COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE DEPARTMENT OF DEFENSE

[DOD-2009-OS-0183/RIN 0790-AI60]

Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities

July 10, 2012

By notice published on May 11, 2012,[1] the Department of Defense ("DOD") issued an interim final rule "to establish a voluntary cyber security information sharing program between DOD and eligible [Defense Industrial Base ("DIB")] companies."[2] Pursuant to DOD's notice, the Electronic Privacy Information Center ("EPIC") submits the following recommendations to ensure transparency, oversight, and accountability over the DOD information disclosure program. At a minimum, the DOD information disclosure program should: (1) narrowly define "cyber incident" and "threat"; (2) remain voluntary; (3) impose liability on private companies that disclose excess information; (4) involve auditing oversight performed by the Attorney General or Inspector General; and (5) fully adhere to the Privacy Act of 1974 and the Freedom of Information Act.

EPIC is a public interest research center located in Washington, D.C. EPIC focuses on emerging civil liberties issues and protecting privacy, the First Amendment, and constitutional values. EPIC has a long history of promoting transparency and accountability for cyber security and government data collection programs, specifically through the enforcement of the Privacy

[1] Department of Defense (DOD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities, 77 Fed. Reg. 27615 (proposed May 11, 2012) (to be codified at 32 C.F.R. pt. 236) [hereinafter "Interim Rule"].
[2] *Id*.

Act.[3] EPIC has submitted administrative agency comments in opposition to a proposed Department of Homeland Security program similar to the current proposal.[4] In addition, EPIC has filed numerous FOIA requests for information regarding state fusion centers that raise significant questions about privacy protection.[5] These "fusion centers," in pursuit of information concerning purported cyber threats, collect vast amounts of personal data on individuals who are suspected of no wrongdoing. EPIC believes that transparency into cyber security programs, as well as aggregation and analysis systems, is crucial to the public's ability to monitor the government's national security efforts and ensure that federal agencies respect privacy rights and comply with their obligations under the Privacy Act.

I. The DOD Should Narrowly Define "Cyber incident" and "Threat"

The Interim Rule permits DIB companies to "receive . . . information about cyber threats and mitigation strategies or share information about cyber incidents that may compromise critical DOD programs and missions."[6] The Interim Rule defines "cyber incident" as "actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein."[7] This definition is much broader and less precise than other language used to describe computer crimes.[8] The definition allows DIB companies to disclose personally identifiable information ("PII") for not only actual "cyber

[3] *See EPIC v. NSA*, 678 F.3d 926 (D.C. Cir. 2012); *Cybersecurity Privacy Practical Implications*, **EPIC**, http://epic.org/privacy/cybersecurity/; *EPIC v. NSA – Cybersecurity Authority*, **EPIC**, http://epic.org/privacy/nsa/epic_v_nsa.html.
[4] *See* EPIC, Comments of the Elec. Privacy Info. Ctr. to the Dep. of Homeland Sec.: Sys. of Records Notice and Notice of Proposed Rulemaking, Dec. 15, 2010, DHS-2010-0052 and DHS-2010-0053 *available at* http://epic.org/privacy/fusion/EPIC_re_DHS-2010-0052_0053.pdf.
[5] *See Information Fusion Centers and Privacy*, **EPIC**, http://epic.org/privacy/fusion/.
[6] Interim Rule, 77 Fed. Reg. at 27615.
[7] *Id.* at 27618.
[8] *See, e.g,*. Computer Fraud and Abuse Act, 18 U.S.C. §1030. The Act proscribes individuals from "exceeding authorized access" or otherwise causing "damage" to federal government computers and computers related to federal activity. The Act defines "exceeds authorized access" as "access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter" and defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(6), (8).

incidents" but also potential "cyber incidents."[9] The Interim Rule defines "threat" as "any circumstance or event with the potential to adversely impact organization operations (including mission, functions, image, or reputation), organization assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service."[10] As with "cyber incident," DOD's definition for "threat" is equally, if not more, nebulous. EPIC objects to these particularly broad definitions because they increase the risk of innocuous online activities being classified as "threats" or "cyber incidents"—thereby providing a pretext for the collection of user data.

For example, recently a group of over fifty university professors, academics, and policy experts published an open letter to Congress asking lawmakers to oppose the Cyber Intelligence Sharing and Protection Act ("CISPA"), because the bill would "encourag[e] the transfer of [internet] users' private communications to US Federal agencies."[11] Further, the letter opposed CISPA "using vague language to describe network security attacks, threat indicators, and countermeasures [because this langauge] allow[s] the possibility that innocuous online activities could be construed as 'cybersecurity' threats."[12]

Like CISPA, the Interim Rule also uses broad and vague langague to describe "cyber incidents" and "threats." As it is written now, the Interim Rule can permit DIB companies to report innocuous online activities to DOD, in complete violation of individual privacy rights. Therefore, DOD needs to refine and clarify the definion of "cyber incident" and "threat."

