



**Privacy and Civil Liberties Oversight
Board (PCLOB)**

2100 K Street, NW, Suite 500

Washington, DC 20427

OCTOBER 2014 - MARCH 2015

SEMI-ANNUAL REPORT



DAVID MEDINE, CHAIRMAN

RACHEL BRAND, BOARD MEMBER

ELISEBETH COLLINS, BOARD MEMBER

JAMES DEMPSEY, BOARD MEMBER

PATRICIA WALD, BOARD MEMBER

THIS PAGE INTENTIONALLY LEFT BLANK.

REPORT DISTRIBUTION

In accordance with Section 801, Implementing Recommendations of the 9/11 Commission Act, 42 U.S.C. § 2000ee, I am pleased to present the fifth Semi-Annual Report of the Privacy and Civil Liberties Oversight Board (“Board”). This Semi-Annual Report demonstrates the depth and breadth of the Board’s work during the reporting period.

This Semi-Annual Report covers the period from October 1, 2014 to March 31, 2015, and is being provided to the President and the following Members of Congress:

The Honorable Thad Cochran
Chairman, U.S. Senate Committee on Appropriations

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

The Honorable Ron Johnson
Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

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

The Honorable Richard Burr
Chairman, U.S. Senate Select Committee on Intelligence

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

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

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

The Honorable Harold 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 Devin Nunes
Chairman, U.S. House of Representatives Permanent Select Committee on Intelligence

The Honorable Adam Schiff
Ranking Member, U.S. House of Representatives Permanent Select Committee on Intelligence

The Honorable Robert 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 Jason Chaffetz
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

The Board's Semi-Annual Reports
are prepared to outline progress made
during the reporting period, including
updates on the Board's operation as an
independent agency and descriptions of
the Board's work in support of its
mission, and provide information
required by rule or law. The Board's
Semi-Annual Reports are also available
online at www.pclob.gov. Copies of other

Board reports, additional news and
information are also available on the
Board's website.

Inquiries may be directed to the
Executive Director, Sharon Bradford
Franklin at:

Privacy and Civil Liberties Oversight
Board
Attention: Sharon Bradford Franklin
2100 K Street, NW, Suite 500
Washington, DC 20427

info@pclob.gov

(202) 331-1986.



David Medine
Chairman of the Board, on behalf of the
Board Members

TABLE OF CONTENTS

INTRODUCTION	1
BOARD AUTHORITIES.....	3
MAJOR ACTIVITIES: OCTOBER 1, 2014 Through MARCH 31, 2015	5
ORGANIZATION, ADMINISTRATION, AND BUDGET.....	5
ORGANIZATIONAL COMPOSITION.....	5
1. WORKFORCE.....	5
2. RELOCATION OF BOARD'S OFFICES	5
3. INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS	6
4. RELATIONSHIP WITH OTHER FEDERAL AGENCIES FOR BOARD OPERATIONS.	7
ADMINISTRATION	7
AGENCY OPERATIONS.....	7
BUDGET	8
OVERSIGHT AND ADVICE ACTIVITIES	8
PUBLIC AND FEDERAL AGENCY OUTREACH	12
FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS	13
NEXT STEPS	13
ORGANIZATION, ADMINISTRATION AND BUDGET.....	14
OUTREACH	14
OVERSIGHT AND ADVICE ACTIVITIES	15
CONCLUSION	15

INTRODUCTION

HIGHLIGHTS OF BOARD ACTIVITIES

The Privacy and Civil Liberties Oversight Board is an independent agency within the executive branch. The mission of the Board is to ensure that efforts by the executive branch to protect the nation from terrorism are appropriately balanced with the need to protect privacy and civil liberties. The Board carries out this mission by conducting oversight and providing advice regarding counterterrorism authorities and activities.¹ This Semi-Annual Report covers the Board's activities between October 2014 and March 2015 (the "Reporting Period").

During the Reporting Period, the Board continued examining issues, programs, and activities outlined in the agenda publicly announced by the Board in July 2014. These include Presidential Policy Directive 28 ("PPD-28"), training, cybersecurity, defining privacy, counterterrorism activities conducted under Executive Order 12333 ("E.O. 12333"), Suspicious Activity Reports, Efficacy, and Section 803 reports. The following summarizes some of the Board's efforts conducted during the Reporting Period. As the highlights below illustrate, the Board continues to conduct oversight of programs and activities as they relate to the Board's statutory

authorities. Each of these activities is described further below.

