July 10, 2012

Submitted through the Federal eRulemaking portal at:
www.regulations.gov
DIB Cyber Security and Information Assurance Program Office
1400 Defense Pentagon
Washington, DC 20301-1400

RE: DOD-2009-OS-0183/RIN 0790-AI60
Comments on "Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities"[1]

To whom it may concern:

On behalf of the American Civil Liberties Union (ACLU), a non-partisan organization with more than a half million members, countless additional activists and supporters, and 53 affiliates nationwide we write to express our concern with the proposed Department of Defense (DoD) rule making the voluntary cybersecurity information sharing Defense Industrial Base (DIB) pilot program permanent.

Cybersecurity information sharing between the DOD and the DIB for the purpose of preventing, assessing, and reducing damage from cyber incidents is certainly a valid goal. The ACLU does not object to cybersecurity information sharing between the defense and the public sectors *per se*; there is technical data that can be shared that, once disentangled from any specific user, would have no privacy implications if disclosed. However, any programs that could expose personally identifiable information (PII) or the content of communications to government scrutiny must have certain basic safeguards. We are concerned that the rule does not explicitly include these protections which may lead to corporate oversharing or government misuse of sensitive data.

This comment recommends that the rule explicitly include privacy protections, discusses the privacy elements that the proposed rule should contain, and flags positive elements of the National Cyber Security Division's Joint Cybersecurity Services Pilot (JCSP)[2] that should be incorporated into the DoD program discussed herein. The ACLU appreciates the opportunity to submit this comment, and looks forward to providing the administration with further information if desired.

[1] Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities, 75 Fed. Reg. 27615 (proposed May 11, 2012) (to be codified at 32 C.F.R. pt. 236) [hereinafter the proposed rule].

I. Privacy protections must be explicitly contained in the text of the rule.

It is imperative that the rule explicitly include privacy protections for sensitive information such as PII or content of communications. As currently drafted, the rule does not do so. It instead references a June 2011 Privacy Impact Assessment (PIA) for the DIB pilot program.[3] The underlying DIB pilot PIA can be changed at any time without public notice, and does not carry the force of law that the proposed rule ultimately will. Putting these protections into the rule, however, will require the government to publicize any further changes that will directly impact privacy and will give the public and Congress the opportunity to comment on them.

It is often argued that explicit privacy protections cannot be drafted for internet or communication based programs because of the constantly evolving nature of technology. That is simply not true. Technology neutral terms can be used to describe techniques and values to protect sensitive information that will be applicable in the future regardless of changes in the underlying technology. Such principles can and should be directly incorporated into the rule.

II. The rule should include directions to minimize the collection and use of sensitive information and mandate public oversight of DIB information sharing.

The ACLU has repeatedly advocated that cybersecurity information sharing programs that implicate personally identifiable information or content abide by several basic principles: that companies make reasonable efforts to suppress sensitive information and only share what is necessary to address a cyber threat; that the government limit its use of cyber information obtained through cybersecurity information sharing programs to cyber security purposes, and that all cybersecurity programs be subject to regular public and congressional oversight.[4] All of these principles can and should be incorporated into the rule to protect any sensitive information that is shared with the government.

A. The rule should require companies to remove sensitive information from data they share with the government.

While sharing technical data can take place without implicating civil liberties, a presumption of privacy should protect PII and content of communications. Sharing PII and content should be an exception and not the norm, even if there could be certain limited exceptions to cover legitimate emergencies or other narrowly defined situations. The proposed rule only states that

[3] Privacy Impact Assessment (PIA) for the Defense Industrial Base (DIB) Cyber Security/Information Assurance Activities, available at http://dodcio.defense.gov/Portals/0/Documents/DIB%20CS-IA%20PIA_FINAL_signed_30jun2011_VMSS_GGMR_RC.pdf [hereinafter DIB pilot PIA].

[4] ACLU Interested Persons Memo on Cybersecurity Information Sharing Legislation and Privacy Implications in the 112th Congress, Apr. 16, 2012, *available at* http://www.aclu.org/files/assets/aclu_interested_persons_memo__re__cyber_leg_info_sharing_april_16_2012.pdf, ACLU letter to House of Representatives, Re: ACLU Opposition to H.R. 3523, the Cyber Intelligence Sharing and Protection Act of 2011 (CISPA); White House Statement of Administration Policy Includes Veto Threat, Apr. 26, 2012, *available at* http://www.aclu.org/files/assets/aclu_opposition_to_h_r__3523_cispa_-_white_house_sap_includes_veto_threat_-_4_26_12.pdf.

"the DIB participant shall perform a legal review of its policies and practices that support its activities under this program, and shall make a determination that such policies, practices, and activities comply with applicable legal requirements."[5] It is not clear that current law would require the protection of this sensitive information, or that privacy laws would in the future if pending cybersecurity legislation were to pass. The rule could include this affirmative protection however, unless such information were necessary to understand a cyber threat, which would offer more privacy protections for those who would be incidentally caught up in the information sharing program.