II. The Cyber Security Information Disclosure Program Must Remain Voluntary

The Interim Rule claims that participation in the DOD's information disclosure program is voluntary and that each DIB participant will have the opportunity to decide whether to

[9] Interim Rule, 77 Fed. Reg. at 27618.
[10] *Id.* at 27619.
[11] Dan Auerbach, *An Open Letter From Security experts, Academics and Engineers to the U.S. Congress: Stop Bad Cybersecurity Bills*, **Electronic Frontier Foundation Blog** (Apr. 23, 2012), https://www.eff.org/deeplinks/2012/04/open-letter-academics-and-engineers-us-congress.
[12] *Id.*

participate.[13] EPIC stresses that should the disclosure program continue, it must remain voluntary. When a member of the public voluntarily provides a private company with PII as part of a commercial transaction, she entrusts the company to use the PII without releasing it to the government. Ensuring that PII is not transferred unnecessarily—even in a voluntary manner—between companies and the government is vital to privacy rights.

The disclosure program's Privacy Impact Assessment ("PIA") states that through the program DOD "provides cyber threat information and information assurance (IA) best practices to DIB companies to help them better protect their unclassified networks to protect DOD unclassified information; and in return, DIB companies report certain types of cyber intrusion incidents" to DOD.[14] This provision should not be interpreted as a *quid pro quo* arrangement between DOD and the DIB participant. First, DOD should provide DIB participants with best practices to protect the participants' networks, and DOD should never intentionally withhold crucial information that could ward against threats. Second, the process set forth in § 236.5(c), should require that DOD provide the DIB with the results of its initial analysis before the DIB participant "voluntarily share[s] additional information that is determined to be relevant."[15] This process should be followed before every additional disclosure of information. At no point in time should the government be allowed to withhold its findings about the incident until the DIB agrees to provide additional information.

Additionally, any unclassified information concerning reported threats that DOD obtains from DIB companies must be made freely available to all DIB participants. The more information that is made available to the DIB participants collectively, the more opportunity individual

[13] Interim Rule, 77 Fed. Reg. at 27616.
[14] Dept. of Def., Privacy Impact Assessment for the Defense Industrial Base (DIB) Cyber Security/Information Assurance Activities 5 (Nov. 2008) [hereinafter Privacy Impact Assessment] *available at* http://dodcio.defense.gov/Portals/0/Documents/DIB%20CS-IA%20PIA_FINAL_signed_30jun2011_VMSS_GGMR_RC.pdf.
[15] Interim Rule, 77 Fed. Reg. at 27620.

participants will have to determine whether they are being attacked, and the better able they will be to assess threats without sharing PII with DOD.

III. The DOD Disclosure Program Needs Oversight and Should Impose Liability on Private Companies for Disclosing Excess Information

The Interim Rule should impose liability on DIB participants that intentionally or negligently disclose more PII than is necessary for identifying cyber threats. As the PIA concedes, during its analysis DOD will find PII "that had not been identified by the DIB company when the information was submitted."[16] It is unacceptable for DIB participants to share more private information than is absolutely necessary to detect a threat. Moreover, DIBs may have a fiduciary obligation to protect the private records of their clients and customers. Therefore, the disclosure program should discourage private companies from unnecessarily leaking PII. To this end and as discussed above, EPIC recommends that DOD narrowly defines cyber "threat" or "incidence" and narrowly prescribes information needed to detect cyber threats. This information should also be given to DIB companies when DOD provides its IA best practices. Additionally, the Interim Rule should be amended to impose fines on private companies that intentionally or negligently disclose excessive PII. These two changes will both limit the scope of the disclosure program and deter companies from leaking PII with abandon.

Finally, in order to make sure that all of privacy protections are sufficiently implemented, EPIC urges the DOD to add a provision which would create independent review power to an external entity. The current rule lacks any type of oversight authority, which means that there is no mechanism for ensuring that DOD and the DIB participants adhere to the procedures set forth in the rule.[17] EPIC recommends that either the Attorney General or the Inspector General be given authority to conduct regular audits on DIB companies' PII disclosure, DOD's leaking of information to other agencies, and DOD's use of the information it receives. The audit process

[16] Privacy Impact Statement, *supra* note 14, at 9.
[17] *See generally* Interim Rule.

should also verify that DOD imposes fines on DIB companies for disclosing excessive PII. Finally, DOD should publish annually for the public an unclassified summary of the audit review.