Cybersecurity – The President's Executive Order 13636 ("E.O. 13636") on Improving Critical Infrastructure Cybersecurity, issued in February 2013, calls upon the Department of Homeland Security ("DHS") to consult with the Board in assessing agency cybersecurity information sharing programs. During the Reporting Period the Board participated in its second annual consultation with DHS and other agencies reporting under the Order regarding privacy and civil liberties policies and practices.

Efficacy – The Board continued its assessment of methodologies utilized by the Intelligence Community to evaluate the efficacy of counterterrorism programs.

E.O. 12333 – The Board continued to examine counterterrorism activities conducted under E.O. 12333, which establishes the framework for the efforts of the Intelligence Community ("IC"), and the implications of these activities for privacy and civil liberties. The Board refined its plan for the activities it will examine in the coming year, and it adopted a project description outlining its plans shortly after the Reporting Period ended. In February 2015, the Board released information about the Attorney General-approved guidelines adopted

¹ Pub. L. No. 108-458, § 1061(c) (2004), as amended by Pub. L. No. 110-53, § 801(a) (2007). 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.

under E.O. 12333 for each element of the Intelligence Community.

PPD-28 – PPD-28 outlines principles for and limits on signals intelligence activities, including the protections to be provided to non-U.S. persons.² It contains a provision encouraging the Board to provide the President with a report assessing the implementation of this Directive on Signals Intelligence. During the Reporting Period, the Board continued to work with the Intelligence Community in assessing the privacy protections to be provided to non-U.S. persons.

Recommendations Assessment Report – In 2014, the Board released reports on the telephone records program conducted under Section 215 of the USA PATRIOT Act and the surveillance program conducted under Section 702 of the Foreign Intelligence Surveillance Act. Through these two reports, the Board made a total of twenty-two recommendations directed at the executive branch, Congress, and the Foreign Intelligence Surveillance Court. On January 29, 2015, the Board released an assessment of the implementation of these recommendations.

Section 803 Reports – The Board continued working with agency privacy and civil liberties officers to identify viable changes to their reporting under Section 803 of the 9/11 Commission Act designed to make those reports more

informative and accessible. Eight federal departments and agencies are required to submit “Section 803 reports” to Congress and the Board on a semi-annual basis covering the activities of privacy and civil liberties officers.

Training – The Board continued its work related to privacy and civil liberties trainings in the context of counterterrorism programs. The Board has completed its assessment of select training materials provided by intelligence community elements with a counterterrorism mission, and will continue to consider and assess privacy and civil liberties training in its oversight reviews.

Other Activities – Also during the Reporting Period, the Board conducted activities related to recruiting and hiring for key staff positions, standing up its operations, and developing policies to govern the Board’s IT systems and other internal operations. The Board has been complying with its statutory mandates to provide oversight of existing counterterrorism programs and advise federal agencies on the development, modification and implementation of current and emerging counterterrorism programs. Nonetheless, as a new and small agency, the Board continues to face administrative and operational challenges, which the Board will continue to address in FY 2016.

² The term “U.S. persons” includes United States citizens, United States permanent residents, and virtually all United States corporations.

BOARD AUTHORITIES

Congress established the Board to serve two essential purposes:

1) Conduct 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.³

Under the heading of *advice and counsel*, Congress 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 components 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.⁴ 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.⁵

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 endeavors to keep Congress updated on Board activities and work with Congress on issues within the Board's jurisdiction.

In addition, the Board has been given specific responsibilities by the President. E.O. 13636, *Improving Critical Infrastructure Cybersecurity*, dated February 12, 2013, provides that 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.⁶ Board Members and staff coordinated and consulted with DHS and other participating agencies in connection with the second cybersecurity report that was released in April 2015, which was a

³ 42 U.S.C. § 2000ee(c).

⁴ *Id.* § 2000ee(d)(1).

⁵ *Id.* § 2000ee(d)(2)

⁶ Exec. Order No. 13636, *Improving Critical Infrastructure Cybersecurity* (2013).

substantial improvement over the prior year.

The President invited the Board to play a second consultative role when he issued PPD-28, a Presidential Policy Directive on Signals Intelligence, 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 encourages the Board 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, and, as described below, has already begun engagement with the IC on this effort.

Shortly after the end of the Reporting Period, Congress passed the USA FREEDOM Act,⁷ which authorizes the Foreign Intelligence Surveillance Court to consider recommendations made by Members of the Board for individuals to serve as *amicus curiae* in certain cases.

⁷ Pub. L. No. 114-23, § 401 (2015).

