



PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

SEMI-ANNUAL REPORT
APRIL 2014 – SEPTEMBER 2014

December 22, 2014

In accordance with Section 801 of the Implementing Recommendations of the 9/11 Commission Act, 42 U.S.C. § 2000ee, I am pleased to present the fourth Semi-Annual Report of the Privacy and Civil Liberties Oversight Board. This Semi-Annual Report is being provided to the President and the following Members of Congress:

The Honorable Barbara A. Mikulski
Chairwoman, U.S. Senate Committee on Appropriations

The Honorable Richard Shelby
Ranking Member, U.S. Senate Committee on Appropriations

The Honorable Thomas R. Carper
Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Tom Coburn
Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Dianne Feinstein
Chairman, U.S. Senate Select Committee on Intelligence

The Honorable Saxby Chambliss
Vice Chairman, U.S. Senate Select Committee on Intelligence

The Honorable Patrick J. Leahy
Chairman, U.S. Senate Committee on the Judiciary

The Honorable Charles Grassley
Ranking Member, U.S. Senate Committee on the Judiciary

The Honorable Hal Rogers
Chairman, U.S. House of Representatives Committee on Appropriations

The Honorable Nita M. Lowey
Ranking Member, U.S. House of Representatives Committee on Appropriations

The Honorable Michael McCaul
Chairman, U.S. House of Representatives Committee on Homeland Security

The Honorable Bennie G. Thompson
Ranking Member, U.S. House of Representatives Committee on Homeland Security

The Honorable Mike Rogers
Chairman, U.S. House of Representatives Permanent Select Committee on Intelligence

The Honorable C.A. “Dutch” Ruppertsberger
Ranking Member, U.S. House of Representatives Permanent Select Committee on Intelligence

The Honorable Bob Goodlatte
Chairman, U.S. House of Representatives Committee on the Judiciary

The Honorable John Conyers, Jr.
Ranking Member, U.S. House of Representatives Committee on the Judiciary

The Honorable Darrell E. Issa
Chairman, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Elijah Cummings
Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform

Inquiries relating to this Report may be directed to Sharon Bradford Franklin, Executive Director, at (202) 296-4129.

Sincerely,



David Medine
Chairman, on behalf of the Board

Privacy and Civil Liberties Oversight Board

David Medine, Chairman

Rachel Brand

Elisebeth Collins Cook

James Dempsey

Patricia Wald



PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD

SEMI-ANNUAL REPORT, APRIL 2014 – SEPTEMBER 2014

I.	INTRODUCTION.....	1
II.	BOARD AUTHORITIES.....	2
III.	MAJOR ACTIVITIES: APRIL 2014 – SEPTEMBER 2014.....	4
	A. Organization, Administration, and Budget.....	4
	B. Activity in Support of the Board’s Mission.....	8
	C. Outreach to the Public and Government Entities.....	11
IV.	FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS.....	13
	A. Findings, Conclusions, and Recommendations.....	13
	B. Each Proposal Reviewed by the Board That: (i) the Board Advised Against Implementation; and (ii) Notwithstanding This Advice, Actions Were Taken to Implement.....	13
	C. Requests for the Issuance of a Subpoena That Were Modified or Denied by the Attorney General.....	14
V.	NEXT STEPS.....	14
VI.	CONCLUSION.....	15
	ATTACHMENT A.....	17
	ATTACHMENT B.....	19

I. INTRODUCTION

The Privacy and Civil Liberties Oversight Board is an independent agency within the executive branch. Under its authorizing statute, the Board's mission is to review existing and proposed counterterrorism programs to ensure that they appropriately balance national security concerns with protecting privacy and civil liberties.¹ This semi-annual report covers the Board's activities between April and September of 2014 (the "Reporting Period").

During the Reporting Period, the Board completed an intensive study that had commenced a year before. Following the unauthorized disclosure of classified documents that began in June 2013, the Board was requested by members of Congress and the President to review the two programs that were the subject of the disclosures, as well as to examine the operations of the Foreign Intelligence Surveillance Court ("FISC" or "FISA court"). These were the programs through which the NSA collects telephone call records or metadata under Section 215 of the USA PATRIOT Act (the "Section 215 Program"), and through which the government collects the content of electronic communications, including phone calls and emails, under Section 702 of the Foreign Intelligence Surveillance Act (the "Section 702 Program").

The Board completed its review of the Section 215 program during the prior Reporting Period, and released its *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* on January 23, 2014. During the current Reporting Period, the Board completed its study of the Section 702 Program, and released its *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* on July 2, 2014.

During the course of the Board's review of these two programs, it held hearings open to the public; and it gathered information and views from key members of the Intelligence Community, the Department of Justice, the White House, congressional committee staff, privacy and civil liberties advocates, and academia. The Board's reports provided detailed descriptions of the two programs and corrected misimpressions about the nature of the programs. The Board's reports gave the public a better understanding of the legal and policy issues involved in the operation of these federal programs, and provided a clear foundation for public debate.

¹ Pub. L. No. 108-458, § 1061(c), *as amended by* Pub. L. No. 110-53, § 801(a). Section 1061 is codified at 42 U.S.C. § 2000ee (hereinafter, the "Enabling Statute"), citations to the Enabling Statute are to its codified version in the United States Code.

