Lisa J. Sotto
Chair, DHS Data Privacy and Integrity Advisory Committee

November 19, 2012

The Honorable Janet Napolitano
Secretary of the Department of Homeland Security
U.S. Department of Homeland Security
Washington, DC 20528

Mr. Jonathan R. Cantor
Acting Chief Privacy Officer
U.S. Department of Homeland Security
Washington, DC 20528

Re: DHS Data Privacy and Integrity Advisory Committee Recommendations on Privacy in Cybersecurity Pilot Programs (Report 2012-01)

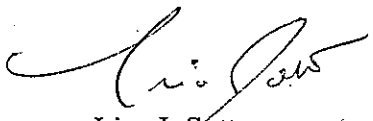
Dear Secretary Napolitano and Mr. Cantor:

It is my pleasure to convey to you the enclosed report that sets forth privacy recommendations for DHS to consider when evaluating the effectiveness of cybersecurity pilots. The report also contains a summary of specific privacy protections for DHS to consider when sharing information from a cybersecurity pilot with other agencies. This report is the result of an extensive effort by both Committee members and subject matter experts working closely with DHS components to research this topic. We are grateful for the Department's cooperation in providing access to important programmatic information on cybersecurity pilot activities and the officials with direct knowledge and expertise on the matter.

We hope you will agree that implementing these recommendations in connection with cybersecurity pilots will enhance the protection of personal information while maintaining the effectiveness of cybersecurity pilots and the Department's mission.

Please do not hesitate to contact me if you have any questions regarding these recommendations.

Sincerely,



Lisa J. Sotto

Enclosure

cc: Members of the DHS Data Privacy and Integrity Advisory Committee

REPORT 2012-01 OF THE DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE (DPIAC)

ON PRIVACY AND CYBERSECURITY PILOTS

As approved in public session

NOVEMBER 7, 2012

Contents

I. Introduction and Objectives

The Department of Homeland Security (DHS) has established a Committee under the Federal Advisory Committee Act (FACA) to provide advice and recommendations to the DHS Secretary and Chief Privacy Officer (CPO) on privacy issues involved in achieving DHS mission objectives. This Committee, the DHS Data Privacy and Integrity Advisory Committee (DPIAC), provides advice on programmatic, policy, operational, administrative, and technological issues within DHS that relate to personally identifiable information (PII), as well as data integrity and other privacy-related matters.

DHS also leads Federal agency cybersecurity operational activities. In 2009, the DPIAC formed an *ad hoc* subcommittee to address privacy issues that relate to cybersecurity, because DHS was increasingly addressing cybersecurity in ways that impacted privacy. The Subcommittee's role has been to provide views about specific questions and programs, as well as to offer general perspectives on how to improve the manner in which privacy is addressed as part of those programs.

a. Request for the Study

The DHS Chief Privacy Officer (CPO) asked the DPIAC for a set of recommendations regarding privacy issues that have an impact on cybersecurity pilot projects. In a letter to the DPIAC Chair from December 6, 2011 (attached as Appendix A), the CPO wrote:

> In order that the Department's cybersecurity efforts may benefit from the DPIAC's substantial experience in both technology and privacy, I request that the Committee provide written guidance on privacy best practices for DHS cybersecurity pilot projects. Specifically, I request that the Committee consider the following issues:
>
> 1. What privacy considerations should DHS include in evaluating the effectiveness of cybersecurity pilots?
>
> 2. What specific privacy protections should DHS consider when sharing information from a cybersecurity pilot project with other agencies?
>
> I ask that the Committee build its guidance on the fact-finding conducted by the Cybersecurity Subcommittee to produce an unclassified report and recommendations so that not only the Department but also the larger cybersecurity community can benefit from the Committee's advice.

b. Summary of Approach

To assist the DPIAC in responding to the CPO's request, the Cybersecurity Subcommittee (hereafter referred to as the Subcommittee) reviewed a variety of materials that could inform findings regarding privacy as part of cybersecurity pilots. The

Subcommittee reviewed discussions and briefings from previous meetings, relevant DPIAC reports, and external sources. This paper and its findings result from that approach, addressing the second DHS question on information sharing first.

c. Scope of Cybersecurity Pilots

Cybersecurity pilots can encompass a broad range of new programs, including those arising from new legislation as well as emerging programs with various private and/or public sector entities. As noted in the letter requesting this report, DHS "uses pilot programs and proof of concept efforts to test new approaches to fulfilling its cybersecurity mission. In so doing, the Department also coordinates with other Federal agencies, with international, state, and local government partners and private sector partners."

