code is considered content or noncontent speech.[45] At the extremes, the First Amendment's free speech protections seemingly do not extend to cover unlawful hacking or transmission of malicious computer code, any more than they extend to a robber telling a bank teller, "This is a stickup."[46] But for activity lying at the margins, it may be difficult to distinguish between constitutionally protected activity and an unprotected cybersecurity threat. As the federal government has conceded, "malicious software may be theoretically capable of being used for lawful purposes"[47] and, once again, the difference between malicious and benign code can be the intent of the programmer or the circumstances under which the code is transmitted.

The use of a scraping tool is illustrative of the problem. A scraping tool is a computer program that accesses a website's publically available HTML source code and compiles it into structured data to enable more in-depth analysis. A malicious actor might use it to conduct reconnaissance against a hacking target, but a nonprofit could also use it to automatically compile and archive the statements of elected officials. Courts have not provided clear guidance as to whether its use is protected by the First Amendment,[48] but some may argue that it constitutes a "cybersecurity threat," as it may result in an unauthorized effort to harm the confidentiality or availability of an information system. To the extent a scraping tool is protected First Amendment speech, a network owner could *not* classify it as a "cybersecurity threat" under CISA. But because the constitutionality of the tool depends on facts and context not known to the network owner, it will be difficult to know *ex ante* whether the activity is excluded from the definition. And since the standard permits an arguable degree of subjectivity and discretion—a threat is an action that "*may* result in an unauthorized *effort*"—this lack of knowledge may lead some to err on the side of classifying such activity as a threat and conducting actions appropriate to such a threat under CISA.

Notwithstanding the ambiguities contained within this critical definition, the Act does provide clear guidance

on one other important point. The Act specifically excludes "any action that solely involves a violation of a consumer term of service or a consumer licensing agreement."[49] Removing these types of violations from the definition of "cybersecurity threat" is an apparent nod to the debate surrounding the Computer Fraud and Abuse Act (CFAA). That law has caused a "sharp division" among the circuit courts regarding the appropriate scope and interpretation of the "exceeds authorized access" provision,[50] which provides criminal penalties for an individual who "intentionally accesses a computer . . . exceeds authorized access, and thereby obtains . . . information from any protected computer."[51] Some circuits argue that this provision, if construed broadly, would criminalize a wide range of ordinary consumer and employee conduct, such as violations of consumer terms of service or licensing agreements (including nonnegotiated "click-through" agreements), and thus invite arbitrary prosecutions. For example, an individual who signs up for a social networking website with false personally identifiable information (e.g., a fake name) does so in violation of most terms of service, which require that a user provide valid identifying information. But is that sufficient to subject an individual to criminal liability under the CFAA? The Ninth Circuit thinks not because doing so "can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved."[52] Other courts, in similar circumstances, have interpreted the statute more broadly and upheld convictions for violations of consumer or employee terms of service.[53] Accordingly, by defining "cybersecurity threat" as excluding the violation of a consumer term of service, the Act does not provide carte blanche to private entities to disclose or monitor information merely because of the relatively common occurrence of a consumer violating terms of service.

What Is a Private Entity Authorized to Do?

CISA authorizes a private entity, for cybersecurity purposes, to monitor information systems; operate defensive measures; and share and receive cyber-threat indicators or defensive measures with other private entities, state and local governments, and the federal government.[54]

Private Entity Monitoring. CISA authorizes a private entity, "notwithstanding any other provision of law," to monitor its own information systems, the information systems of another nonfederal or federal entity (provided that it receives the appropriate written authorizations), and the information that is stored on, processed by, or transiting an information system that is monitored by the private entity.[55] CISA provides a definition for "monitor"—it means to "acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system."[56] This definition seemingly includes two categories of activity: identify/scan and acquire/possess.

This is one of the most important provisions in the Act because it authorizes private entities to monitor their information systems for "cybersecurity purposes" and, in so doing, acquire the information it identifies. As noted, because the standard for what activity constitutes a "cybersecurity threat" is potentially broad (an action that *may* result in an unauthorized *effort* . . .) and because an entity that believes it is under attack may not know whether it is, in fact, under attack at the time it is observing the irregular activity, some entities may scan and acquire a large amount of legitimate information.

A key privacy question stems from the definition of "monitoring." If CISA authorizes the monitoring of information systems for cybersecurity purposes, and the definition of "monitoring" includes acquisition and possession of information that is processed by or transiting an information system, may a private entity use that acquired information for other non-"cybersecurity purpose"-related functions? This is especially important given that the private entity may not have otherwise had the legal authority to "acquire" the information but for CISA's authorization to conduct the monitoring. CISA specifies that while nothing in the Act shall be construed to affirmatively authorize the use of information obtained through such monitoring other than as provided by the Act, it also states that nothing shall be construed to limit otherwise lawful activity.[57] As a result, the law may be construed to allow acquisition of a larger scope of information, while not restricting other nonprohibited use of that information.