Also during the Reporting Period, the Board conducted activities related to recruiting and hiring for key staff positions, standing up operations, and developing policies to govern the Board's IT systems and internal operations. With regard to the Board's mission, in addition to completing the study of the Section 702 Program, it held a public meeting in July of 2014 and announced an eight-point agenda about a wide range of projects, which are described in more detail herein. The Board has been actively complying with its statutory mandates to provide oversight of existing programs and advise federal agencies on the modification of current programs and the development of new ones. Nonetheless as a new and small agency, the Board continues to face significant administrative and operational challenges.

II. BOARD AUTHORITIES

Congress established the Board to serve two essential purposes:

- 1) Conducting oversight by analyzing and reviewing actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties; and
- 2) Providing advice to ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism.²

To accomplish these two statutory purposes, Congress, under the heading of *advice and counsel*, charged the Board with reviewing proposed legislation, regulations, and policies related to efforts to protect the Nation from terrorism, and advising the President and the departments, agencies, and elements of the executive branch to ensure that privacy and civil liberties are appropriately considered in the development and implementation of such legislation, regulations, policies, and guidelines.³ Congress, under the heading of *oversight*, also charged the Board with continually reviewing the regulations, policies, and procedures, of the executive branch, as well as its other actions to protect the Nation from terrorism, to see that such actions (i) appropriately protect privacy and civil liberties; and (ii) are consistent with governing laws, regulations, and policies regarding privacy and civil liberties.⁴

² 42 U.S.C. § 2000ee(c).

³ *Id.*, § 2000ee(d)(1).

⁴ *Id.*, § 2000ee(d)(2).

Under its Enabling Statute, the Board must periodically submit, not less than semiannually, (a) a report describing its major activities during the preceding period; and (b) information on the Board's findings, conclusions, and recommendations in connection with its advice and oversight functions. The Board is also charged with periodically interacting with and serving as a resource to the Congress on issues within the Board's jurisdiction.

In addition to the authorities the Board was granted under its enabling legislation, the Board has been given responsibilities by the President. Executive Order (E.O.) 13636, *Improving Critical Infrastructure Cybersecurity*, dated February 12, 2013, provides that the Department of Homeland Security ("DHS") shall consult with the Board in producing a report that assesses, and recommends steps to mitigate, the privacy and civil liberties risks associated with the cybersecurity programs undertaken by federal agencies under the Order.⁵ Although the PCLOB was not consulted early enough to be able to play a significant role in the development of the first DHS report, released in April 2014, the Board did provide feedback to the DHS by letter of March 21, 2014.⁶ Board members and staff look forward to coordinating and consulting with DHS and the other participating agencies in connection with the second cybersecurity report that will be released in March 2015.

The President invited the Board to play a second consultative role when he issued a Presidential Policy Directive *On Signals Intelligence* ("PPD-28"), on January 17, 2014. PPD-28 provides that in connection with the Nation's signals intelligence activities, all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information. PPD-28 further provides that U.S. signals intelligence activities must include appropriate safeguards for the personal information of all individuals, regardless of their nationality or where they reside. Section 5 of PPD-28 then encouraged the PCLOB to provide the President with a report that assesses the implementation of any matters contained within the directive that fall within its mandate. The Board has indicated that it will provide the requested assessment.

⁵ Exec. Order No. 13636, *Improving Critical Infrastructure Cybersecurity* (2013).

⁶ See Letter to Karen Neuman, DHS Chief Privacy Officer, and Megan Mack, DHS Chief Civil Rights and Civil Liberties Officer, from David Medine, Chairman, Privacy and Civil Liberties Oversight Board (March 21, 2014) accessible at: <http://www.pclob.gov/Library/Letter-DHS-Cyber-3-21-2014.pdf>.

It is also worth noting that several bills have been proposed in Congress that would provide additional oversight roles for the Board, although it is unknown whether any of these bills will be enacted. For example, proposed cybersecurity legislation would give the Board responsibility to assess privacy and civil liberties issues raised by the information sharing facilitated by that legislation. The USA FREEDOM Act legislation that recently failed to proceed in the Senate but may be reintroduced in the next Congress, would require the Foreign Intelligence Surveillance Court (“FISC”) to consult with the Board when selecting special advocates to appear before that tribunal.

III. MAJOR ACTIVITIES: APRIL 2014 – SEPTEMBER 2014

During the Reporting Period, the Board continued to establish itself as an independent agency, and focused on three areas:

- Organizational composition, administration, and budget;
- Activities in support of the Board’s mission; and
- Outreach to members of the public and government entities.

A. ORGANIZATION, ADMINISTRATION, AND BUDGET

Organizational Composition

1. Workforce

The Board significantly increased its hiring during the Reporting Period with the goal of “right-sizing” the agency. The Board hired additional staff members with subject-matter expertise in law, technology, administration, security, and business management. While the Board’s recruitment efforts have somewhat eased the strain on fulfilling its basic statutory responsibilities, the Board still needs to continue to expand its workforce to support its ever-increasing workload. Hiring efforts during the Reporting Period included:

- Hiring three Attorney-Advisors and one Board Counselor. These positions were developed to assist the Board on various projects related to the agency’s mission (discussed in more detail below), as well as to enable the Board to comply with its obligations as a federal agency. As part of the Board’s oversight and advice roles, these staff members play a significant role in researching and analyzing counterterrorism programs and providing support to Board Members in assessing these programs. These staff members have also assisted the Board in complying with its obligations as a federal agency—serving as its FOIA officer, responding promptly to Freedom of Information Act (“FOIA”) requests; as its Records Management Officer, developing a records management program and protocols; as its Ethics Official; and as its Security Officer.