An example of one such pilot program that the Subcommittee has been briefed on is based on a set of agreements with the Department of Defense (DoD). Specifically, DHS and DoD have agreed to coordinate on cybersecurity pilots that identify solutions for automated cybersecurity tools and processes to benefit mutual stakeholders, consistent with each department's authorities. The "Joint Cybersecurity Pilot Program" provides a formal vehicle to source and identify pilot technologies for implementation, by creating an expedited, comprehensive, coordinated, and repeatable selection and evaluation methodology to rapidly develop, assess, and transition cybersecurity solutions. Under this program, pilots are designed to evaluate innovative technology solutions that inform and advance cybersecurity capabilities; pilots are expected to last 6 to 12 months (following acquisitions, planning, and environment setup).

Pilots under this program address one or more of the following criteria:

- Evaluate viable cybersecurity technology solutions in an efficient, rapid, and repeatable methodology in support of DHS and DoD missions.

- Provide a formal method to source and identify pilot technologies, by creating an expedited, coordinated, and repeatable selection and evaluation methodology for the rapid piloting and transitioning of cybersecurity solutions.

- Leverage common mission elements, foster collaboration, and preserve each department's authorities.

- Reduce duplication of effort.

- Eliminate ineffective and inefficient solutions from further consideration.

- Inform DHS component agencies about cybersecurity solutions and opportunities.

Although these criteria do not yet address privacy, DHS's request for an assessment from the DPIAC reflects its understanding that privacy needs to be part of the process for any pilot, so that privacy requirements and controls can be built into pilots going forward.

In response to the DHS request, the remainder of this paper focuses on key findings and recommendations that can be operationalized by the Agency.

II. What specific privacy protections should DHS consider when sharing information from a cybersecurity pilot project with other agencies?

Subcommittee Findings

The Subcommittee notes that one of the goals of any cyber pilot is to ensure that when information is received on a cyber risk, vulnerability, threat, or incident, the information reaches the right people at the right time.

The Subcommittee believes that DHS policy should be based on criteria that leverage the DHS Fair Information Practice Principles (FIPPs) and, consistent with current law, should attempt to minimize any negative impact on individual privacy caused by new technology.

The Subcommittee believes that the recommendations in this report can help to improve how pilots incorporate safeguards to protect privacy that are based on the FIPPs, which underpin most privacy laws, including the Privacy Act.

Committee Recommendations

Basic Considerations

- A cybersecurity pilot should first seek less privacy-invasive alternatives (i.e., those that do not involve PII, involve less of it, or reduce the PII's sensitivity).

- Cybersecurity pilots should continue to incorporate robust privacy safeguards, such as those that implement the FIPPs, rather than follow the minimum statutory requirements.

- The content of messages (which includes the body of an email, attachments, and the subject line, but does not include identifying or "header" information) should be examined only in cases where the level of risk indicates that such a measure is necessary or appropriate.

Data Minimization Rules

- DHS should develop and implement clear data minimization rules and policies in a cybersecurity pilot to ensure that, consistent with the FIPPs, PII and the content of private communications:
    - are only collected, used, or shared when necessary for program purposes;
    - are only collected when they are a necessary part of the cyber threat information; and
    - have mechanisms in place to protect that information after collection.

  Such rules can serve as a model for agencies partnering with DHS in a pilot.

- When data collected during a cyber pilot includes PII that is then found to be not relevant to cybersecurity (e.g., over-inclusive analysis), the information should be deleted as soon as practicable.

Notice

- Employees and public users of Federal systems should receive notice, to the greatest extent practicable, about the collection, use, and sharing of information for cybersecurity purposes.

- This notice can be accomplished through a variety of vehicles, including log-on banners and user agreements for internal users, privacy policies posted on Federal websites, and the publication of unclassified Privacy Impact Assessments (PIAs) for the public.

- Where technologically and economically feasible and where it does not compromise security or an active investigation, notification should be provided to those individual's whose computers are the cause of a significant data leakage or other significant problem involving threats to PII or the content of private communications.