Private Entity Defensive Measures. CISA authorizes a private entity to operate defensive measures, "notwithstanding any other provision of law."[58] Such defensive measures may be applied "to . . . an information system of such private entity in order to protect the rights or property of the private entity" or the information systems of another nonfederal or federal entity, upon written consent of that entity.[59] What exactly is a "defensive measure"? A July 2014 precursor version of CISA provided for the operation of "countermeasures" instead of "defensive measures."[60] *Defensive*, as opposed to *counter*, implies a more limited scope, yet the statutory definitions drafted by the legislators were nearly identical.[61] Is the name change merely cosmetic, or reflective of some more substantive difference?[62]

The Act defines a defensive measure as "an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability."[63] The key part of the definition, and the distinguishing factor between "countermeasures" and "defensive measures," lies in the exclusions to the definition. "The term 'defensive measure' does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by" the private entity or another entity that authorized the operation of that defensive measure.[64] The proposed definition for countermeasures contained no such limitation, implying a far broader scope to

countermeasures as compared to defensive measures.[65]

The Senate Committee Report stated that the definition of defensive measures "does not authorize the use of measures that are generally to be considered 'offensive' in nature, such as unauthorized access of or executing computer code on another entity's information systems or taking an action that would substantially harm another private entity's information systems."[66] Nonetheless, the Report acknowledged "that defensive measures on one entity's network could have effects on other networks"[67] and stated that it intended to exclude defensive measures that cause substantial harm to other information systems, regardless of whether that harm was "intended or foreseen by the implementing entity."[68]

This definition contains some critical ambiguities. First, what does it mean for a defensive measure to provide "unauthorized access" to an information system? In the CFAA context, legal scholars have derived three categories of theories for determining when an individual accesses a computer without authorization: agency-based, code-based, and contract-based.[69] In this context as well, the choice of theories for defining "unauthorized access" has broad implications. Second, what does it mean for a defensive measure to "*substantially* harm" information or an information system? Is there some lesser harm that would be permissible, and who would determine what qualifies as a less-than-substantial harm? Would the key distinction be whether the defensive measure executes some code on another system, or could a more "passive" defense, such as blocking access from that system, also constitute "substantial harm"? Third, an entity is prohibited from operating certain types of defensive measures on an information system not "owned" by it, but in the era of increasingly popular virtual private servers,[70] what does it mean to "own" an information system?

One last point on defensive measures bears mentioning. As previously discussed, a private entity may operate defensive measures only to protect "the rights or property" of the private entity or of the consenting nonfederal or federal entity.[71] In practice, to what extent does the "rights or property" clause limit the operation of defensive measures? It could be argued that *any* "cybersecurity threat" or "security vulnerability" poses a threat to the rights or property of an entity's information system. Under the parallel provision in the Wiretap Act (the so-called 'service provider' exception), courts have permitted network providers to monitor their networks to prevent fraud[72] or otherwise protect their "monetary resources,"[73] but not to gain a commercial advantage.[74] Assuming this precedent would guide the interpretation of CISA, at a minimum, a private entity may operate defensive measures to prevent fraud or protect its resources, but not necessarily to gain insight into the operations of its competitors.

Private Entity Information Sharing. CISA authorizes non-federal entities to share and receive information with other nonfederal and federal entities.[75] Such sharing must be done for a "cybersecurity purpose" and in a manner that protects classified information.[76] A nonfederal entity is also required to implement a security control system to guard against unauthorized access to or acquisition of information it receives from another entity.[77] Further, prior to sharing a cyber threat indicator, a nonfederal entity must manually or automatically review the information and if it contains any information "not directly related to a cybersecurity threat that the nonfederal entity *knows at the time of sharing* to be personal information of a specific individual or information that identifies a specific individual," it must remove such information.[78] Once it has shared or received such information, a nonfederal entity may use it to "monitor or operate a defensive measure" applied to an information system, or it may be "otherwise used" subject to lawful restrictions placed by the sharing entity or other generally applicable provisions of law.[79]

There are a number of ambiguities relating to the "use" of shared or received information. First, prior to sharing, a nonfederal entity must remove private information that is "not *directly* related to a cybersecurity threat"[80]—but no guidance is provided on the required nexus between the threat and potentially private information. Perhaps in recognition of this ambiguity, CISA requires, as part of the federal government's Biennial Report on Compliance, an assessment of the policies, guidelines, and practices relating to this specific provision.[81] More significantly, CISA requires the publication of interim and final policies, procedures, and guidelines that will provide guidance on several critical portions of the Act.[82]

Second, a nonfederal entity's obligation to remove this personal information only applies to information *that is known, at the time of sharing*, to be personal information or information that identifies a specific individual.[83] While providing the benefit of a hard-line rule and arguably minimizing lag time in information sharing that could occur if an entity were required to manually review and scrub all information before sharing, as opposed to a subjective standard or a duty to investigate, this knowledge requirement nonetheless begs further guidance: who in the entity must "know"; how would knowledge be determined in light of the option for technical capabilities for automated removal of personal information;[84] how much effort, if any, is a company required to undertake in order to make this determination; and what documentation, if any, could an entity provide to show that it had no knowledge at the time of sharing? Some have alleged that the knowledge requirement would effectively incentivize private entities to share information and turn a blind eye to whether it may contain personal information requiring deletion.[85] Like other ambiguous provisions in CISA, private entities should seek to engage with the federal government and provide input into the mandated final guidelines.[86]