- Hiring two Technologist-Advisors. These positions were developed to provide advice to the Board on the underlying technological understanding of the programs the Board reviews as well as to serve the Board’s internal information technology needs. Intelligence programs, while posing challenging legal and policy issues, often are also technologically complex, making it critical to have full-time technologists on the Board’s staff. These individuals also serve as the Board’s Chief Information Officer (“CIO”) and Chief Information Security Officer (“CISO”), managing the Board’s IT systems, architecture, and infrastructure and ensuring compliance with federal law and regulations, as appropriate. During the short period of time the CIO and CISO have been with the agency they have worked to bring the Board’s information systems up to proper standards, and have provided the Board with expertise on several substantive high priority projects.
- Hiring a Chief Management Officer to manage the full spectrum of the Board’s business operations. This includes finance, budget development, human resources, space management, procurement of goods and services, service level agreements, infrastructure requirements, resource management, policy development, and advising the Board on these and related matters.
- Hiring a Chief Security Officer (“CSO”) whose dual role also includes Administrative Officer duties. This position was developed to plan and participate in the identification and resolution of complex or sensitive security related issues and concerns for PCLOB, and facilitate collaboration between the Board and the appropriate security entities, the Intelligence Community, Congress, and the White House. The CSO provides substantive guidance, support, and policy development pertaining to personnel, physical, and area security.
- During the Reporting Period, the Board also recruited key personnel to serve as the Board’s General Counsel and Public Affairs/Legislative Officer. Also during the Reporting Period, the Board recruited additional Attorney Advisors and Counselors.

2. Relocation of Board’s Offices

One of the more significant challenges the Board has been faced with during the Reporting Period is beginning the process of identifying and acquiring new office space within a Sensitive Compartmented Information Facility (“SCIF”) for its mandatory physical move in FY 2016. The Board is currently occupying a leased space through the General Services Administration (“GSA”) in northwest D.C., which is scheduled to be demolished in the latter part of 2016. The Board cannot perform its core statutory function without having a

dedicated SCIF in which to review, analyze, and report on classified information regarding counterterrorism programs; and perform its oversight and advisory roles. The programs overseen by the Board often involve highly classified information and require appropriate protective measures, storage, and custodianship of said information. Unfortunately, SCIF space is limited in the Washington metro area, SCIF build out is very costly, and the Board does not currently have an operating budget sufficient to address this resource requirement.

3. Information Technology and Telecommunications

During the Reporting Period the Board made significant progress in modifying and upgrading its unclassified IT networks. Among other steps, the Board, in June 2014, began managing its own unclassified IT systems and through GSA it awarded a contract for support services ensuring the proper operation, maintenance, and support of its network and website. After the Board assumed control over its own systems, it was determined that the configuration and structure of the agency's unclassified network needed to be upgraded in order to meet the standards and requirements set forth under the Federal Information Security Management Act ("FISMA") of 2002. The Board also identified and remediated potential information security gaps, and took the necessary steps to prepare for a migration (in October, after the Reporting Period) of the Board's unclassified email system from Microsoft's commercial "cloud" service to a protected government community "cloud" service. The assessment of the Board's unclassified network security posture involved extensive research, conducting diagnostic monitoring, securing mobile access solutions, and upgrading and improving the agency's public website.

4. Relationship With Other Federal Agencies for Board Operations

Although the Board is an independent agency, it has established numerous contracts, memoranda of agreement and other arrangements through which it obtains support from other federal agencies for its SCIF requirements, badging, security protocol, systems, etc. The Board spends a considerable amount of time negotiating support for its infrastructure and other unique requirements. As an example, the Board renewed its "fee-for-service" agreements with the GSA for the Board's financial services, payroll, acquisitions, legal services, leasing, and human resource services.

Administration

Implementation of New Policies and Procedures

As an independent federal agency, the Board must comply with a large number of statutes, regulations, executive orders and executive branch policies, many of which require that the

Board also develop its own implementing policies and procedures. To this end, during the Reporting Period the Board adopted several policies, including:

- a) A general policy establishing office procedures, covering on-board processing, leave, work schedule duty hours and telework, mandatory training, and performance plans;
- b) A Prepublication/Classification Review Policy, to protect against inadvertent disclosures of classified information in connection with writings by Board members and staff;
- c) Four new policies specific to information technology, including 1) a policy governing the rules of behavior by employees for the use of information systems, 2) a policy governing information systems access and termination, 3) a policy specific to the responsibilities of the Chief Information Officer and Chief Information Security Officer, and 4) a privileged access account policy.
- d) A Performance Evaluation Review Policy specific to the performance process, the performance rating scale, and employee requirements.

Budget

The Board has jurisdiction to review all existing and proposed federal counterterrorism programs, to ensure that they include adequate safeguards for privacy and civil liberties. Most of these programs are conducted by the 17 different agencies that comprise the Intelligence Community, whose cumulative budget for FY 2013 was \$49 billion. By contrast, the Board's FY 2013 budget was only \$0.9 million and its FY 2014 budget was appropriated at \$3.1 million. During the Reporting Period the Board focused on the following priorities:

- The Board's continued stand-up to ensure full operational capability, with a focus on sufficient staffing, strong information technology infrastructure, and preparing for its mandatory 2016 office move;
- Integration into the ongoing business of the federal government and its structure, particularly through acquisition of the right skills and number of personnel to ensure effective engagement, and by seeking early involvement in the executive branch policy-making process;
- Examining issues within the Board's mandate and providing advice and guidance to the federal government, through inquiry, investigation, analysis and drafting and releasing reports; and
- Ensuring transparency to the public through outreach, public hearings and meetings, and to include access to the Board through its public website.