IV. The DOD Disclosure Program Should Fully Adhere to the Privacy Act and Freedom of Information Act

The Interim Rule states that the information shared by DIB participants under this program could potentially include "extremely sensitive proprietary, commercial, or operational information that is not customarily shared outside of the company, and that the unauthorized use or disclosure of such information could cause substantial competitive harm to the DIB participant that reported that information."[18] While the DOD is keenly aware of DIB companies' "extremely sensitive proprietary" information, DOD needs to also fully protect individuals' sensitive PII that it obtains through the disclosure program. One effective way to do this is by fully adhering to the Privacy Act of 1974.

The Privacy Act of 1974 places extensive obligations on federal agencies that collect and use personal information.[19] The Interim Rule states:

> [N]othing in this rule or program abrogates the Government's or the DIB participants' rights or obligations regarding the handling, safeguarding, sharing, or reporting of information, or regarding any physical, personnel, or other security requirements, as required by law, regulation, policy, or a valid legal contractual obligation.[20]

Therefore, the DOD should not exempt records that it collects through this program from Privacy Act provisions. Moreover, the DOD should not claim broad "routine use" disclosures of records that it collects from DIB companies.

In addition to the Privacy Act, the DOD disclosure program should fully adhere to the openness requirements of the Freedom of Information Act ("FOIA"). The Interim Rule states "the Government will protect sensitive nonpublic information under this Program against unauthorized public disclosure by asserting applicable FOIA exemptions, and will inform the non-Government source or submitter (e.g., DIB participants) of any such information that may be subject to release

[18] Interim Rule, 77 Fed. Reg. at 27620.
[19] 5 U.S.C. § 552a (2006).
[20] Interim Rule, 77 Fed. Reg. 27617.

in response to a FOIA request, to permit the source or submitter to support the withholding of such information or pursue any other available legal remedies."[21] Presumably, DOD will assert Exemption 4, which allows agencies, in some circumstances, to withhold "trade secrets and commercial or financial information obtained from a person and privileged or confidential."[22]

A narrrow interpretation of FOIA Exemption 4 is essential to providing oversight of the disclosure program because it will allow the public to assess the agency's conduct, which is the central purpose of the FOIA. In *Pub. Citizen Health Research Group v. FDA*, *704 F.2d 1280, 1288 (D.C. Cir. 1983),* the Court of Appeals for the D.C. Circuit rejected a broad definition of "trade secrets" and held that for the purposes of FOIA, a "trade secret" should be limited to: "a secret, commercially valuable plan, formula, process, or device that is used for the making, preparing, compounding, or processing of trade commodities and that can be said to be the end product of either innovation or substantial effort." A narrow interpretation of Exemption 4 should be adopted in this Interim Rule because a broader definition would be contrary to the FOIA's express mandate that the exemptions be narrowly construed.[23]

Furthermore, EPIC underscores that FOIA's purpose is to facilitate transparency by providing public oversight of government operations. Therefore the DOD should only apply FOIA exemptions when they are absolutely necessary. The (b)(4) exemption should not be used to conceal wrongful conduct. For example, in a recent FOIA matter involving the Federal Communications Communication ("FCC") investigation of Google StreetView, the agency's final report included extensive redactions, which the agency based on the (b)(4) exemption.[24] But when the full report without redactions became available, it was clear that the agency had asserted the

[21] Interim Rule, 77 Fed. Reg. at 27620.
[22] 5 U.S.C. § 552(b)(4).
[23] *Dep't of Air Force v. Rose*, 425 U.S. 352, 360-62 (1976).
[24] *FCC Investigation of Google Street View*, **EPIC**, http://epic.org/privacy/google/fcc_investigation_of_google_st.html.

exemption to conceal its own conduct in the matter. [25] This was improper and other federal agencies should be cautious about representing that they will assert the (b)(4) exemption.

Conclusion

Should the DOD's information disclosure program continue, the agency must uphold its obligations under the Priacy Act and the Freedom of Information Act. EPIC urges the agency to adopt the recommendations to the Interim Rule set out above, and EPIC anticipates the agency's specific and substantive responses to each of these proposals.

Respectfully submitted,

Marc Rotenberg
EPIC Executive Director

Khaliah Barnes
EPIC Open Government Fellow

Amie Stepanovich
EPIC Associate Litigation Counsel

Valerie O'Driscoll
EPIC Law Clerk

Pavel Sternberg
EPIC Law Clerk

[25] *Id.*