Issues Relating to the Federal Government's Role in CISA

Government Roles and Receipt of Information. CISA designates the Department of Homeland Security as the primary agency to receive cybersecurity

information from nonfederal entities, but at the same time, the law also permits the president to designate an additional federal entity (other than the Department of Defense (DoD) or the National Security Agency (NSA)) to develop and implement a parallel set of capabilities and processes to receive and share information.[87] As the primary agency, DHS must ensure that all of the "appropriate federal entities"[88] receive "in an automated manner such cyber threat indicators and defensive measures shared through the real-time process within the [DHS]."[89] This seemingly innocuous provision is significant because an alternative legislative effort advanced in the House of Representatives—the Protecting Cyber Networks Act of 2015—specifically prohibited DHS from sharing this information, either automatically or manually, with either the NSA or any other DoD component,[90] while DoD is an "appropriate federal entity" under CISA.[91]

As a practical matter, Title II of the Cybersecurity Act of 2015 directs a DHS component, the National Cybersecurity and Communications Integration Center (NCCIC), to develop capabilities in support of the information-sharing program envisioned by CISA.[92] Although NCCIC activities were previously functional, Title II codifies these roles and seeks to further develop them—though significant details remain to be addressed. Additionally, the Act directs that these information-sharing procedures incorporate, "to the greatest extent practicable, existing processes and existing roles and responsibilities of federal entities . . . including sector specific [ISACs]."[93] To the extent that these currently existing processes within the ISACs become or remain part of the DHS process, private entities that shared information with the ISACs prior to the Act's passage may now be able to share information and take advantage of the Act's protection from liability provisions.[94]

Further, although DHS is designated as the primary agency to receive and share cybersecurity information, CISA does not prohibit a private entity from otherwise sharing information with other federal entities, including in situations where an entity reports known or suspected criminal activity, responds to compelled participation in a federal investigation, or provides information as part of a statutory or authorized contractual requirement.[95] A private entity sharing cybersecurity information with another federal agency and outside the DHS procedure in these situations *may be* ineligible for liability protection under CISA,[96] though the language of the bill could be read to suggest otherwise.

With regard to the receipt of information, although the success of CISA hinges on private entities *voluntarily* sharing information, the Act acknowledges the potential for government coercion of private entities to provide information in accordance with the Act.[97] CISA thus provides that nothing in the title is to be construed "to require a non-federal entity to provide information" to another entity; to condition the receipt of information on an entity's willingness to share; and, significantly for government contractors, to "condition the award of any federal grant, contract, or purchase on the provision of a cyber threat indicator" to another entity.[98] Although this important section removes many of the larger "sticks" from the federal government's arsenal, it remains to be seen whether it can or will resort to lesser forms of coercion, or offer "carrots" for participating in "voluntary" information sharing. At the very least, nonparticipation in any voluntary activity authorized by CISA may not be construed to subject an entity to liability.[99] And the voluntary regime in CISA does not displace any otherwise lawful disclosures, including mandated breach disclosures by cleared defense contractors,[100] regulated entities sharing information with regulators,[101] reporting of known or suspected criminal activity[102] such as child pornography traversing a network,[103] or other voluntary participation in a federal investigation.

Government Use of Information. One significant issue relates to what the federal government can—and, more importantly, cannot—do with the information it receives. CISA provides that cyber-threat indicators and defensive measures may be "disclosed to, retained by, and used by" any federal agency or employee of the federal government, in a manner consistent with otherwise applicable provisions of federal law, for the following purposes:

- A "cybersecurity purpose";
- The purpose of identifying a cybersecurity threat or the source thereof, or a security vulnerability;
- The purpose of responding to, preventing, disrupting, or prosecuting a specific threat of death, serious bodily harm, or serious economic harm, including a terrorist act or a use of a weapon of mass destruction;
- The purpose of responding to, investigating, prosecuting, or otherwise preventing a serious threat to a minor, including sexual exploitation;
- The purpose of preventing, disrupting, or prosecuting an offense "arising out of a threat" listed in:
  - 18 U.S.C §§ 1028–1030 (relating to identity fraud, access device fraud, and computer fraud and abuse);
  - 18 U.S.C. §§ 791–799 (relating to espionage, censorship, and unauthorized communication and use of classified information); and
  - 18 U.S.C. §§ 1831–1839 (relating to protection of trade secrets).[104]

Significantly, the Act states that the federal government may *not* disclose, retain, or use cyber-threat indicators and defensive measures provided to it pursuant to CISA for any other purpose.[105] This is significant for government contractors who may be concerned that sharing information with the government would later adversely affect their ability to be awarded contracts; the law seems to state that the list of purposes is exhaustive.[106]

The scope of permissible government uses of information shared was a significant point of contention for

privacy advocates. From a legislative history perspective, it is clear that Congress had the option to authorize the federal government to use the information for a much wider range of purposes. The Cybersecurity Information Sharing Act of 2012, for example, permitted a cybersecurity exchange to disclose cybersecurity threat indicators to a law enforcement entity if such information "*appears* to pertain to a crime which has been, is being, *or is about to be committed*."[107] The list of uses that ultimately became part of CISA is considerably narrower; it mostly deals with preventing and prosecuting serious acts of violence (especially against children) and terrorism.