The Board continues to make significant progress in modernizing its technological systems. It is imperative that the Board continue to keep pace with the technological developments and the technological capacity of those agencies over which it has oversight.

As noted above in the discussion of the Board's authorities, there are also new and emerging requirements for the Board that will have financial implications in the near term. These include E.O. 13636 on Cybersecurity and PPD-28 on Signals Intelligence Activities, as well as various proposed bills that would increase the Board's authorities and responsibilities.

B. ACTIVITY IN SUPPORT OF THE BOARD'S MISSION

The Section 702 Report

On July 2, 2014, the Board issued its *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (the "Section 702 report"). In the Section 702 report, the Board reviewed this surveillance program that targets the international telephone and Internet communications of non-United States Persons overseas. The Board provided a descriptive, legal, and policy analysis of this program. Notably, the report contains an unclassified narrative detailing the highly complex program's operations that spanned over sixty pages, including over one hundred previously classified facts for which the Board successfully sought and obtained declassification. The overall report, including the separate statements of Board members, encompassed over one-hundred-sixty pages.

The Section 702 report filled key gaps regarding the public's understanding of how the program operated, and it dispelled a number of misunderstandings that had resulted from press coverage. The Board found these programs to be within the statutory authority granted by Congress. The Board also found that the core of the Section 702 Program – acquiring the communications of specifically targeted foreign persons who are located outside the United States – fits within the "totality of the circumstances" standard for reasonableness under the Fourth Amendment of the Constitution, and that the program has been effective in combating terrorism as well as in collecting important foreign intelligence information. Nevertheless, the report highlighted certain areas of concern, in particular, the "incidental" collection of U.S. persons' communications, the use of "queries" to search among the collected data for the communications of specific U.S. persons, and the collection of so-called "about" communications. The Board's report addressed some of these concerns with ten recommendations designed to promote transparency and to ensure that the Section 702 program includes adequate and appropriate safeguards for privacy and civil

liberties. Chairman Medine and Board Member Wald issued a separate statement urging additional steps be taken to protect privacy and civil liberties in connection with queries of collected communications using U.S. person identifiers and minimization of communications by U.S. persons that lack foreign intelligence value. Board Members Brand and Cook issued a separate statement in which they suggested a different approach to queries of collected Section 702 information, which they believed matched the scope of the problem, while not unnecessarily impairing the government's ability to conduct counterterrorism and other national security-related investigations.

Other Board Initiatives

The completion of the Section 702 Report in July 2014 allowed the Board and its staff to focus on other initiatives. At the Board's public meeting on July 23, 2014, the Board identified eight issues for its short term agenda: PPD-28, Executive Order 12333, training, cybersecurity, defining privacy, suspicious activity reports, Section 803 reports, and efficacy. During the Reporting Period, efforts on these projects included:

1. The Board began a review of intelligence activities operated pursuant to E.O. 12333, which governs much of the foreign intelligence and counterintelligence activities of the United States. In connection with this review, the Board and its staff have begun to receive briefings on the different programs and activities conducted by the intelligence agencies pursuant to this executive order. In addition, the Board continued to encourage federal agencies to update their guidelines under E.O. 12333 (which address the collection, retention, and dissemination of U.S. persons' information in the context of intelligence-gathering). In the past, the Board has noted that several agencies and departments are operating under guidelines that have not comprehensively been updated, in some cases in almost three decades, despite significant changes in information use and technology.
2. Pursuant to Section 803 of the 9/11 Commission Act,⁷ eight federal agencies are required to produce semi-annual reports on the activities of their privacy and civil liberties officers. These reports, known as Section 803 reports, must be submitted to the Board, and must include, among other things, the number and nature of the complaints received by the agencies for alleged privacy or civil liberties violations and the dispositions of these complaints. Many agencies' Section 803 reports are not informative, containing some quantitative

⁷ 42 U.S.C. § 2000ee-1.

information but little narrative explanation or context. The Board has been working with these reporting agencies to help make their Section 803 reports more meaningful and informative.

3. As noted above, E.O. 13636 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 a privacy and civil liberties assessment report, making recommendations to “minimize or mitigate” the “privacy and civil liberties risks of the functions and programs” undertaken pursuant to the Order. The Board’s staff is now working with DHS to ensure that the Board can play a robust role consulting with the DHS and the other agencies reporting under this executive order as they prepare their reports for 2015.
4. The Board has begun to assess the actions taken by the intelligence community in response to PPD-28, the January 17, 2014 Presidential Policy Directive requiring changes to the Nation’s signals intelligence programs to better address and account for the privacy and civil liberties of non-U.S. persons located abroad.
5. The Board continues to collect privacy and civil liberties training materials from executive branch agencies with a counterterrorism mission and has begun to work with the Information Sharing and Access Interagency Policy Committee Training Working Group to identify best practices across the training materials. The Board’s activities are conducted with a view toward developing a set of best practices for training programs to include core concepts and training tactics.
6. The Board continues to develop a set of working principles to use when assessing the privacy impacts of the government’s anti-terrorist efforts. During the Reporting Period, the Board planned for a public meeting (ultimately held after the Reporting Period, in November, 2014), at which the Board heard the views of a variety of experts from government, academia, industry, and advocacy organizations on how to define privacy in the context of counterterrorism programs. The event was designed to help the Board identify principles and to help guide the Board’s review of programs going forward.
7. The Board began an effort to both assess and further develop the mechanisms utilized by the government to measure the efficacy of its counterterrorism programs. As captured in Recommendation 10 of the Section 702 Report, the Board is asking the government to develop a comprehensive methodology to measure the effectiveness of its counterterrorism programs, so policy makers and courts can effectively weigh the interests of the government in conducting a