B. The rule should limit government use of information shared for cyber security purposes.

Information shared with the government under the new DIB program should only be used for cybersecurity purposes. This program should not become a backdoor collection tool for the government to collect intelligence, criminal or other information to repurpose or use as it sees fit. For example, the rule should require the government to immediately dispose of inadvertently collected PII that is not directly relevant to the cyber incident. The DIB pilot PIA referenced in the rule[6] makes mention numerous times of inadvertently collected information being used for "cyber security *or other lawful purposes*."[7] The fact that information has been voluntarily given to the government should not license full and unfettered use of such information.

C. The rule should create an oversight and accountability structure that includes public and congressional reporting.

The executive branch must provide regular, substantive and public reporting, ideally by Inspectors General and/or privacy officers. Such reporting would incentivize the sharing of only minimal amounts of information, that the government uses shared information responsibly, that there are consequences for the abuse of information, and that Congress and the public are regularly and meaningfully informed. Reports by IGs and Privacy Officers should be in unclassified form and made public, subject to a classified annex if deemed necessary by the submitter.

III. More robust protections exist in the Department of Homeland Security Information Sharing Program that can be incorporated into the rule.

The Department of Homeland Security (DHS) is facilitating a parallel pilot information sharing program to receive information directly from cybersecurity providers, known as the Joint Cybersecurity Pilot (JCSP).[8] In a Privacy Impact Assessment from January of 2012, DHS discussed in more detail the types of information to be shared and clear directives to dispose of information irrelevant to cybersecurity.[9] This demonstrates that such clarity and limitation is possible and practicable.

---

[5] Proposed rule at § 236.6 (c).
[6] DIB pilot PIA.
[7] *Id*. at G(2) (emphasis added).
[8] Privacy Impact Assessment for the National Cybersecurity Division Joint Cybersecurity Services Pilot (JCSP), DHS/NPPD-021 (Jan. 13, 2012) *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_nppd_jcsp_pia.pdf [hereinafter JCSP PIA].
[9] *Id.*

First, the JCSP PIA defines the specific types of information that might be shared: "e-mail addresses and other information that might be included in the message header or subject line,"[10] "domain names and simple mail transfer protocol (SMTP) strings,"[11] "to/from free-flow text fields, or subject line from individuals using federal websites or JCSP participants' networks and systems."[12] The identification of what information could be shared with DHS serves to inform the public of the level of PII that is handed over to the government in a given information-sharing arrangement.

Second, the JCSP has strict language regarding what can be done with any PII that is collected: "US-CERT will review all information it receives during the JCSP and only retain information that could be considered PII if that information is analytically relevant, otherwise, US-CERT will delete it."[13] It further states that"[o]nly information determined to be directly relevant and necessary to accomplish the specific purposes of the program will be retained, otherwise, the data is deleted,"[14] and "[if] information submitted contains information that could be considered PII, the analyst must determine if that information is related to the cyber threat. If the information is not related to the cyber threat, it is deleted."[15] This sort of guidance, if embedded within the proposed rule, will serve to protect PII from uses that are unrelated to cyber security.

Third, the JCSP-collected threat indictors or other threat information is not maintained by US-CERT in a "system of records."[16] In other words, to the extent that sensitive information is retained, it cannot be recalled or accessed by a personal identifier. The cybersecurity data base can't be searched by name, for example. The ACLU recommends that this important limitation also be explicitly incorporated into the DoD rule.

Finally, the JCSP includes a number of other important protections that the proposed rule should appropriate: participants must implement measures to ensure authorized end user consent to monitoring and interception,[17] quarterly internal reviews are conducted,[18] and all actions are logged within the JCSP analytic system.[19]

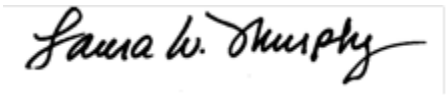
IV. Conclusion

The ACLU appreciates your consideration and looks forward to discussing the proposed rule. Again, we strongly recommend that the rule explicitly include privacy protections, including requirements to minimize the collection, retention and use of sensitive information and other limitations that have proven workable in the National Cyber Security Division's Joint

[10] *Id.* at Overview p. 4.
[11] *Id.* at Overview p. 3.
[12] *Id.* at 2.1.
[13] *Id.*
[14] *Id.* at 2.5.
[15] *Id.*
[16] *Id.* at 1.1.
[17] *See id.* at 4.2.
[18] *See id.* at 8.1.
[19] *See id.* at 8.2.

Cybersecurity Services Pilot (JCSP). Please contact Michelle Richardson at 202-544-1681 with any questions.

Sincerely,



Laura W. Murphy, Director
ACLU, Washington Legislative Office

Michelle Richardson, Legislative Counsel
ACLU, Washington Legislative Office