General Sharing and Use Restrictions

- When DHS receives information that includes PII and/or the content of private communications, information sharing should be limited to what is necessary to serve the pilot's purposes. That data should be protected consistent with the FIPPs, such as through the use of aggregate formats, wherever possible.

- Data collected for cybersecurity pilots should only be used, or shared with other agencies, for cybersecurity purposes, unless required by existing law. A record of the organizations with whom the data is shared should be maintained with DHS's copy of the data.

Limit Law Enforcement Sharing

- If DHS shares information with law enforcement that it has received through a cybersecurity pilot, and that information contains PII or the content of private communications, then DHS should do so in a manner that is strictly limited to avoid the risk of a criminal investigation of an individual without sufficient predicate.

- Although law enforcement officials participating in a cybersecurity pilot in real time may need immediate access to information flowing into DHS to enable them to respond as necessary to protect networks from a cyber threat, stricter privacy safeguards and ongoing protection of the information are needed before law enforcement should be permitted access to PII received through a cyber pilot for purposes of a criminal investigation or prosecution.

- If law enforcement officials or agencies seek to conduct a criminal investigation or prosecution unrelated to cybersecurity using information obtained as part of a cyber pilot, such access should be limited; in this situation, unless otherwise required by law, DHS should only provide access to information about specific individuals or the content of private communications:
    - when DHS finds that there is reasonable suspicion, based on specific and articulable facts, to believe that the information is evidence of a crime that has been or is about to be committed, or
    - in exigent circumstances, such as for use in protecting individuals from an imminent threat of death or serious bodily harm or a serious threat to the safety of minors.

National Security Sharing and Use

- Private information shared with DHS for cybersecurity pilots should not be used for national security purposes unrelated to cybersecurity, except in exigent circumstances (as described above) or as required by existing law.

- DHS should participate in a cybersecurity pilot in which information from private networks is shared with a defense or intelligence agency only under rigorous governance and oversight processes, which are consistent with the FIPPs and make use of the technology protections described below.

Civilian Agency Sharing

Cybersecurity pilots for civilian government networks, and information sharing programs with the private sector, should be led or overseen by DHS, as the civilian agency with operational oversight over cybersecurity (see OMB Memorandum 10-28).

More Robust Safeguards for Information from Private Networks

When a pilot program provides DHS with access to information from private networks, privacy risks may increase. Therefore, DHS should ensure that the program is designed to incorporate robust safeguards to mitigate against these privacy risks, including:

- The government should not directly monitor or collect content on private networks, unless properly authorized under law (e.g., with a valid warrant).

- For pilots in which private companies share information about cybersecurity threats with DHS, DHS should encourage companies to make reasonable efforts to remove information that can be used to identify specific persons unrelated to the cybersecurity threat, as well as the content of private communications, before sharing the information with DHS. If DHS receives such unrelated PII from a company as part of a pilot, DHS should remove that information from any databases as soon as practicable.

- DHS should provide education, information, and tools as appropriate to government and industry stakeholders to assist with the identification and removal of PII or the content of private communications.

Data Retention Policies

- Records should not be kept any longer than needed to fulfill the purpose of the pilot; specifically, strict data retention periods for a pilot should limit the retention periods for PII and the content of private communications for the time frame necessary to address the particular cyber threat for which the information is being retained.

- Retention periods should be documented in a records schedule consistent with guidance issued by the National Archives and Records Administration.

Technology

- Privacy-by-design and privacy-enhancing technologies should be examined as a part of system development. DHS should rely on technological tools to provide robust privacy protections in pilots.

- Privacy technology guidance for pilots should address protection of information when developing systems that include: access control at the human, machine, or software level; databases that include cybersecurity information; and logs that are enabled at all times and are later available for audit.

- DHS should consider technology best practices to implement in pilots. Once rules to protect PII and the content of private communications are in place, a number of tools and techniques exist to implement those protections in a way that mitigates the risk of privacy abuses (e.g., randomization, obfuscation, and encryption).

Data Integrity and Quality Assurance

DHS should address the quality and integrity of data involving PII that are used during cybersecurity pilots. Specifically, DHS should assure that any data under a cyber pilot be handled carefully to preserve its physical and logical integrity -- including relevant metadata that would allow tracking data provenance, in order to facilitate corrections and redress when required. Many technologies provide substantial support for data integrity and quality; DHS should consider their use in the context of pilot design.