At the same time, an examination of some of the statutes included in the list of permitted uses reveals some theoretically broad applications. As noted, there remains the potential to interpret broadly "cybersecurity purpose," depending in part on the definition of a "cybersecurity threat." Further, under CISA, any federal government agency may use cybersecurity threat information to prevent, disrupt, investigate, or prosecute an offense arising out of the CFAA—a statute that, as discussed, has generated controversy through some interpretations of the law.[108] Significantly, when submitting to Congress CISA's mandated Biennial Report on Compliance, the federal government is only required to report the *prosecutions* that resulted from this information sharing; the report does not necessarily require the federal government to report on its attempts to prevent, investigate, or disrupt violations arising out of the information shared with it.[109]

Additionally, a federal government agency may investigate, disrupt, or prosecute[110] an offense arising out of the improper disclosure or use of classified information.[111] This is especially significant given that both a private entity sharing or receiving cybersecurity information must do so in a manner consistent with the protection of classified information[112] and, at the same time, CISA implicitly questions whether cyber-threat indicators and defensive measures will be properly classified, at least during the early stages of CISA's implementation.[113]

Protection from Liability

Private entities may receive protection from liability for monitoring information systems in accordance with CISA's requirements, and for sharing or receiving a cyber-threat indicator or defensive measure in accordance with CISA's requirements (e.g., through either the process established by DHS or one of the exceptions in the Act).[114] CISA, however, seemingly does not provide liability protection for private entities that *operate* defensive measures in accordance with CISA's requirements.[115] The Act solely provides that "no cause of action shall lie . . . for the *sharing or receipt of a* . . . defensive measure,"[116] but does not include the operation of such measures. Defensive measures are thus only authorized by the Act "notwithstanding any other provision of law."[117] Private entities seeking to operate defensive measures pursuant to CISA should be especially cautious and consult with counsel as appropriate.

More broadly, liability protection for monitoring, sharing, or receiving information is contingent on an entity acting *in accordance with the Act's requirements*.[118] SSCI's Senate Report accompanying a precursor to CISA specifically stated that it intended that entities sharing information in a manner consistent with the Act's requirements should "not be subject to burdensome litigation."[119] But the Report also acknowledged that "activities conducted in contravention of this Act's provisions are not entitled to such liability protection [though] the Act does not create any cause of action for such non-compliance."[120] Therefore, it is especially critical that contractors and other private entities pay close attention to the statutory obligations, interim and final guidelines set to be published in winter and spring of 2016, and DHS's processes and procedures.[121]

Because of the protracted legislative attempts to enact cybersecurity information-sharing legislation, and because private-sector liability protection has been a key issue since the earliest legislative attempts, a review of the previously proposed legislation offers some critical insights into what is *not* included in this subsection. First, nearly all of the previously proposed legislation included a "good faith" standard, which would have provided protection from liability for entities that monitored, shared, or received information in good faith in accordance with CISA's requirements.[122] This may have broadened the scope of protection from liability and was an understandable attempt to counterbalance the difficulties in interpreting and applying some of the previously discussed provisions. It is uncertain whether entities engaging in these protected activities and seeking to benefit from the Act's liability protection will be able to avail themselves of a "good faith" argument in a suit challenging compliance with CISA.

Second, all of the previously proposed legislation provided that an entity engaged in willful misconduct or gross negligence would be ineligible for liability protection.[123] As the first version to omit the express retention of liability for willful misconduct, the Act seemingly suggests that, notwithstanding other provisions of law, such a theory may not provide the basis for liability—or at least the failure to receive protection from liability.

Conclusion

The passage of CISA offers contractors and other private entities the opportunity to reexamine their information and network security procedures and engage in information sharing and defensive measures to better protect information systems from external threats. But with these opportunities come significant challenges in interpreting and applying key provisions of CISA. To best position themselves to take full advantage of all that CISA offers, and ensure protection from liability, contractors and other private entities should be well advised to remain engaged in the federal government's drafting of the interim and final guidelines and to ensure that internal policies and procedures comply with CISA's requirements. PL

Endnotes

1. The authors gratefully acknowledge the feedback from Leah Schloss, senior associate at WilmerHale.

2. White House, Defending America's Cyberspace: National Plan for Information Systems Protection Version 1.0, at xxiv–xxv (2000), *available at* http://tinyurl.com/j3weqqt.

3. *Id.* at 52.

4. White House, The National Strategy to Secure Cyberspace (2003) [hereinafter National Strategy], *available at* http://tinyurl.com/hzplmb3. The Homeland Security Act of 2002, which established the Department of Homeland Security (DHS), required DHS to establish procedures on information sharing that would "limit the redissemination of such information to ensure that it is not used for an unauthorized purpose . . . [and] ensure the security and confidentiality of such information." 6 U.S.C. § 141.

5. *See* National Strategy, *supra* note 4, at 24.

6. For example, the Cyber Security Enhancement Act of 2002 amended the Electronic Communications Privacy Act (ECPA) by providing an "emergency disclosure exception" for electronic communication service providers or remote computing service providers who believe, in good faith, "that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency." *See* Homeland Security Act of 2002, Pub. L. No. 107-296, § 225(d)(1), 116 Stat. 2135, 2156 (codified at 18 U.S.C. § 2702(b)(8)).