particular activity with the intrusions on privacy and civil liberties that it may cause. To that end, the Board is working with intelligence agencies to review the metrics agencies currently use to evaluate the effectiveness of their intelligence collection and counterterrorism activities.

8. The Board continues to provide advice and oversight with respect to its statutory responsibilities to oversee information sharing within the various agencies and entities involved with the government's anti-terrorism efforts, including fusion centers. This is within the Board's statutory mandate to provide advice in connection with information sharing activities related to counterterrorism programs.
9. Finally, the Board continues to work with executive branch agencies, providing advice and counsel as these agencies develop new programs or seek to modify existing ones to better address privacy and civil liberties concerns. The Board's advice and counsel is particularly valuable due to the independence of the Board. Much of this work must be confidential to ensure the candor and openness of the exchange with the agencies that are developing and operating the programs. Providing such advice and counsel is a critical statutory requirement under the Board's enabling statute.

C. OUTREACH TO THE PUBLIC AND GOVERNMENT ENTITIES

As noted above, part of the Board's statutory mission is ensuring, to the extent possible, that its efforts and reports be transparent to the public. The Board fulfills its statutory mandate through extensive outreach, Board meetings and hearings open to the public, and by disseminating its findings to the public, as appropriate. The Board members frequently collaborate with and speak at events hosted by a variety of groups and organizations, including bar associations, business organizations, educational institutions, and other government agencies to foster a better understanding of its oversight role. The Board members have spoken at other government agencies and organizations, including: 1) the National Security Alliance Intelligence and National Security Summit of the Armed Forces Communications Electronics Association and the Intelligence and National Security Alliance; 2) the NSA Compliance Office; 3) the DHS Privacy Office; 4) the National Protection and Program Directorate; 5) the Intelligence Community Legal Conference; 6) a meeting of the Federal Communications Bar Association; 7) the Privacy Law Scholars Conference; 8) the Media Law Conference in Reston, VA; 9) the Privacy Law Salon: Policymaker Roundtable; 10) the ABA's Annual Meeting in Boston, MA; 11) the Federalist Society; 12) Constitution Day events at the Newseum, in Washington, D.C., and at the Law School of the University of North Carolina at Chapel Hill; 13) the annual meeting of the

Missouri Bar Association; and 14) the Stanford Journal of International Law Conference, *Governing Intelligence: Transnational Threats and the National Security State*.

During the Board's review of the Section 702 Program, the Board held extensive discussions with various federal agencies, including the FBI, the CIA, the NSA, the ODNI, the State Department, and the Department of Justice. These meetings focused on the government's collection, use, and dissemination practices under the program, including internal and external oversight measures. The Board members and staff also met with industry representatives, non-profit and advocacy groups, academics and private individuals. Finally, the Board solicited and received extensive written public comments on the Section 702 Program. Prior to the release of the 702 report the Board met and reviewed its recommendations with staff for the White House, the House Permanent Select Committee on Intelligence, the House Judiciary Committee, the Senate Select Committee on Intelligence, and the Senate Judiciary Committee. The Board's 702 report is available on the Board's website at <http://www.pclob.gov/library/702-Report.pdf>. The Notice of the July 2, 2014 meeting was published in the Federal Register and that notice is included as Attachment A of this Report. As noted above, the Board held a public hearing on July 2, 2014, formally adopting its Section 702 report and its conclusions and recommendations in a public setting.

After the issuance of its Section 702 Report, on July 23, 2014, the Board conducted an open meeting and solicited public comment regarding issues that should be on the Board's agenda for review. Notice of this meeting was published in the Federal Register and is included as Attachment B of this Report.

Finally, the Board members have accepted invitations to meet and speak with foreign ambassadors and ministers including (after appropriate consultation with the State Department) the German Ambassador to the U.S. (Peter Wittig) and the German Federal Minister of the Interior (Thomas de Maiziere) to discuss balancing national security with privacy. In addition, two Board members spoke at the Intelligence Security Forum organized by the Congressional Taskforce on Terrorism and Unconventional Warfare chaired by Congressman Pittenger, to educate representatives of European Union countries and others on U.S. surveillance policies, PCLOB's stand-up operations, and the Board's roles and responsibilities. In addition, the Board's Executive Director met with a Member of the Parliament of Germany. The Board members and staff also participated in a forum on PPD-28 and international law and surveillance sponsored by American Society of International Law, the Center for Democracy and Technology, and the Brennan Center for Justice.