MAJOR ACTIVITIES: OCTOBER 1, 2014 THROUGH MARCH 31, 2015

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

- Organizational composition, administration, and budget;
- Oversight and advice activities; and
- Outreach to members of the public, Congress, and federal agencies.

ORGANIZATION, ADMINISTRATION, AND BUDGET

ORGANIZATIONAL COMPOSITION

1. WORKFORCE

The Board continued its hiring efforts during the Reporting Period with the goal of “right-sizing” the agency. Hiring during this period included filling key roles. 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 workload. Hiring efforts during the Reporting Period included:

- Hiring a General Counsel. The Board hired a permanent General Counsel to serve as chief legal officer for the Board. Previously this role had been filled by individuals serving as Acting General Counsel or Legal Counsel.
- Hiring one Attorney-Advisor and three Counselors. These positions were developed and hired to assist the Board on various projects

related to the agency’s mission (discussed in more detail below), to enable the Board to comply with its obligations as a federal agency, and to ensure that individual Members of the Board are adequately staffed. 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.

2. RELOCATION OF BOARD’S OFFICES

One of the more significant challenges the Board has faced during the Reporting Period was continuing the process of procuring new office space for its mandatory physical move in FY 2016. The Board is currently occupying leased space through the General Services Administration (“GSA”) in Northwest D.C., which is scheduled for demolition in the latter part of 2016. The Board must ensure that its new offices meet requirements as a Sensitive Compartmented Information Facility (“SCIF”). The Board cannot perform its core statutory mission without having a dedicated SCIF in which to review, analyze, and report on classified counterterrorism programs, and perform its oversight and advisory roles. The programs overseen by the Board are often highly classified and require appropriate protective measures, storage, and custodianship of said information. Unfortunately, SCIF space is limited in the

Washington metro area. The Board is working with GSA to explore cost-effective options, but recognizes that any office build out that may be necessary to meet SCIF requirements would be very costly, and the Board does not currently have an operating budget sufficient to address this resource requirement. Since the Board is required to move, it seeks to locate office space that can accommodate security requirements as well as an unclassified space in which the Board can hold public meetings.⁸

If the Board is authorized and appropriated its FY 2016 budget request, it will have the resources necessary 1) to “right-size” its staff and operational budget in order to more effectively and efficiently address its statutory authorities; and 2) appropriately address all funding requirements in connection with procuring new office space that meets all SCIF requirements, and includes dedicated unclassified space to hold public meetings and forums on a more regular basis.

3. INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

During the Reporting Period, the Board made significant progress in modifying and upgrading its unclassified IT systems and networks. Among other steps, the Board accomplished the following:

- *Migration of Board Email to a government certified cloud service provider (October 2014)* – In late October, the IT team successfully migrated the Board’s unclassified

email system to a certified cloud service provider taking full advantage of cloud computing benefits and minimizing cost. Additionally, the IT team implemented additional security controls to maintain the surety of the Board’s data and information systems. This effort significantly improved the Board’s overall information security posture by reducing potential pathways for cyber-attack and enhancing the system’s audit capabilities over the IT system. The features of the new email system allow for better records management, increased protection of personally identifiable information (“PII”), and greater flexibility for the staff to work on unclassified matters remotely.

- *Migration of the Board’s Public Website (October 2014)* – During the Board’s email cloud migration, the IT team rebuilt and deployed the Board’s website to the FEDRAMP certified cloud environment. The cloud solution allowed a fast and seamless transition and enabled security features not available within the original architecture.
- *HTTPS by Default for Board Website (March 2015)* – In early March, the IT team deployed HTTPS encryption by default to the Board’s public website, PCLOB.gov. This effort instantiates OMB guidelines to encrypt traffic between the visitor’s browser and

⁸ 42 U.S.C. § 2000ee(f)(2).

the PLOCB web server which ensures visitors are securely receiving official PCLOB content.

- Deployment of the Board's "Bring Your Own Device" ("BYOD") Program (December 2014) – In early December, the Board approved a new BYOD policy and the IT team deployed a set of solutions to allow users to access Board unclassified information via Board member and staff personal devices. These solutions have improved the ability of Board Members and staff to engage in telework and stay connected on travel, without creating new security vulnerabilities. The application that the Board has adopted keeps Board-related communications completely separate from Member/staff personal communications on personal devices.
- Development of Comprehensive IT Program Plan (January 2015) – The CIO developed a comprehensive IT Program Plan in January to provide a general guide to IT costs and scenarios over the FY 2015-2021 timeframe. The program plan will be updated as informed decisions are made. The plan describes the number of users and type of support required, before detailing the individual system and license purchases required to support that architecture. The plan was updated in March 2015 to group costs according to the Office of Management and Budget ("OMB") Budget Object Categories.