Security

Cybersecurity pilots can create attractive targets for malicious actors. High security controls should be implemented to control external access to the system and protect the data.

III. What privacy considerations should DHS include in evaluating the effectiveness of cybersecurity pilots?

Subcommittee Findings

The Subcommittee notes that effective privacy controls are not yet listed among the outcomes for cybersecurity pilot programs described on page 4 of this paper and should be included in an evaluation of such pilots.

DHS's designation of this Cybersecurity Subcommittee under the DPIAC, whose members represent a broad spectrum of non-Federal privacy experts fully cleared at the appropriate national security level, could itself be viewed as a best practice. The Subcommittee has been periodically briefed at each stage of the EINSTEIN program, and has received briefings and provided feedback on advance copies of PIAs. Although the formation and use of such a group may not be necessary for every pilot, this approach may be useful for pilots and subsequent programs that have significant implications for privacy.

DHS also performed a Privacy Compliance Review (PCR) to assess compliance with the privacy measures articulated in the EINSTEIN PIAs. This public review, which assessed whether the program had the intended privacy controls in place, was productive and should be repeated at regular intervals.

The Subcommittee finds that transparency of cybersecurity pilot efforts is vital, and applauds DHS for publishing unclassified PIAs at each stage of EINSTEIN's development.

Committee Recommendations

Develop PIAs

- Before implementing a cybersecurity pilot, DHS should develop a PIA, and provide this PIA as a model for agencies partnering with DHS under the pilot. As it has done with the Comprehensive National Cybersecurity Initiative (CNCI) Initiative 3 PIA, DHS should continue to publish unclassified versions if any future cybersecurity PIAs require classification.

- DHS should continue to develop PIAs for pilots and programs that involve sharing cybersecurity information.

- PIAs should be part of upfront planning to indicate cost-effective means for addressing privacy as part of cybersecurity pilots.

- DHS should continue to perform PCRs to assess compliance with specified privacy measures for pilots.

First Assess the Adequacy and Efficacy of a Cybersecurity Pilot Involving PII

- For any pilot in which PII or the content of private communications may be collected, DHS should analyze the "fit for purpose" of the pilot, in a manner consistent with DPIAC's Framework for Privacy Analysis of Programs, Technologies, and Applications.
    - First, DHS should assess whether the pilot can produce useful results.
    - Then, DHS should review the effectiveness of proposed security measures in meeting threats, including by conducting risk analyses and considering alternatives.

  If a pilot cannot effectively assess the program, then it is not worth any intrusion into privacy rights.

- During a pilot evaluation, if effectiveness is not established and the pilot is deemed not worthwhile, DHS should not collect PII or the content of private communications as part of a program based on that pilot.

- Once effectiveness has been established and the program is deemed worthwhile, privacy safeguards should be incorporated into the program's design from the beginning.

- Ultimately, DHS will need to review the performance of cybersecurity pilots and how information is shared with other agencies to evaluate pilot effectiveness. Appendix B lists a series of questions to consider for inclusion in such an evaluation.

Ensure Scalability

To ensure that cybersecurity pilots can scale to a larger and longer-term state in which privacy is appropriately addressed, the Committee recommends that DHS devote proper attention to analyzing the scalability of privacy safeguards as pilots move beyond their initial phase. This should be done in a manner consistent with the DHS FIPPs, and can be built into ongoing PIAs.

Involve Privacy Experts

Privacy officers, or other officials whose job responsibilities include examination of privacy issues (e.g., agency CPOs), should be actively involved in developing cyber pilots from the beginning, not brought in after the fact.

Strengthen Oversight

- Identification and analysis of privacy risks should be used to inform the level of oversight and protection; high risks or threats to privacy should receive more scrutiny.

- Protecting privacy as part of information sharing in cybersecurity pilots calls for a strong oversight process. The Committee believes that DHS should continue to build robust, meaningful, and transparent oversight of cybersecurity pilot programs to assess compliance with the privacy rules recommended above, including:
    - Regular, periodic privacy reviews conducted by the Privacy Office as programs are designed, developed, and implemented;
    - Periodic Inspector General reports, including at the unclassified level (i.e., at least every two years), to assess the extent to which use restrictions, minimization policies, data retention limits, and all other privacy rules have been followed; and
    - Submission of any newly proposed program for review by an independent entity, such as the Privacy and Civil Liberties Oversight Board (PCLOB) if that entity becomes operational, and collaboration with that entity in ongoing, regular reviews of the implementation of programs.