IV. FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

The Board's Enabling Statute requires that the Board, in its semi-annual reports, provide information on the findings, conclusions, and recommendations of the Board resulting from its advice and oversight functions, as well as the minority views in this respect.⁸ The Enabling Statute also requires the Board to identify each proposal reviewed under subsection (d)(1) that—

- (i) the Board advised against implementation; and
- (ii) notwithstanding such advice, actions were taken to implement.⁹

Finally, the Enabling Statute requires the Board to identify for the preceding period, any requests submitted to the Attorney General for the issuance of subpoenas that were modified or denied.¹⁰

A. Findings, Conclusions, and Recommendations

During the Reporting Period, the bulk of the Board's attention was focused on fact finding and evaluation of privacy and civil liberties concerns related to the federal government's surveillance activities conducted pursuant to Section 702 of the FISA. As noted above, on July 2, 2014, the Board issued a public report on the Section 702 Program, which included findings, legal conclusions, and recommendations resulting from the Board's extensive review of the program. The Board made ten recommendations regarding the Section 702 program. Several Board members also expressed individual views, as noted above. The Board's Section 702 report, and all minority views thereto, are currently available at <http://www.pclob.gov/library/702-Report.pdf>.

B. Each Proposal Reviewed by the Board That: (i) the Board Advised Against Implementation: and (ii) Notwithstanding This Advice, Actions Were Taken to Implement

For the Reporting Period, the Board has no items to report under this section.

⁸ 42 U.S.C. § 2000ee(e)(2).

⁹ *Id.*, § 2000ee(e)(2)(D).

¹⁰ *Id.*, § 2000ee(e)(2)(E).

C. Requests for the Issuance of Subpoenas That Were Modified or Denied by the Attorney General

For the Reporting Period, the Board has no items to report under this section.

V. NEXT STEPS

The Board expects the following priorities to guide its focus and efforts for FY 2015:

Organization, Administration and Budget

- Continuing to integrate the Board into the ongoing business of the federal government and its structure;
- Enhancing and promoting public access and participation in the Board's activities;
- Working with the executive and legislative branch to ensure the Board's budgets for FY 2015 and FY 2016 are sufficient to support the Board's operations and upcoming move, and to acquire necessary staff;
- Identifying and securing new office space for a required physical move in late FY 2016 of the Board's infrastructure and staff to a new SCIF location;
- Continuing to recruit and hire staff with the required skill sets in order to balance workload requirements against available resources;
- Managing and maintaining the Board's IT infrastructure and solutions that will advance the Board's mission and improve the overall operating efficiency; and
- Ensuring the security of classified information and information systems through annual assessment of information security and related program policies, procedures, and monitoring practices.

Outreach

- Supporting federal agencies and privacy civil rights/civil liberties officers as they exercise oversight of counterterrorism programs within the United States Government;
- Continuing to reach out and establish lines of communication with public stakeholders, including holding additional public meetings;

- Continuing to post materials and information online for the benefit of federal agencies and to educate the general public and specialized audiences about privacy and civil liberties concerns related to government efforts to protect the nation against terrorism; and
- Developing a capability to respond to the media and general public regarding specific plans and projects pending before the Board, and execute public outreach programs that advance Board goals.

Activities in Support of the Board's Mission

- Reviewing counterterrorism activities conducted under E.O.12333;
- Reviewing cybersecurity issues as they relate to terrorism pursuant to E.O. 13636 on critical infrastructure cybersecurity;
- Conducting oversight of existing counterterrorism programs identified by the Board as priority areas, and issuing public reports as appropriate;
- In addition to carrying forward the Board's work on the eight issues identified by the Board for its short term agenda in July 2014—PPD-28, E.O. 12333, training, cybersecurity, defining privacy, suspicious activity reports, Section 803 reports, and efficacy—the Board will continue to identify additional programs and issues for review, and will create a system for prioritizing which issues to address. The process for identifying new programs and issues will include extensive outreach to agencies conducting counterterrorism programs, as well as efforts to seek input from congressional staff and public stakeholders such as industry groups and advocacy organizations. As staff identify issues and conduct background research, the Board will evaluate the various proposals and assess which ones to prioritize;
- Exercising the Board's advice function and consulting with agencies developing new counterterrorism programs, or modifying existing ones, to ensure that these programs include appropriate safeguards for privacy and civil liberties; and
- The Board expects to periodically interact with and serve as a resource to the Congress on issues within the Board's jurisdiction.

VI. CONCLUSION

During the Reporting Period, the Board completed its second oversight report on July 2, 2014, examining the federal government's surveillance program operated pursuant to Section 702 of the FISA. The Board also initiated several new projects, detailed in this report, and thus continued to fulfill the advice and oversight responsibilities that comprise its substantive mandate. With the additional staff that the Board has hired,

the Board has made significant progress in expanding its ability to provide oversight and advice to the executive branch, but the Board continues to face serious administrative and financial constraints. In particular, the Board is still significantly understaffed, and must be responsive to the immediate need to identify and secure SCIF office space for its mandatory FY 2016 physical move.

The Board appreciates all of the collaboration and collective efforts of other federal agencies, Congress, the executive branch, advocacy groups, industry representatives, and members of the public who have engaged with the Board during this Reporting Period. The Board will continue to strengthen these relationships in furtherance of its statutory mandate as it moves forward in its efforts to ensure that counterterrorism programs include adequate safeguards to protect privacy and civil liberties.

ATTACHMENT A
NOTICE OF JULY 2, 2014 MEETING
AS PUBLISHED IN THE FEDERAL REGISTER

customers regarding promotional marketing campaigns in which they have participated or would like to participate. Such information would include details about the business, whether the business would like to participate in a mailing, shipping or Postal-related program, and any ideas the business may have for programs that might best suit its needs.

