July 9, 2012

Federal Docket Management System Office
4800 Mark Center Drive, East Tower, Suite 02G09
Alexandria, VA 22350-3100

Re: Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities

The Constitution Project (TCP) submits this comment in response to the Department of Defense interim final rule, "Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities," instituted May 11, 2012. The interim final rule, 32 C.F.R. Part 236, establishes a voluntary cyber security information sharing program between the DoD and eligible DIB companies in order to safeguard DoD information. TCP agrees that a carefully crafted information sharing program that incorporates robust safeguards for privacy rights can be an important tool to protect against cyber threats that could compromise information critical to U.S. national security and economic security interests. However, there are two aspects of the rule that raise concern: the lack of adequate protection of personally identifiable information (PII) and the content of private communications, as well as the insufficiency of measures to ensure effective application of Executive Order 13556, "Controlled Unclassified Information."

TCP is a nonprofit organization in Washington, DC that promotes and defends constitutional safeguards by bringing together liberals and conservatives who share a common desire to preserve civil liberties. The Constitution Project's bipartisan Liberty and Security Committee, launched in the aftermath of the September 11 attacks, includes members of the law enforcement community, legal academics, former government officials, and advocates from across the political spectrum who develop and advance proposals to protect civil liberties as well as our nation's security.

In January 2012, TCP's Liberty and Security Committee released a report entitled *Recommendations for the Implementation of a Comprehensive and Constitutional Cybersecurity Policy.*[1] The report recognizes that government operates in an increasingly digital world which requires new and cooperative strategies to secure networks storing information critical to U.S. national security and economic interests. However, when new cybersecurity strategies increase the flow of information from private networks to government agencies, the government must also extend Fourth Amendment guarantees.

The *Cybersecurity* report analyzes the protection of civil liberties in current and proposed government cybersecurity programs. The report recommends government cybersecurity programs incorporate safeguards to ensure protection of fundamental constitutional rights. Such safeguards include effective oversight; procedures to limit the sharing of PII between private

[1] The Constitution Project's Liberty and Security Committee, *Recommendations for the Implementation of a Comprehensive and Constitutional Cybersecurity Policy* (2012) (hereafter *TCP Cybersecurity* report), available at http://www.constitutionproject.org/pdf/TCPCybersecurityReport.pdf.

sector and government actors; and limits on government access to, or use of, content acquired through cyber security operations.[2]

In this comment, TCP first addresses the protection of privacy rights within the interim final rule, 32 C.F.R. Part 236 of "DoD-DIB Voluntary Cyber Security and Information Assurance Activities." While TCP applauds the DoD's recognition of the privacy concerns involved, the interim final rule lacks sufficient safeguards to limit the sharing and use of personally identifiable information and content of private communications. Thus, TCP recommends amending the rule to incorporate tighter restrictions on DIB disclosure of PII and content of communications to the DoD, limits on DoD disclosure of PII and content to law enforcement, and strong accountability mechanisms.

In addition to TCP's Liberty and Security Committee's concern with restricting the flow of personal information from the private sphere to the government, TCP also aims to expand the flow of information from the government to the public. The Committee released a report in July 2009 entitled *Reining in Excessive Secrecy: Recommendations for Reform of the Classification and Controlled Unclassified Information Systems*,[3] which advocates reforming the controlled unclassified information (CUI) framework to create a uniform, interagency policy regarding the categorization and treatment of sensitive but unclassified information. The goal of such reform is to promote information sharing among government agencies and across the branches of government as well as maximize transparency to the public.

The *Reining in Secrecy* report discusses the history and status of CUI, particularly the lack of clarity and consistency concerning what constitutes CUI and how it should be treated. TCP recognizes the importance of a CUI category, but over-marking information as CUI threatens government transparency and accountability, while undermining efforts to keep truly sensitive information secure. Moreover, hundreds of agency-assigned labels for sensitive information impede information sharing and weaken collaboration crucial to U.S. national security. The report argues that universally used and understood procedures are necessary to protect both civil liberties and U.S. national interests. The report made recommendations to promote openness and limit secrecy within the government and with the public.[4]

In November 2010, the Obama administration issued Executive Order 13556, "Controlled Unclassified Information,"[5] which incorporates many of TCP's recommendations and began the process of establishing a national, uniform CUI framework. TCP commends the DoD interim rule for recognizing that the DIB CS/IA program must be consistent with, and support, Executive Order 13556. However, the interim rule has not fully achieved that objective. Thus, in this comment, TCP provides three recommendations to ensure effective application of Executive Order 13556 to DoD-DIB Voluntary Cyber Security and Information Assurance Activities.

