PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD

March 21, 2014



Karen Neuman
Chief Privacy Officer
Department of Homeland Security
650 Massachusetts Avenue, NW
Washington DC 20528

Megan Mack
Civil Rights and Civil Liberties Officer
Department of Homeland Security
131 M Street, NE
Washington DC 20002

Dear Ms. Neuman and Ms. Mack,

I write on behalf of the Privacy and Civil Liberties Oversight Board to provide feedback on the draft Executive Order 13636 Privacy and Civil Liberties Assessment Report that you submitted to the Board on February 24, 2014. As you know, Section 5(c) of Executive Order 13636 on Improving Critical Infrastructure Cybersecurity requires that "the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of DHS shall consult with the Privacy and Civil Liberties Oversight Board" in producing this report, which, under Section 5(b), must make recommendations to "minimize or mitigate" the "privacy and civil liberties risks of the functions and programs" undertaken pursuant to the Order.

The Board recognizes that this first year's report is based upon the preliminary start up activities of the Department of Homeland Security (DHS) and the other agencies tasked with responsibilities under EO 13636. The coming year will provide far greater opportunities for assessment of agency activities and how protection of privacy and civil liberties has been addressed. The Board looks forward to engaging in a dialogue with DHS as part of the "consultation" process for revisions to the report in future years.

The PCLOB has not been involved in the development of the policies discussed in this first year's report and has not yet had the opportunity for any in-depth study of the privacy and civil liberties issues presented by the cybersecurity programs called for in the Executive Order. As a result, our feedback consists of highlighting encouraging aspects of the report, noting places where we believe the policies and recommendations described in the report should be further developed or improved

going forward, and identifying areas that we believe require more substantial improvement as implementation of EO 13636 proceeds in the coming years.

As a preliminary matter, we note that the draft report submitted to the Board consists of a series of separate reports produced by DHS and nine other agencies. These separate chapters are not uniform in format or content. While some agencies, such as DHS, the Department of Defense (DOD), and the Office of the Director of National Intelligence (ODNI) have provided detailed analyses of the privacy and civil liberties issues raised by their cybersecurity programs and activities, others like the Department of the Treasury and the Department of Justice did not examine in detail their programs or the privacy and civil liberties issues presented. Finally, certain agencies, like the Department of Transportation, candidly and appropriately stated that the agency "has not implemented any programs or systems under EO 13636 during the reporting period," and explained that they were submitting the report to explain their work in support of the interagency process. The Board urges that either the agencies choose to create one integrated report next year, which would enable readers to more comprehensively understand the efforts that are being made, or that, at minimum, all agencies employ the same format and provide a detailed analysis of the issues presented.

Encouraging Aspects of the Report

The Board would like to highlight the following areas of the report that demonstrated agencies are carrying out the terms of EO 13636:

1) Section 5(a) of the Order directs that agencies shall ensure that privacy and civil liberties protections are incorporated into cybersecurity programs developed under the Order, and states that these protections "shall be based upon the Fair Information Practice Principles." Several agencies – DHS, DOD, and ODNI – conducted a thorough analysis of their activities under the Fair Information Practice Principles (FIPPs). In particular, DOD's chart summarizing its FIPPs analysis explains the protections provided in a clear and accessible manner. The Department of Commerce also conducted a short analysis of compliance with the FIPPs in connection with the development of the Cybersecurity Framework.

2) Both DHS and DOD recognize that the cybersecurity information sharing called for under the Order can lead to the collection and sharing of personally identifiable information (PII). Similarly, ODNI, while noting that the Intelligence Community will not be collecting additional information under the terms of EO 13636, recognizes that the Order requires greater dissemination of information, which may include PII. All three agencies conducted a detailed analysis of the privacy issues raised by this potential sharing of PII, including the extent to which PII may be shared. DHS and DOD note that in some situations individuals

may voluntarily share their information, in which case protections relating to notice and minimization may be readily applied. All three agencies also explain that in other circumstances, PII may be shared without the subject's consent because the information is part of cyber threat information (e.g., malware as part of an email) – both in the context of cyber threat information provided *by* the government *to* the private sector or as a component of information received *from* the private sector that is then further shared by one government agency with other government agencies. The agencies correctly note that in these situations it will not be possible or appropriate to provide the type of prior notice that would otherwise be called for by application of the FIPPs.

3) Section 4(c) of EO 13636 requires the expansion of the Enhanced Cybersecurity Services program (ECS) to all critical infrastructure sectors. Both DHS and DOD – the two agencies with primary responsibilities under the current ECS program – have developed procedures to limit the amount of PII that is shared under this program, so that private sector entities only share anonymized aggregated information with government entities and do not share PII.