The Postal Service is also amending categories of records in the system, business specific information, to reflect additional data elements that will be maintained in the Customer Registration application.

II. Rationale for Changes to USPS Privacy Act Systems of Records

System of Records 810.100, *www.usps.com* Registration, is being modified to account for the collection of additional information pertaining to the computers, devices, networks, and software that customers use to conduct transactions through *usps.com*. This information includes: (1) Device identification number (device ID), which is a unique or distinctive number associated with a smartphone or other digital device, (2) Media Access Control (MAC) address, a unique identifier assigned to network interfaces for communications and associated with the computer hardware that enables a device such as a smartphone or laptop to connect to a computer network, and, (3) user agent information, which contains information about the software acting on behalf of the customer when the customer connects and interacts with a Web site such as *usps.com*.

The organization routinely will analyze data collected from the customer, including the additional information specified above, thereby enhancing current fraud protection controls. When specific fraud is identified against a customer account, the organization will communicate the incident to the registrant and offer recommended steps to enhance the customer's protection.

Collecting information from businesses regarding promotional marketing campaigns would further a purpose already listed within this system of records—"To permit customer feedback in order to improve *usps.com* or USPS products and services." The Postal Service values its business customers, and welcomes any information they wish to share in connection with USPS promotional marketing campaigns. By associating this information with a business customer's account, the Postal Service will be better able to learn about and serve that customer. Additionally, such

information may aid the Postal Service in making improvements to *usps.com* as well as to Postal Service products and services.

This SOR is also being amended to include information on whether a USPS business customer is a mail owner, a mail service provider, a PC Postage user, and/or a PC postage vendor. Such information, which is currently collected and stored in other postal information systems (Program Registration and Postalone!) will now be maintained in the Customer Registration database and will enable businesses to participate in Package Service programs, to receive mail tracking data, to receive incentives on certain mail volumes, or to avail themselves of other postal features available to business customers.

III. Description of Changes to Systems of Records

The Postal Service is modifying one system of records listed below. Pursuant to 5 U.S.C. 552a(e)(11), interested persons are invited to submit written data, views, or arguments on this proposal. A report of the proposed modifications has been sent to Congress and to the Office of Management and Budget for their evaluations. The Postal Service does not expect this amended system of records to have any adverse effect on individual privacy rights. The affected systems are as follows:

USPS 810.100
SYSTEM NAME: *www.usps.com*
Registration

Accordingly, for the reasons stated, the Postal Service proposes changes in the existing system of records as follows:

USPS 810.100

SYSTEM NAME:
www.usps.com Registration

CATEGORIES OF RECORDS IN THE SYSTEM

* * * * *

[CHANGE TO READ]

3. *Business specific information:* Business type and location, business IDs, annual revenue, number of employees, industry, nonprofit rate status, mail owner, mail service provider, PC postage user, PC postage vendor, product usage information, annual and/or monthly shipping budget, payment method and information, planned use of product, age of Web site, and information submitted by, or collected from, business customers in connection with promotional marketing campaigns.

* * * * *

7. *Online user information:* Internet Protocol (IP) address, domain name,

operating system versions, browser version, date and time of connection, Media Access Control (MAC) address, device identifier, information about the software acting on behalf of the user (i.e., user agent), and geographic location.

* * * * *

Stanley F. Mires,
Attorney, Legal Policy & Legislative Advice.
[FR Doc. 2014-14404 Filed 6-19-14; 8:45 am]
BILLING CODE 7710-12-P

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

[Notice-PCLOB-2014-03; Docket No.2014-0001 Sequence No. 3]

Sunshine Act Meeting

TIME AND DATE: Wednesday, July 2, 2014 from 10:00 a.m.—11:00 a.m. (Eastern Standard Time). Confirm the date on *www.pclob.gov*.

PLACE: Will be announced on *www.pclob.gov*.

STATUS: This meeting will be open to the public.

MATTERS TO BE CONSIDERED: The Privacy and Civil Liberties Oversight Board will meet for the disposition of official business. At the meeting, the Board will be voting on the issuance of its report on the surveillance program operated pursuant to Section 702 of the Foreign Intelligence Surveillance Act. Additional information on the Board's review of this program, such as the prior public workshop and hearings, is available at *www.pclob.gov*.

Procedures for Public Observation

The meeting is open to the public. Pre-registration is not required. Individuals who plan to attend and require special assistance should contact Sharon Bradford Franklin, Executive Director, 202-331-1986, at least 72 hours prior to the meeting date.

CONTACT PERSON FOR MORE INFORMATION: Sharon Bradford Franklin, Executive Director, 202-331-1986.

Dated: June 17, 2014.

Peter Winn,
Acting General Counsel, Privacy and Civil Liberties Oversight Board.

[FR Doc. 2014-14603 Filed 6-18-14; 4:15 pm]

BILLING CODE 6820-B3-P

ATTACHMENT B

**NOTICE OF JULY 23, 2014 MEETING
AS PUBLISHED IN THE FEDERAL REGISTER**

[FR Doc. 2014-16091 Filed 7-8-14; 8:45 am]

BILLING CODE 7710-12-P

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

[Notice-PCLOB-2014-04 Docket No. 2014-0001; Sequence 4]

Sunshine Act Meetings

TIME AND DATE: Wednesday, July 23, 2014 from 1:00 p.m. through 3:00 p.m. (Eastern Standard Time).