---

[2] *Id.*
[3] The Constitution Project's Liberty and Security Committee, *Reining in Excessive Secrecy: Recommendations for Reform of the Classification and Controlled Unclassified Information Systems* (2009) [hereafter *TCP CUI* Report], available at http://www.constitutionproject.org/pdf/178.pdf.
[4] *Id.*
[5] Exec. Order 13556, 75 Fed. Reg. (Nov. 9, 2010) [hereafter Exec Order 13556], available at http://www.archives.gov/isoo/policy-documents/eo-13556.pdf.

As demonstrated by these two reports, TCP both strives to protect individual privacy for information flow *from* companies *to* the government, and also promotes information sharing and transparency for information flow *to* companies *from* the government. TCP promotes both civil liberties and an open government; such principles are not only consistent, but mutually reinforcing. In this comment, TCP explains how the DoD's DIB CS/IA program can protect PII and the content of private communications as well as encourage information sharing and openness.

I. Protection of Personally Identifiable Information and Private Communications

TCP commends the DoD for recognizing the serious privacy risks involved with the DIB CS/IA program. Under the program, DoD provides cyber security threat information to DIB companies to enable them to protect DoD information, and the DIB companies in return voluntarily share information with DoD regarding cyber incidents. Under the rule, the DoD affirms "a foundational element of this bilateral information sharing model is the recognition that the information being shared between the parties includes extremely sensitive nonpublic information, which must be protected against unauthorized uses and disclosures."[6] The interim rule acknowledges that the government and DIB companies may share the most sensitive types of unclassified information including individuals' PII and private communications.[7] The DoD cites their own Privacy Impact Statement (PIA) for the DIB CS/IA program, which describes privacy risks associated with the collection of such personal information and how the DoD will address these risks to safeguard civil liberties.[8] While recognition of privacy concerns is an essential first step, the interim final rule contains insufficient safeguards to limit the sharing and use of PII and the content of private communications.

Information flow from private DIB companies to the government can contain PII and the content of private communications. Indicators of known or suspected cyber threats that are shared with the DoD may contain PII, such as e-mail addresses, location and other information that might be included in the message header. Malware can also be embedded within the content of an email so private communications, like the body of an email, may be shared with the DoD in addition to PII. Unnecessary sharing of PII and private communications impedes on individual privacy, threatening the Fourth Amendment. The interim final rule limits information sharing to protect trade secrets, but there are little to no restrictions on the sharing of PII and content of private communications. Thus, TCP recommends the following:

1. Adopt a stringent standard for DIB disclosure of PII and private communications to DoD

The interim rule's language authorizes unlimited and extraneous sharing of PII and the content of private communications from DIB companies to the DoD. The DIB CS/IA program should regulate the original flow of PII and content of communications from DIBs to the DoD. This is especially important because once the DoD obtains PII or content of communications as part of an incident report or other reporting by a DIB company to the government, DoD may then

[6] Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities, 77 Fed. Reg. Background, 27616 (May 11, 2012) [hereinafter *Interim Rule*] (to be codified 32 C.F.R. pt 236).
[7] *Id.*
[8] *Id.*

seek to share the threat information with other DIB companies to enable them to protect against the threat. Thus, although information flowing from the government to private companies is less likely to contain PII or private content, this scenario would pose such a risk.

Within the interim rule, there is no stringently defined standard to limit when DIB companies can share PII and content of communications with the DoD. Section 236.5(c) states generally that DIB participants may share information that is "determined to be relevant to a reported incident, including information regarding forensic analyses, mitigation and remediation, and cyber intrusion damage assessments."[9] There are no specific rules requiring that PII or the content of private communications be stripped from information before it is shared or otherwise limiting such sharing. In fact, the rule promotes "sharing to the greatest extent possible information to provide the clearest understanding of the cyber threat."[10] TCP fully supports complete DIB reporting of information indicating cyber threats to covered defense information, but PII and content of communications should be stripped from this reported information. There must be limits on the disclosure of PII and content in order to mitigate the privacy risks involved with government handling of information.