4. RELATIONSHIP WITH OTHER FEDERAL AGENCIES FOR BOARD OPERATIONS.

Although the Board is an independent agency, it has established numerous interagency agreements, and other arrangements through which it obtains support from other federal agencies to meet needs such as facility security, personnel security, classified information systems support, finance and payroll service, human resources, and acquisitions. As an example, the Board renewed its "fee-for-service" agreements with GSA for the Board's acquisition, leasing, human resource services, payroll, and security services. The Board also renewed its fee-for-service agreement with the United States Department of Agriculture for financial services, which was previously with GSA; and with DHS for building security, guard services, and computer monitoring.

ADMINISTRATION

AGENCY OPERATIONS

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. The Board is committed to establishing policies and procedures that will guide Board Members and staff as they carry out the Board's mission. The Board is also committed to submitting required reports and improving agency infrastructure.

For example, during the Reporting Period, the Board developed and submitted two reports regarding the

Board's compliance with the Freedom of Information Act: the Board's first Freedom of Information Act Officer Report, which covered activities from March 17, 2014 through March 15, 2015 and its first Annual Freedom of Information Act Report, which covered activities from October 1, 2013 through September 30, 2014.

BUDGET

The Board has jurisdiction to review existing and proposed federal counterterrorism programs to ensure they include adequate safeguards for privacy and civil liberties. Many of these programs are conducted by the 17 different agencies that comprise the IC, whose cumulative budget request for FY 2014 was approximately \$52.2 billion. By contrast, the Board's FY 2014 appropriated budget was \$3.1 million, and its FY 2015 appropriated budget was \$7.5 million.

During the Reporting Period, the Board continued to ensure full operational capability, with a focus on sufficient staffing, strong information technology infrastructure, and preparing for its mandatory 2016 office move.

The Board is also making significant progress in modernizing its internal IT and business systems.

Furthermore, it remains essential that the Board also continue to keep abreast of the technological advances and capacity of those agencies over which it has oversight.

As noted in the discussion of the Board's authorities, there are current 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

OVERSIGHT AND ADVICE ACTIVITIES

During the Reporting Period, the Board focused on the following oversight and advice priorities:

- Examining oversight issues within the Board's counterterrorism jurisdiction, including the eight agenda items identified by the Board in July 2014 (PPD-28, training, cybersecurity, defining privacy, counterterrorism activities conducted under E.O. 12333, Suspicious Activity Reports, Efficacy, and Section 803 reports); and
- Providing advice and guidance to the executive branch to ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to counterterrorism; and

Specific examples of the Board's work have included:

Advice Function – The Board has had the opportunity to engage with several agencies and with White House staff in its advice capacity, providing feedback and in the development of policies.

Cybersecurity – The Board's principal work on cybersecurity has centered on its role under E.O. 13636. The Order directs DHS to consult with the Board in developing a report assessing

the privacy and civil liberties implications of cybersecurity information sharing and recommending ways to mitigate threats to privacy and civil liberties. This was the second year the Board operated under the Order, and this year, the Board was consulted early in the E.O. 13636 process. This was a substantial improvement over the prior year, enabling the Board to play a significant role in the second DHS report. Between mid-December and early January, the Board engaged with the various agencies that are implementing E.O. 13636 and provided feedback as they prepared their reports. Shortly after the close of the Reporting Period, DHS issued the final report under the Order.

Defining Privacy – The Board held a public meeting on November 12, 2014 with industry representatives, academics, technologists, government personnel, and members of the advocacy community on the topic: "Defining Privacy". The event consisted of four panels, each of which explored a different aspect of the topic. The Board was able to hear from a variety of experts, and the input from the speakers will assist and guide the Board in its ongoing work, as it evaluates a range of privacy issues associated with counterterrorism programs.

The event was open to members of the general public and was covered by C-SPAN. It thus served both to educate the Board and to inform the public. The transcript from the event is available on the Board's website.

Efficacy – During the Reporting Period, the Board continued to work with the Office of the Director of National Intelligence ("ODNI") to hold Board Member briefings on the manner in which the IC measures the value and

effectiveness of their counterterrorism activities, which included a briefing on the National Intelligence Priorities Framework. Additionally, Board staff worked with various components of the IC to discuss initiatives undertaken by the individual components to measure the value of their counterterrorism programs.