- Any oversight process should involve reviews of policy for how cybersecurity pilots are designed, as well as compliance for how pilots are operationalized; compliance activities to be evaluated include periodic, random audits and evaluations, to help ensure that security policies are met.

- A sound process should have a high degree of transparency and public engagement, but be able to invoke closed/classified sessions with appropriate justification (as PIAs do now).

- A pilot should also include a process for training staff about proper information handling.

APPENDIX A:
DHS Request Letter to DPIAC

December 6, 2011

Mr. Richard Purcell, Chairman
DHS Data Privacy and Integrity Advisory Committee (DPIAC)
P.O. Box 104
Nordland, Washington 98358

Re: DPIAC Guidance on Cybersecurity Pilot Programs

Dear Richard,

As you know, the Department of Homeland Security uses pilot programs and proof of concept efforts to test new approaches to fulfilling its cybersecurity mission. In so doing, the Department also coordinates with other Federal agencies, with international, state, and local government partners and private sector partners.

In order that the Department's cybersecurity efforts may benefit from the DPIAC's substantial experience in both technology and privacy, I request that the Committee provide written guidance on privacy best practices for DHS cybersecurity pilot projects. Specifically, I request that the Committee consider the following issues:

1. What privacy considerations should DHS include in evaluating the effectiveness of cybersecurity pilots?

2. What specific privacy protections should DHS consider when sharing information from a cybersecurity pilot project with other agencies?

I ask that the Committee build its guidance on the fact-finding conducted by the Cybersecurity Subcommittee to produce an unclassified report and recommendations so that not only the Department but also the larger cybersecurity community can benefit from the Committee's advice. If my office may provide any assistance to you as the Committee undertakes this tasking, please don't hesitate to let me or Martha Landesberg know.

Best Regards,

Mary Ellen Callahan
Chief Privacy Officer
U.S. Department of Homeland Security

Appendix B:
Questions to Address in Evaluating the Effectiveness of Privacy Protections in Cybersecurity Pilots

The Committee believes that explicitly reviewing privacy as part of any evaluation will be critically important to enable sustained implementation of successful pilots. In light of the principles, policies, and processes discussed throughout this report, potential questions that such evaluations should assess include:

- What limits have been put in place to ensure that PII and the content of communications not relevant to the cybersecurity pilot are not collected or stored?
- When PII or the content of communications are collected, have they been obfuscated/anonymized to protect privacy where practicable, and was the supplier of that information advised that it contained PII and that it was obfuscated/anonymized?
- What protections will be put in place to limit how those with whom the data will be shared will use the data?
- How do protections for individuals continue as the process unfolds?
- What information will be used from other places to help analyze the data?
- How will the data and results be stored (e.g., where, for how long, with access by whom, with what security measures)?
- What logging capabilities are used to record access, sharing, and use of the data, and what mechanisms are in place to safeguard the integrity of the log?
- What audit controls will be used to determine compliance with policy?
- What risk assessment system will be used to periodically audit the system?
- What safeguards are in place to govern third party access to information from the pilot?
- How can individuals seek redress for how their information is used within the pilot?
- How can corrections to the supplied data be communicated to DHS?
- What is the oversight structure for reviewing the pilot?
- What is the likelihood that privacy protections of the pilot project will be overtaken by foreseeable changes in technology or law?
- If the pilot project is successful and a full-scale project is approved, would this represent a significant substantive change in privacy for the relevant data subjects?

Appendix C:
Members of the DPIAC Ad Hoc Cybersecurity Subcommittee

Dan Chenok, IBM Center for the Business of Government, Chair

Ramon Barquin, Barquin International
Steven M. Bellovin, Columbia University
Fred Cate, Indiana University
Sharon Bradford Franklin, The Constitution Project
Morton H. Halperin Open Society Foundations
David Hoffman, Intel Corporation
Lance Hoffman, George Washington University
Linda Koontz, Mitre Corporation
Joanne McNabb, California Department of Justice
Christopher T. Pierson, LSQ Holdings
Richard Purcell, Corporate Privacy Group

Note: Organizations are listed for identification purposes only; the views in this report represent subcommittee member perspectives.