At a minimum, the DoD should incorporate into the regulation the limits to sharing that are outlined in its own Privacy Impact Assessment (PIA) for this program. The DoD's PIA states that DIB companies will only provide the DoD with PII that is "relevant and material to understanding the technical attributes of the incident."[11] The PIA continues to explain that any inadvertently collected PII is reviewed by DoD personnel and is only further processed or retained if it is "necessary for subsequent analysis in furtherance of its DIB CS/IA activities."[12]

An even more effective model is provided by the Department of Homeland Security's (DHS) PIA, since DHS is also a partner in the DIB program and its PIA provides more robust privacy safeguards. The DHS PIA describes how to limit disclosure of PII and private communications to the government in the context of the DIB CS-IA program. The PIA states information is only shared if it is "reviewed and pre-determined to be an indicator of a known or suspected cyber threat."[13] In addition, during the pilot program, US-CERT developed procedures for "removing unnecessary PII, encrypting certain information, and marking and handling of PII data collected."[14]

TCP recommends the DoD adopt a specific and stringent standard to limit DIB disclosure of PII and content of private communications to the DoD. As suggested by the PIAs, PII and content of private communications should only be transferred from DIBs to the DoD if it is a necessary part of a cyber-threat indicator, needed to understand the technical attributes of the incident, and necessary for subsequent analysis in furtherance of DIB CS/IA activities. When

---

[9] *Id*. 27620 Sec. 236.5(c).
[10] *Id*. 27616, Background.
[11] Department of Defense CIO, *Privacy Impact Assessment for the Defense Industrial Base (DIB) Cyber Security/Information Assurance Activities* (2008) [hereinafter *DoD PIA*], available at http://dodcio.defense.gov /Portals/0/Documents/DIB%20CS-IA%20PIA_FINAL_signed_30jun2011_VMSS_GGMR_RC.pdf.
[12] *Id.* 9.
[13] Department of Homeland Security, *Privacy Impact Assessment for the National Cyber Security Division Joint Cybersecurity Services Pilot (JCSP) DHS/NPPD-021* 4 (2012) [hereinafter *DHS PIA*], available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_nppd_jcsp_pia.pdf.
[14] *Id*. 12.

DIB participants send the DoD information, they should remove all unnecessary PII and anonymize as much information as possible without hindering cybersecurity efforts. Further, as explained below, the rule should impose use restrictions to limit DoD's sharing and use of any PII or content it obtains.

2. Impose limits on DoD sharing of PII and private communications with law enforcement

Any PII and content of communications that the government obtains through the DIB CS/IA program should be used only for cybersecurity operations and not general law enforcement or intelligence fact gathering. TCP's *Cybersecurity Report* recommends that PII and content acquired through cybersecurity operations should only be used as necessary to implement the cybersecurity program and protect networks. Law enforcement should not have access to such personal information without a warrant or probable cause; otherwise such broad sharing risks violating individuals' Fourth Amendment rights. Without tight limits on sharing of PII and content of communications, the DoD could hand over private information to law enforcement for uses unrelated to cybersecurity crimes.

The interim final rule contains insufficient limits on internal government sharing of PII and the content of private communications acquired through cyber security operations. In Sec. 236.5(e), the interim rule authorizes internal use and disclosure of attribution information to government personnel and government support contractors as long as they are "bound by appropriate confidentiality obligations and restrictions relating to the handling of this sensitive information and are engaged in lawfully authorized activities."[15] This provision is insufficient to safeguard highly personal information that could be turned over to law enforcement. Moreover, section 236.6(d) states that "none of the restrictions on the Government's use or sharing of information under the DIB CS/IA program shall limit the Government's ability to conduct law enforcement, counterintelligence activities, or other activities in the interest of national security."[16] Although TCP agrees that the program should not impose new limits on the government's ability to conduct law enforcement or counterintelligence activities, it is also important that private information received through the DIB program should not be shared with other government agencies for such purposes, except under very limited circumstances as explained below.

TCP recommends that the DoD place meaningful restrictions on sharing PII and the content of private communications obtained through the DIB CA/IA program with other government agencies. TCP's 2012 *Cybersecurity* report outlines effective limits on sharing PII and private communications with law enforcement agencies. Specifically, the report urges that PII and content of communications should not be shared with law enforcement officials or relied upon as evidence for a non-cybercrime unless the PII/content was legitimately obtained as a necessary component of the data specifically flagged as a possible cybersecurity threat. If the PII or content of communications collected is not necessary to describe or indicate a cybersecurity crime, there must be probable cause and a warrant before the information is shared with law enforcement. While TCP recommends a probable cause standard for disclosure of PII or private communications to law enforcement, we note that the interim rule does not even apply a requirement for reasonable suspicion based on specific and articulable facts equivalent to the

[15] *Interim Rule* at 27620 Sec. 236.5(e).
[16] *Id.* 27620 Sec. 236.6(d).

standard in section 2703(d) of the Stored Communications Act.[17] The interim rule should be amended to ensure a proper predicate before personal information is shared with law enforcement.