Need for Further Development

The Board recognizes that most of the implementation of EO 13636 remains to be completed in the coming year and beyond. In addition, over the course of the coming year many of the policies described by agencies require further development and/or further explanation in order to assess whether they appropriately balance national security concerns with privacy and civil liberties. For example:

1) DHS' assessment states that the Privacy Office will conduct "an in-depth Privacy Compliance Review of the entire ECS Program in 2014" and will report on the results in next year's report under the Order. Similarly, the Department of Commerce has noted that it will complete an assessment of the privacy and civil liberties risks associated with the Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST) – required under Section 7 of the Order and released by NIST in February 2014 – in the coming year. However, the report does not explain how the reviews will be conducted or the metrics that will be applied.

2) The Department of Energy (DOE) provided a recitation of the FIPPs with reference to existing agency policies, which is helpful. However, the report does not examine how these policies may apply to any cybersecurity activities by DOE or any other programs DOE may be undertaking under EO 13636. For example, while the discussion of sharing and dissemination notes that agency personnel must review personal information to be shared

before making it available, there is no discussion of the types of personal information the agency expects to share as part of DOE cybersecurity programs or of how and when personal information will be minimized.

3) As noted above, both DHS and DOD recognize that when PII is a component part of a cyber threat indicator, it will not be appropriate or possible to provide notice to the individual or minimize the PII. However, the agencies were inconsistent in recognizing the possibility that an individual whose PII is provided to the government as a component part of cyber threat information may actually be a victim of a cyberattack rather than the perpetrator (or, as described elsewhere in the analysis, as opposed to someone who is voluntarily providing PII to the government). This concept that victims of cyberattacks may have their personal information involuntarily shared with the government is recognized in some places (e.g., DHS pp. 18, 20), but not in others (e.g. DHS pp. 13-14; DOD pp. 5, 8, 22). Although prior notice would still not be appropriate in such cases (e.g., a victim of spearphishing does not voluntarily provide PII to the government and cannot be given meaningful prior notice before such sharing), the agencies should examine whether other FIPPs would nonetheless apply to such situations, such as in providing a meaningful redress mechanism. In addition, DOD should recognize that when Defense Industrial Base (DIB) companies voluntarily provide information to DOD, this does not mean that any individuals whose PII may be provided have voluntarily chosen to share their information with DOD (e.g., DOD p. 22).

4) Similarly, DHS and DOD should give greater attention to the appropriate minimization standards to be applied when individuals' PII is involuntarily shared with the government. In describing situations where PII may be shared as a component part of cyber threat information, the agencies sometimes note that PII will only be shared if it is "necessary" to characterize a cyber threat (e.g., DHS p. 14; DOD pp. 11, 13), but in other instances the agencies state that information will be shared if it is merely "relevant" to the cyber incident (e.g. DOD pp. 12, 14). The former standard – "necessary" to describe the cyber threat information – appears to provide more robust privacy safeguards than the relevance standard, and it is not clear whether there is any rationale for applying different standards in different situations or what those differences might be. It would also be helpful for the report to address what oversight mechanisms will be in place to ensure that involuntarily shared PII will only be disclosed where necessary. In addition, the reports should not treat this PII as "inadvertent PII," (e.g., DOD pp. 2, 3, 9, 11, 22) since it may be collected and shared deliberately as a component part of the cyber threat information. Viewing this PII is "embedded in" the information being shared (e.g., DOD pp. 3, 9) is a more accurate way to

describe it. (The DHS report at p. 27 correctly acknowledges that PII may be a key element of cyber threat information.)

5) As noted, the report envisions situations in which involuntarily obtained PII will be shared either with other government agencies or private sector firms. The report should address what restrictions have been or can be imposed on use or dissemination of such information, including statutory or regulation requirements or contractual restrictions, to restrict use of such information to cybersecurity purposes. Similarly, DHS states that sharelines "will minimize PII," (e.g. DHS p. 8), but the word "minimize" has multiple meanings depending on context. It would be helpful if a more specific word were used, or if DHS would otherwise spell out more specifically what is meant by "minimize" each time that term is used (e.g., DHS pp. 14, 21, 38.)

6) In many places in the report, agencies provide broad general statements of policy without the details necessary to assess whether protections for privacy and civil liberties will be adequate or appropriate. For example, DHS notes that it may retain "considerable amounts of data" which will be "generally in minimized form" in connection with warnings about cyber threats, without detailing or referring to established minimization procedures. Similarly, DOD notes that in the unlikely event that information shared for cybersecurity purposes "contains information about how an individual exercises their First Amendment rights," DOD will "apply appropriate handling safeguards" which include "compliance with strict need-to-know access controls." No further detail is provided as to the nature of those controls. The Board recognizes that at this stage such generalities may be necessary given the fact the implementation of the Order is only preliminary. However, it will be important to develop more specific standards in the coming year.