7. White House, Cyberspace Policy Review (2009), *available at* http://tinyurl.com/gu3e8ug.

8. White House, The Comprehensive National Cybersecurity Initiative (2009), http://tinyurl.com/owaodey.

9. *See* Cyberspace Policy Review, *supra* note 7, at 18–19.

10. *See* Exec. Order No. 13,636, 3 C.F.R. 217 (2014).

11. The Cybersecurity Act of 2010, which was first introduced in the Senate in April 2009, envisioned a "public-private clearinghouse" that would receive and share cybersecurity threat and vulnerability information. Cybersecurity Act of 2010, S. 773, 111th Cong. § 403. The proposed law left much up to the president and his designated agency—it required that the designated agency promulgate rules and procedures in several important areas. *See id.* § 403(c).

12. Senator Ron Wyden voted against the omnibus appropriations bill because it included CISA, which in his view "harms security & liberty." Ron Wyden (@RonWyden), Twitter (Dec. 18, 2015, 9:04 AM), http://tinyurl.com/j8a32cv. He described CISA as "a surveillance bill by another name" and argued that it will "do little, if anything, to protect America against sophisticated hacks." #STOPCISA, Ron Wyden Senator for Or., http://tinyurl.com/hh3zvvx (last visited Feb. 19, 2016).

13. Letter from Advocacy Groups & Security Experts to Senate Select Committee on Intelligence (Mar. 2, 2015), http://tinyurl.com/zkdjzp4.

14. President Obama threatened to veto one version of the Cyber Intelligence Sharing and Protection Act (CISPA) for failing to sufficiently protect privacy interests. *See, e.g.*, Ellen Nakashima, *Obama Threatens to Veto CISPA Cybersecurity Bill, Citing Privacy Concerns*, Wash. Post, Apr. 25, 2012, http://tinyurl.com/za759y3.

15. Protecting Cyber Networks Act, H.R. 1560, 114th Cong. (2015); National Cybersecurity Protection Advancement Act of 2015, H.R. 1731, 114th Cong.; Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong..

16. Not all legislators consider its passage to be a success. Representative Justin Amash proposed legislation to repeal CISA. *See* Kevin Collier, *Congressman Plans Bill to Repeal CISA-Like Legislation Included in Omnibus*, Daily Dot, Dec. 30, 2015, http://tinyurl.com/hap2zkp.

17. Andy Greenberg, *Congress Slips CISA into a Budget Bill That's Sure to Pass*, Wired (Dec. 16, 2015), http://tinyurl.com/j4l9394.

18. In November 2001, Richard Clarke, then counterterrorism advisor to President George W. Bush, warned of a "digital Pearl Harbor." *See* Alison Mitchell, *To Forestall a "Digital Pearl Harbor," U.S. Looks to System Separate from Internet*, N.Y. Times, Nov. 17, 2001, http://tinyurl.com/zd55lwn. That theme has since been repeated and modified by many other officials, including then defense secretary Leon Panetta in 2012, *see* Elisabeth Bumiller & Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, N.Y. Times, Oct. 11, 2012, http://tinyurl.com/9te493h, and director of national intelligence James Clapper, who somewhat downplayed the scope of the risk, *see* Tony Capaccio, *Cyber-Armageddon Less Likely Than Predicted, Clapper Says*, Bloomberg Bus. (Feb. 25, 2015), http://tinyurl.com/zun32fq.

19. In 2011, in response to a potential threat to the U.S. electric grid, one unnamed official was reported to have said, "If you shut down our power grid, maybe we will put a missile down one of your smokestacks." *See* Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War*, Wall St. J., May 31, 2011, http://tinyurl.com/pznb3u3. In October 2014, Federal Bureau of Investigation director James Comey gave his first major television interview to CBS's *60 Minutes*, and stated that "there are two kinds of big companies in the United States. There are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese." Scott Pelley, *FBI Director on Threat of ISIS, Cybercrime*, CBS News (Oct. 5, 2014), http://tinyurl.com/l5b7vhu (transcript of *60 Minutes* segment "The Director").

20. In July 2012, then director of the National Security Agency, Keith Alexander, described cybercrime and theft as the "greatest transfer of wealth in history" and estimated that it cost companies $338 billion annually. *See* Josh Rogin, *NSA Chief: Cybercrime Constitutes the "Greatest Transfer of Wealth in History,"* Foreign Pol'y (July 9, 2012), http://tinyurl.com/zatgr2f.

21. In November 2015, Representative Sheila Jackson Lee noted that harm to the electric grid would impact the ability to obtain water, electricity, and sewage, among other vital services. *See* Cory Bennett, *Congress Struggles to Secure Nation's Power Grid*, The Hill (Nov. 26, 2015), http://tinyurl.com/oksdtmt.

22. Consolidated Appropriations Act, 2016, H.R. 2029, 114th Cong. div. N, § 104(a)(1) [hereinafter CISA].

23. *Id.* § 104(b)(1).

24. *Id.* § 104(c)(1).

25. *Id.* § 105(d)(3).

26. *Id.* § 104(e)(1).

27. *Id.* § 104(d)(4)(A).

28. *Id.* § 104(d)(4)(C).