3. Strengthen accountability mechanisms

In the interim rule, the limited privacy protections regulating government handling of PII and the content of private communications are not mandatory or enforceable. The DoD asserts that the DIB participants "typically" treat information regarding potential cyber intrusion incidents as extremely sensitive information and tightly control it.[18] However, a description of common practice does not create safeguards against abusive or extraneous use of PII or content of private communications obtained through the program. In addition, the DoD refers to its PIA to ensure there are safeguards in place to protect individual privacy,[19] but PIAs have no regulatory force and thus cannot be enforced. If the DoD or DIB participants did not abide by the safeguards articulated in the PIA, individuals harmed in the process would have no avenue of recourse.

In order to strengthen enforcement mechanisms and accountability in the DIB CA/IA program, TCP offers two recommendations. First, the DoD should integrate robust safeguards into the text of the interim rule, not just the PIA. For example, TCP's first recommendation above advocates including the PIA's standard for DIB sharing of PII and private communications within the interim rule. Second, TCP recommends robust and meaningful oversight. The DHS PIA concerning the DIB CA/IA pilot program explains that the DHS uses the US-CERT Oversight and Compliance Office to ensure procedures are in place and that all personnel are familiar with, understand, and adhere to the guidelines. The US-CERT Oversight and Compliance Office conducts quarterly internal reviews to evaluate the program and assess its compliance with applicable guidelines, procedures, and applicable laws and regulations.[20] The DoD should use the DHS oversight procedures as a model; it should require regular internal audits to ensure the program's compliance with regulations and relevant guidelines.

II. Application of Executive Order 13556: Controlled Unclassified Information

Executive Order 13556, "Controlled Unclassified Information," which limits use of control markings and promotes information sharing, should be fully integrated into the DoD's interim rule. The rule focuses on defense against cyber threats to covered defense information within DIB and DoD networks. Covered defense information, as defined by the DoD, is unclassified information that is marked for restricted distribution in accordance with DoD policy,[21] which means it is controlled unclassified information (CUI). Thus, the interim final rule regulates information that falls under the Executive Order on CUI.

The Executive Order establishes that control markings – which limit the circumstances under which the information may be shared – may only be justified by statute, regulation, or government-wide policy, which significantly limits the extent of government secrecy. Most

[17] 18 U.S.C. §§ 2703.
[18] *Interim Rule* at 27616, Background.
[19] *Id.*
[20] *DHS PIA*, 14.
[21] *Interim Rule* at 27618, Sec. 236.2(c).

importantly, the EO encourages information sharing by establishing a presumption of openness.[22] The Order limits the kind of information that constitutes CUI and sharing of CUI within and among the branches of government to enhance government accountability and strengthen cooperative strategies.

TCP applauds the DoD for recognizing the application of Executive Order 13556 to the DIB CA/IA program. The DoD states "the rule and program are intended to be consistent and coordinated with, and updated as necessary to ensure consistency with and support for other federal activities… such as those that are being led by the National Archives and Records Administration pursuant to Executive Order 13556."[23] The interim final rule recognizes confidentiality of information exchanged under the program can only be protected to the extent "authorized by law, regulation, and policy," which includes executive orders.[24] However, the rule does not properly ensure implementation of the new CUI framework from Executive Order 13556 into its treatment of covered defense information. Therefore, TCP recommends the following:

1. Do not apply sharing limitations to non-sensitive Government Furnished Information

The interim rule limits the extent to which all Government Furnished Information (GFI) may be shared. As explained above, the rule's definition of covered defense information constitutes CUI. However, the rule applies restrictions to the sharing of all GFI. GFI is defined broadly as information provided by the Government under the voluntary DIB CS/IA program, including but not limited to cyber threat information and information assurance practices. The rule's restrictions on sharing GFI are problematic because not all GFI is CUI; some GFI could be non-sensitive information. Thus, the rule restricts the sharing and exposure of information that should be open to the public. For example, the DoD states that the "DIB participants shall not share GFI outside of their company or organization, regardless of personnel clearance level."[25] This is overly restrictive because not all GFI, information furnished by the government in connection with the DIB CA/IA program, is sensitive.