7) Similarly, DHS provides a series of recommendations in its report which will require far greater detail, including specific metrics, in order to provide meaningful guidance. For example, DHS urges the establishment of "specific procedures" for limiting dissemination of PII or other sensitive information in "shareline" reports, without providing any details on the type of dissemination limits that should be applied.

8) Both DOD and ODNI refer to existing audit procedures, but do not specify how often such audits are conducted, by whom, or the metrics that are applied. Likewise other reporting agencies should address whether audit procedures will be employed, and what these procedures will involve.

9) The Department of Health and Human Services and the Department of Transportation specifically noted that, thus far, they have not implemented any programs under EO 13636 and to date their work has consisted of participating in interagency review of certain government-wide policies under EO 13636. Similarly, the General Services Administration (GSA) states that its role has been limited to procurement of information and communications technology, and GSA provides a brief analysis of how these activities have complied with the FIPPs. Should these agencies' roles increase in the future, more details and a more in-depth analysis under the FIPPs will be necessary.

Aspects of the Report that Need Improvement

The Board notes the following areas needing improvement.

1) The agencies have not followed uniform standards in conducting their analyses, and the reports vary widely in the comprehensiveness of the review provided. The Board understands that the participating agencies decided that DHS would only *compile* and would not synthesize the separate reports submitted by all the participating agencies. The Board urges, however, that for next year, either the agencies work together to create one unified report, or alternatively, all agencies should apply the same standards and level of rigor in their analysis – and this should involve increasing the comprehensiveness of some reports so they are on par with each other.

2) Some agencies, like the Department of the Treasury and the Department of Justice, did not include any meaningful assessment of the privacy and civil liberties risks of programs undertaken by their agencies as required by Section 5(b) of the Order, despite acknowledging that their agencies do play a role in implementing the Order. The Treasury Department's report simply notes that they will apply "certain protocols, such as removing any personally identifiable elements that are not relevant to cybersecurity" and that "any dissemination [of cyber threat information] must be consistent with applicable authorities including laws protecting privacy, civil liberties, and national security information." The Justice Department simply states that actions taken under the Order must "be consistent with the need to protect privacy and civil liberties" and notes that information stored in the iGuardian database will only include "relevant information" that will be "covered by the privacy compliance documentation" for the Guardian database. Neither report includes any actual analysis of privacy risks nor any description of protections to be provided so that readers of the report can evaluate the steps that have been or will be taken.

3) In some places agencies have set forth rules or recommendations that should be strengthened. For example, DHS recommends that the agency "should give consideration

to requiring a review or audit of sharelines" by DHS's Privacy Office and Civil Rights and Civil Liberties Office. The Board urges that this be strengthened to require such audits. Regular audits could include examination of an appropriate sample of sharelines and would enable reviewers to test the adequacy of safeguarding procedures. For example, DHS notes that it is not feasible to try to anticipate all the types of information that may be incidentally associated with cyber threats (DHS p. 21). Regular audits could enable agencies to determine what types of information are being shared so that any need for adjustments in privacy protections can be identified. In addition, it would be helpful to conduct audits of operations under the ECS program. DHS notes that "mission drivers will enhance accuracy of any PII in the threat reporting" under ECS (DHS p. 30), but audits assessing the accuracy and utility of threat information could provide an additional mechanism for improving accuracy.

4) Toward the end of its report, DOD provides a short analysis of Fourth and First Amendment issues. We are concerned that unlike DOD's detailed treatment of the FIPPs analysis, this brief and fairly conclusory constitutional analysis raises more questions than it answers. We assume that there has already been an in-depth legal analysis of the ECS program or its predecessor, the DIB program, and it might be better to just reference that more detailed analysis.

Process Going Forward

As noted above, the Board recognizes that agencies had little time to begin implementation of EO 13636 before starting to prepare this initial report, and consequently the report does not, and cannot, provide a great amount of detail on how safeguards for privacy and civil liberties will actually be implemented. We anticipate that revisions to the report under EO 13636 in the coming years will address many questions that are unanswered in the current report.

As we have discussed, in order to make the PCLOB's consultation role under the Executive Order meaningful, the Board requests that DHS informally confer with the Board much earlier in the process in the coming year. We look forward to working with you in this context.

Sincerely,

David Medine

David Medine
Chairman