29. *Id.* § 105(d)(1).

30. *Id.* § 105(d)(5)(A)(i).

31. *Id.* § 102(4).

32. CISA defines "information system" by reference to the definition found in 44 U.S.C. § 3502(8), which in turn defines it as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." That definition is repeated, in mostly identical forms, in other legislation and regulation. *See* 38 U.S.C. § 5727; 48 C.F.R. § 204.7301.

33. The Cybersecurity Act of 2012, introduced in the Senate on February 15, 2012, contained an identical formulation. *See* S. 2105, 112th Cong. § 701.

34. *See* CISA § 102(17) (defining security vulnerability as "any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control").

35. S. Rep. No. 114-32, at 3 (2015) (all emphasis added unless otherwise indicated).

36. ECPA, comprised of both the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.*, and the Wiretap Act, 18 U.S.C. §§ 2510 *et seq.*, permits providers to "intercept, disclose, or use" certain information that is a necessary incident to the rendition of the service, *see* 18 U.S.C. § 2511(2)(a)(i), or to protect the "rights or property" of the provider, *see* 18 § U.S.C. 2702(b)(5), (c)(3). These exceptions are relatively limited in scope. *See, e.g.*, United States v. Councilman, 418 F.3d 67, 82 (1st Cir. 2005) (finding that copying all e-mails

transiting a network to gain commercial advantage did not qualify for the Wiretap Act's service provider exception).

37. Cyberspace Policy Review, *supra* note 7, at 18–19.

38. CISA § 102(5)(A).

39. S. Rep. No. 114-32, at 4. CISA, as passed, drew from three different proposed laws, so the weight of this report is uncertain.

40. A botnet is an "interconnected network of computers infected with malware without the user's knowledge and controlled by cybercriminals." *What Is a Botnet Attack?—Definition*, Kaspersky Lab, http://tinyurl.com/ja5zhb5 (last visited Feb. 19, 2016).

41. *Security Tip (ST04-015): Understanding Denial-of-Service Attacks*, U.S. Computer Emergency Readiness Team (Nov. 4, 2009), http://tinyurl.com/cjopv26.

42. The definition of "cybersecurity threat" is not limited to threats experienced by the ultimate target; it also includes threats that are "on *or through*" an information system. *See* CISA § 102(5)(A). An ISP may thus experience a "cybersecurity threat" regardless of whether it is the intended target or merely providing the network over which the threat transits.

43. In a typical DDoS attack, the packets transiting the network do not appear any different from other "legitimate" packets. *See* Paul Froutan, *How to Defend against DDoS Attacks*, Computer World (June 24, 2004), http://tinyurl.com/jf95ef8 ("What makes DDoS attacks such a challenge is that illegitimate packets of data are virtually indistinguishable from legitimate ones."). As a result, the difference between DDoS attacks and legitimate network activity can be the amount of information transiting the network. To date, the largest publicly reported DDoS attack was recorded at 400 gigabits per second (Gbps). *See* John E. Dunn, *World's Largest DDoS Attack Reached 400Gbps, Says Arbor Networks*, TechWorld (Jan. 27, 2015), http://tinyurl.com/pbmdcns. But according to security researchers studying a recent trend, many attacks are now much smaller, and at peak speeds of less than 1Gbps, significantly harder to distinguish from legitimate network activity. *See* Stephanie Weagle, *Are DDoS Attacks Getting Bigger or Smaller?*, Corero: DDoS Protection Blog (Mar. 24, 2015), http://tinyurl.com/j76fzso (describing "sub-saturating" attacks).

44. S. Rep. No. 114-32, at 21 ("Additional Views of Senator Ron Wyden").

45. *See* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 451 (2d Cir. 2001) ("[The] realities of what code is and what its normal functions are require a First Amendment analysis that treats code as combining nonspeech and speech elements, i.e., functional and expressive elements."); Junger v. Daley, 209 F.3d 481, 485 (6th Cir. 2000) ("Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment."); Def. Distributed v. U.S. Dep't of State, No. 1-15-CV-372, 2015 WL 4658921, at *6 (W.D. Tex. Aug. 4, 2015) (finding, for the purposes of a preliminary injunction analysis, open-source computer code providing instructions to 3D print weapon parts to be protected by the First Amendment).

46. United States v. Ulbricht, 31 F. Supp. 3d 540, 568 (S.D.N.Y. 2014) (rejecting constitutional challenge by operator of Silk Road website to conviction under the Computer Fraud and Abuse Act). Admittedly, *Ulbricht* is an extreme example. The defendant operated a marketplace for hacking tools, malicious software, and other cybersecurity exploits.

47. Memorandum of Law in Opposition to Defendant's Motion to Dismiss the Indictment, *Ulbricht*, 31 F. Supp. 3d 540 (No. 1:14-cr-00068-KBF), 2014 WL 7151214.

48. *See, e.g.*, EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 64 (1st Cir. 2003) (acknowledging the question but deciding the case on narrower grounds).