If the information obtained through the program is not CUI or classified information, DIB participants and the DoD should make the information easily available to the public so as to promote government transparency and accountability. When the interim rule outlines restrictions on the exposure of cybersecurity information, it should not refer to all GFI, but only "covered defense information," including, but not limited to, critical program information, technical information restricted according to DoD directives, PII, or information that can be interpreted or pieced together by hostile intelligence systems to derive critical intelligence.[26]

2. Ensure that CUI is not restricted to the same extent as classified information

Strict handling restrictions, like distribution on a "need to know" basis, should only apply to classified information. The DoD's use of the umbrella term GFI means that under the interim rule CUI—and even non-sensitive information -- must be treated as strictly as classified

[22] Exec. Order 13556.
[23] *Interim Rule* at 27617, Background.
[24] *Id.* 27620, Sec. 236.6(a).
[25] *Id.* 27619 Sec. 236.4(i).
[26] *Id.* 27618, Sec. 236.2(c).

information even though it is due a less stringent level of protection. For example, section 236.4(g) states the "DIB participants may only share GFI within their company or organization on a need to know basis, with distribution restricted to U.S. citizens."[27] While CUI should be protected as needed, such information should be available to government and trusted non-government actors when the information is relevant to their work. E.O 13556 states, "The mere fact that information is designated as CUI shall not have a bearing on determinations pursuant to any law requiring the disclosure of information or permitting disclosure as a matter of discretion, including disclosures to the legislative or judicial branches."[28] Sharing information only on a "need to know" basis is too restrictive for CUI. The rule should, in accordance with the Executive Order, promote information sharing.

3. Clarify that prior labels for CUI will be phased out

TCP recognizes prior designations for CUI information, such as "Sensitive But Unclassified" and others noted in section 236.2(2)(vi), are still in use because Executive Order 13556 is not yet fully implemented. While the interim rule may currently apply to those prior labels, it should also clarify that as government agencies adapt to the new universal CUI Framework, prior labels will be phased out. The rule should state that once the Executive Order is fully implemented, restrictions on the sharing of covered defense information will only apply to CUI labeled information.

III. Safeguard PII while implementing Executive Order 13556

TCP urges that DoD modify the interim rule both to protect privacy and to promote government openness. These goals are consistent; while the DoD promotes broad information sharing of CUI, it can, and should, still safeguard PII and the content of private communications. As discussed above, the information flow *from* companies *to* the government creates threats to privacy requiring robust privacy safeguards, whereas the information flow *to* companies *from* the government requires rules to promote information sharing and transparency.

As also noted above, in the DIB CA/IA program, the government may seek to distribute cyber threat information that it received from one DIB company to other DIB companies in the program. If DoD amends the rule to adopt TCP's first recommendation above – requiring that DIB companies may only share PII and/or content of communications that is a necessary component of the threat information– then the scope of PII and content contained in cyber threat information that DoD could share back with other DIB companies would be limited.

However, if the DoD does receive extraneous PII or content of communications from DIB companies, the DoD should strip the information of the PII and content before distributing it to all DIB participants or other government agencies. Where applicable, this can be done by providing the information in aggregate format or by using other anonymization techniques. Thus, the solution is not to prevent sharing of the threat information, but simply to remove the PII and content of private communications before sharing. This is consistent with Executive Order 13556 because Sec 6(a) states "this order should be implemented in a manner consistent with: (1) applicable law, including protections of confidentiality and privacy rights; (2) the

[27] *Id.* 27620, Sec 236.4(g).
[28] Exec. Order 13556, Sec 2(b).

statutory authority of the heads of agencies, including authorities related to the protection of information provided by the private sector to the Federal Government."[29]

In sum, TCP promotes broad information sharing of covered defense information, but only if PII and the content of private communications are effectively safeguarded in the process.

Conclusion

TCP commends the recognition of the privacy risks involved with the DIB CA/IA program, and the explicit reference to Executive Order 13556 for handling of covered defense information. However, TCP has outlined two problem areas. First, the DoD's interim final rule lacks sufficient safeguards to limit the sharing and use of PII and the content of private communications. Second, the interim rule fails to effectively incorporate Executive Order 13556 into the government handling policy of the DIB CA/IA program. Finally, TCP explained how the DoD could safeguard PII and the content of private communications while promoting an open and transparent government in accordance with Executive Order 13556. The Constitution Project encourages the DoD to revise and expand 32 C.F.R. Part 236 according to the comments and recommendations above, as well as TCP's two reports, *Cybersecurity* and *Reining in Secrecy*.

Sharon Bradford Franklin
Senior Counsel
The Constitution Project
1200 18th Street, NW
Suite 1000
Washington, DC 20036
202-580-6928

[29] *Id.* Sec6(a).