PLACE: Will be announced on the PCLOB's Web site www.pclob.gov.

STATUS: This meeting will be open to the public.

MATTERS TO BE CONSIDERED: The Privacy and Civil Liberties Oversight Board will meet for the disposition of official business. The meeting is being held for three items of business. First, the Board will consider and vote on the release of its third semi-annual report to the President and Congress. Second, the Board will announce its short-term agenda. Third, the Board will receive the views of non-governmental organizations, the business community and the general public on its mid-term and long-term agenda.

Procedures for Public Observation

The meeting is open to the public. Pre-registration is not required. Individuals wishing to address the meeting orally must provide advance notice to Sharon Bradford Franklin, at info@pclob.gov no later than 5:00 p.m. Friday, July 18, 2014, Eastern Standard Time. The notice must include the individual's name, title, organization, and a concise summary of the subject matter to be presented. Oral presentations may not exceed ten (10) minutes. The time for individual presentations will be reduced proportionately, if necessary, to afford all participants who have submitted a timely request an opportunity to be heard. Participants wishing to submit a written statement for the record must submit a copy of such statement no later than 11:59 p.m. Friday, August 29, 2014, Eastern Standard Time. Such statement must be typewritten, double-spaced, and may not exceed ten (10) pages. The Board will prepare an agenda, which will be available at the hearing, that identifies speakers and the time allotted for each presentation. Individuals who plan to attend and require special assistance should contact Sharon Bradford Franklin, Executive Director, 202-331-1986, at least 72 hours prior to the meeting date.

ADDRESSES: Submit comments identified by Notice PCLOB 2014-04, Sunshine Act Meeting by any of the following methods:

- *Regulations.gov:* <http://www.regulations.gov>. Submit comments via the Federal eRulemaking portal by searching "PCLOB 2014-04". Select the link "Comment Now" that corresponds with "Notice PCLOB 2014-04, Sunshine Act Meeting". Follow the instructions provided on the screen. Please include your name, company name (if any), and "Notice PCLOB 2014-04, Sunshine Act Meeting", on your attached document.

- *Mail:* General Services Administration, Regulatory Secretariat Division (MVCB), 1800 F Street NW., Washington, DC 20405. ATTN: Ms. Flowers/Notice PCLOB 2014-04, Sunshine Act Meeting.

- *Instructions:* Please submit comments only and cite Notice PCLOB 2014-04, Sunshine Act Meeting, in all correspondence related to this collection. All comments received will be posted without change to <http://www.regulations.gov>, including any personal and/or business confidential information provided.

CONTACT PERSON FOR MORE INFORMATION: Sharon Bradford Franklin, Executive Director, 202-331-1986.

Dated: July 7, 2014.

Peter Winn,

Acting General Counsel, Privacy and Civil Liberties Oversight Board.

[FR Doc. 2014-16155 Filed 7-7-14; 4:15 pm]

BILLING CODE 3820-83-P

SECURITIES AND EXCHANGE COMMISSION

Proposed Collection; Comment Request

Upon Written Request, Copies Available From: U.S. Securities and Exchange Commission, Office of Investor Education and Advocacy, Washington, DC 20549-0213.

Extension:

Rule 15g-9; SEC File No. 270-325, OMB Control No. 3235-0385.

Notice is hereby given that pursuant to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*), the Securities and Exchange Commission ("Commission") is soliciting comment on the collection of information described below. The Commission plans to submit this existing collection of information to the Office of Management and Budget for extension and approval.

Section 15(c)(2) of the Securities Exchange Act of 1934 (15 U.S.C. 78a *et*

seq.) (the "Exchange Act") authorizes the Commission to promulgate rules that prescribe means reasonably designed to prevent fraudulent, deceptive, or manipulative practices in connection with over-the-counter ("OTC") securities transactions. Pursuant to this authority, the Commission in 1989 adopted Rule 15a-6, which was subsequently redesignated as Rule 15g-9, 17 CFR 240.15g-9 (the "Rule"). The Rule requires broker-dealers to produce a written suitability determination for, and to obtain a written customer agreement to, certain recommended transactions in penny stocks that are not registered on a national securities exchange, and whose issuers do not meet certain minimum financial standards. The Rule is intended to prevent the indiscriminate use by broker-dealers of fraudulent, high pressure telephone sales campaigns to sell penny stocks to unsophisticated customers.

The Commission staff estimates that there are approximately 221 broker-dealers subject to the Rule. The burden of the Rule on a respondent varies widely depending on the frequency with which new customers are solicited. On the average for all respondents, the staff has estimated that respondents process three new customers per week, or approximately 156 new customer suitability determinations per year. We also estimate that a broker-dealer would expend approximately one-half hour per new customer in obtaining, reviewing, and processing (including transmitting to the customer) the information required by Rule 15g-9, and each respondent would consequently spend 78 hours annually (156 customers × .5 hours) obtaining the information required in the rule. We determined, based on the estimate of 221 broker-dealer respondents, that the current annual burden of Rule 15g-9 is 17,238 hours (221 respondents × 78 hours).

Written comments are invited on: (a) Whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimates of the burden of the proposed collection of information; (c) ways to enhance the quality, utility, and clarity of the information on respondents; and (d) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or other forms of information technology. Consideration will be given to comments and suggestions submitted in