49. CISA § 102(5)(B).

50. United States v. Valle, 807 F.3d 508, 524 (2d Cir. 2015) (collecting circuit court decisions, and finding that because there was support in the statute for both interpretations, applying the rule of lenity and adopting the narrower interpretation of "exceeds authorized access"); *see also* Cloudpath Networks, Inc. v. SecureW2 B.V., No. 15-cv-0485-WJM-KLM, 2016 WL 153127, at *8–17 (D. Colo. Jan. 13, 2016) (summarizing the circuit split and the development of the interpretation of this provision).

51. 18 U.S.C. § 1030(a)(2)(C).

52. United States v. Nosal, 676 F.3d 854, 860 (9th Cir. 2012); *see also* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 205 (4th Cir. 2012).

53. *See, e.g.*, United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010); United States v. John, 597 F.3d 263, 272 (5th Cir. 2010) (affirming conviction of bank account manager who, in violation of employment policy, accessed internal database and provided customer account information to co-conspirator, who used the information to commit fraud); United States v. Drew, 259 F.R.D. 449, 461 (C.D. Cal. 2009) (concluding that "an intentional breach of the [terms of service] can potentially constitute accessing the . . . computer/server without authorization and/or in excess of authorization under the statute").

54. CISA § 104(a)–(c).

55. *Id.* § 104(a).

56. *Id.* § 102(13).

57. *Id.* § 104(a)(2).

58. *Id.* § 104(b)(1).

59. *See id.*

60. Cybersecurity Information Sharing Act of 2014, S. 2588, 113th Cong. § 2(4).

61. *Compare id.*, *with* CISA § 102(7).

62. *See* Greg Nojeim, *CISA Manager's Amendment Falls Short on Privacy and Security*, CDT (Aug. 3, 2015), http://tinyurl.com/gsbovrc (referring to defensive measures as a euphemism for countermeasures). The possibility of authorizing "countermeasures" furthered the debate over whether a victim could (or should be authorized to) lawfully "hack back" against the system it believed to be attacking it. *See* Mark Raymond, Greg Nojeim & Alan Brill, *Private Sector Hack-Backs and the Law of Unintended Consequences*, CDT (Dec. 15, 2015), http://tinyurl.com/oepkmxs.

63. CISA § 102(7)(A).

64. *Id.* § 102(7)(B).

65. S. 2588.

66. S. Rep. No. 114-32, at 5 (2015).

67. *Id.*

68. *Id.*

69. Katherine Mesenbring Field, *Agency, Code, or Contract: Determining Employees' Authorization under the Computer Fraud and Abuse Act*, 107 Mich. L. Rev. 819, 822 (2009).

70. A virtual private server (VPS) is a virtual machine that is sold as a service by an Internet hosting service. It permits the user to satisfy its computing and storage needs without purchasing otherwise cost-prohibitive hardware. The user is allocated a portion of a much larger physical server, though it appears to the user as if he or she is utilizing an entirely independent computer system. Contractual obligations aside, would a VPS user, whose "ownership" of the server is uncertain, be authorized to operate certain defensive measures on that server?

71. *See* CISA § 104(b)(1)(A), (B).

72. *See* United States v. Pervaz, 118 F.3d 1, 5 (1st Cir. 1997) (cloned cell phone fraud).

73. *See, e.g.*, Browning v. AT&T Corp., 682 F. Supp. 2d 832, 837 (N.D. Ill. 2009) (dismissing cell phone customer's invasion of privacy claim on the basis that the service provider was permitted to disclose the allegedly delinquent customer's records to collection agency pursuant to the service provider's protection of its "rights or property" under 18 U.S.C. § 2511(2)(a)(i)).

74. *See* United States v. Councilman, 418 F.3d 67, 82 (1st Cir. 2005).

75. CISA § 104(c).

76. *Id.*

77. *Id.* § 104(d)(1).

78. *Id.* § 104(d)(2).
79. *Id.* § 104(d)(3).
80. *Id.* § 104(d)(2)(A).
81. *Id.* § 107(b)(2)(A), (D).
82. *See id.* § 105(a)–(c).
83. *Id.* § 104(d)(2).
84. *Id.* § 104(d)(2)(B).
85. *See, e.g.*, Andy Greenberg & Yael Grauer, *CISA Security Bill Passes Senate with Privacy Flaws Unfixed*, Wired (Oct. 27, 2015), http://tinyurl.com/n9nueeo.
86. CISA § 105(b)(2).
87. *Id.* § 105(c)(1), (2).
88. CISA provides that "appropriate Federal entities" means the following departments: Commerce, Defense, Energy, Homeland Security, Justice, and Treasury, and the Office of the Director of National Intelligence. *Id.* § 102(3).
89. *Id.* § 105(c)(1)(C).
90. Protecting Cyber Networks Act of 2015, H.R. 1560, 114th Cong. § 6(a), (b).
91. CISA § 102(3)(B).
92. *Id.* § 203.
93. *Id.* § 103(b)(1)(B).
94. *See id.* §§ 105(c)(1)(B), 106(b)(2).
95. *See id.* § 105(c)(1)(E).
96. *Compare id.* § 106(b)(2) (explaining that in order to receive protection from liability the information must be shared in a manner that is "consistent with" § 105(c)(1)(B), which is the section establishing the DHS capability and process), *with id.* § 105(c)(1)(B) (requiring DHS to develop and implement a capability and process within DHS that "fully and effectively operates"), *and id.* § 105(c)(1)(E) (requiring that the same capability and process be developed and implemented in a manner that does not limit or prohibit otherwise lawful disclosures of communications, including through voluntary participation in a federal investigation).
97. *Id.* § 108(h).
98. *Id.*
99. *Id.* § 108(i).
100. *See* 48 C.F.R. § 204.7300.
101. *See* CISA § 105(c)(1)(B)(ii).
102. *Id.* § 108(a)(1).
103. *See* 18 U.S.C. § 2258A(a)(1).
104. CISA § 105(d)(5)(A).
105. *Id.* § 105(d)(5)(B).
106. *See* Deborah Norris Rodin, *The Cybersecurity Partnership: A Proposal for Cyberthreat Information Sharing between Contractors and the Federal Government*, 44 Pub. Cont. L.J. 505, 525 (2015) (discussing potential consequences to government contractors for cybersecurity information sharing and proposing a FAR amendment to limit the use of the information to adversely impact contractors).
107. Cybersecurity Information Sharing Act of 2012, S. 2102, 112th Cong., § 7(f).
108. *See* Computer Crime & Intellectual Prop. Section, Criminal Div., Dep't of Justice, Prosecuting Computer Crimes 10–11 (2015), *available at* http://tinyurl.com/qa9ydwm; *see also* United States v. Drew, 259 F.R.D. 449, 461 (C.D. Cal. 2009). In acknowledging the potential for overbroad applications of the CFAA, the Department of Justice proposed an amendment that would clarify and narrow the definition of "exceeds authorized access." *See Prosecuting Privacy Abuses by Corporate and Government Insiders*, Dep't of Justice (Mar. 16, 2015), http://tinyurl.com/meubo3e (remarks of Assistant Attorney General Leslie R. Caldwell).
109. *See* CISA § 107(b)(2)(D)(iii). The biennial report must also include "[a] review of the actions taken by the Federal Government based on cyber threat indicators or defensive measures shared" with it, including a review of "[t]he appropriateness of subsequent uses and disseminations of cyber threat indicators or defensive measures." *Id.* § 107(b)(2)(C)(i). Given that the law only requires a review of the "appropriateness" of subsequent uses—which implies an assessment rather than an explicit enumeration—it is doubtful that the federal government is required to report these other less-than-prosecution uses. Had Congress wanted a report on these uses, it would have provided for such a report. On the other hand, Congress could argue that the list of contents in the biennial report is not exhaustive, as it mandates "a review of actions . . . *including* a review of the following." *Id.* § 107(b)(2)(C).
110. Prosecutions under the Espionage Act are exceptionally rare, but have increased somewhat in the last decade. *See* Scott Shane & Charlie Savage, *Administration Took Accidental Path to Setting Record for Leak Cases*, N.Y. Times, June 19, 2012, http://tinyurl.com/gpovs7z; Alan Rozenshtein, *A Explainer on the Espionage Act and the Third-Party Leak Prosecutions*, Lawfare Blog (May 22, 2013), http://tinyurl.com/haqxp8v.
111. *See* 18 U.S.C. § 798(a).
112. *See, e.g.*, CISA §§ 103(a)(1), 104(c)(1).
113. Section 107(a)(2)(B) requires that the heads of the appropriate federal entities submit to Congress a "detailed report concerning the implications" of CISA, which, among other items, requires the entities to provide "an assessment of whether cyber threat indicators or defensive measures have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for the purpose of sharing cyber threat indicators or defensive measures with the private sector."
114. CISA § 106(a), (b).
115. *See id.* § 104(b).
116. *Id.* § 106(b).
117. *Id.* § 104(b)(1).
118. A cleared defense contractor may, under certain circumstances, also avail itself of other sources of liability protection for reporting cyber incidents and network penetrations of information systems. *See* H.R. Rep. No. 114-270, at 391 (2015) (Conf. Rep.).
119. S. Rep. No. 114-32, at 13 (2015).
120. *Id.*
121. *See* CISA § 105(a)–(c).
122. All of the following previously proposed laws included a "good faith" standard:
- Protecting Cyber Networks Act of 2015, H.R. 1560, 114th Cong. § 6(a), (b);
- Cyber Intelligence Sharing and Protection Act, H.R. 234, 114th Cong. § 3(b)(3)(A), (B) (2015);
- Cybersecurity Information Sharing Act of 2014, S. 2588, 113th Cong. § 6(c);
- Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. § 3(b)(3) (2013);
- Cybersecurity Act of 2012, S. 3414, 112th Cong. § 706(b); and
- Cybersecurity Information Sharing Act of 2012, S. 2102, 112th Cong. § 7(f).

By contrast, the Cybersecurity Information Sharing Act of 2015 had no "good faith" standard. *See* S. 754, 114th Cong. § 6(c)(1).
123. All of the following previously proposed laws included a "gross negligence" or "willful misconduct" exception, or the equivalent thereof (e.g., "intent to injure"):
- H.R. 1560, § 6(c);
- Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. § 6(c)(1);
- H.R. 234, § 3(b)(3)(B);
- S. 2588, § 6(d)(1);
- H.R. 624, § 3(b)(3)(B);
- S. 3414, § 706(g); and

8 S. 2102, § 7(f).