E.O. 12333 – The Board continued its review of counterterrorism activities conducted under E.O. 12333. In connection with this review, the Board and its staff received overview briefings from IC elements on their counterterrorism activities, including the privacy and civil liberties protections established under the framework of the Order. Board staff also reviewed and analyzed E.O. 12333 implementing procedures of Intelligence Community elements.

In addition, Board staff began work on a public report that explains how the legal framework of E.O. 12333 and its implementing procedures governs the collection, use, retention, and dissemination of information concerning U.S. persons.

Shortly after the reporting period ended, on April 8, 2015, the Board voted to adopt a project description that memorializes the Board's approach to its work in the coming year on this project. The Board explained its intent to select, conduct in-depth examinations of, and write reports on specific counterterrorism-related activities governed by E.O. 12333. The project description also explains that for these in-depth examinations the Board plans to focus on activities of the CIA and NSA, and to draw on these examinations, as appropriate, to inform the Board's public

report described above. Board staff met with staff for the congressional intelligence committees to update them on these efforts and explain the Board's work on this project.

In addition, in February 2015, the Board posted on its website a table outlining the status of the Attorney General-approved implementing procedures under E.O. 12333 regarding collection, retention, and dissemination of information concerning U.S. persons. The table lists the dates on which each agency or department's current guidelines were adopted and provides links to all of the guidelines that are not classified, providing greater transparency to the public.

The Board's efforts also included meeting with representatives of non-governmental organizations and other advocates, who shared with the Board their concerns about E.O. 12333 based upon information currently available to the public, as well as the questions they would like the Board to potentially address in its inquiry. Minutes from this meeting have been made public on the Board's website.

PPD-28 – As described above, PPD-28 was issued by the President in January 2014, outlining principles for and limits on signals intelligence activities. It includes a provision encouraging the Board to provide the President with a report assessing the implementation of this Directive.

In preparation for the one-year anniversary of the issuance of the Directive, IC elements worked to develop guidance on how each agency plans to implement its terms. This includes

providing protections to non-U.S. persons in the context of U.S. signals intelligence programs. As agencies worked to develop their policies, the Board engaged with them under its advice function. The Board provided input on draft policies, including efforts to create policies that would provide greater transparency to the public.

Recommendations Assessment Report – In 2014, the Board released detailed reports on two government surveillance programs: the telephone records program conducted under Section 215 of the USA PATRIOT Act, and the surveillance program conducted under Section 702 of the Foreign Intelligence Surveillance Act. In these two reports, the Board made a total of twenty-two recommendations directed at the executive branch, Congress, and the Foreign Intelligence Surveillance Court.

During the Reporting Period, the Board conducted an assessment regarding the implementation of the recommendations made in its Section 215 and Section 702 reports. The Board consulted with representatives from the Justice Department and IC agencies in conducting this review. On January 29, 2015, the Board released a public report discussing the status of each recommendation's implementation. The Board's 25-page public report is accompanied by a summary table, outlining the extent to which each recommendation had been implemented. The Board found that overall, the Administration had been responsive to the Board's input, but explained that many recommendations were still in the process of being acted upon and that certain recommendations had not been implemented.

Section 803 Reports – The Board has worked in coordination with the White House Office of Science and Technology Policy (“OSTP”) to make more informative and accessible the Section 803 reports, which are issued by privacy and civil liberties officers of designated departments and agencies. Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 requires that certain executive branch departments and agencies file semi-annual⁹ reports describing the activities of the agencies’ privacy and civil liberties officers. These reports must be submitted to the heads of each agency, designated committees in Congress, and the Board.

Board staff met with OSTP staff during the fall of 2014 to set goals for their collaboration, and later met with personnel from the eight departments and agencies required to file Section 803 reports: the Office of the Director of National Intelligence, the Central Intelligence Agency, and the Departments of Defense, Health and Human Services, Homeland Security, Justice, State, and Treasury. Board staff also participated in a meeting with NGOs as part of the Administration’s National Action Plan on open government, to solicit input on how Section 803 reports could be improved.

The Board’s staff subsequently analyzed the statutory requirements of Section 803 and surveyed existing reports to identify potential areas for improvement, with the goal of formulating recommendations to make the reports more informative and

accessible. During the next Reporting Period, the Board will draft detailed guidance that provides an interpretation of Section 803’s requirements and offers suggestions to improve the usefulness of the reports.

Suspicious Activity Reports – The Program Manager for the Information Sharing Environment (“PM-ISE”) released a suspicious activity report standard, the ISE-SAR Functional Standard version 1.5.5, in February 2015. The Board had provided comments to the PM-ISE prior to the current Reporting Period.

Since then, the Board has begun reviewing information regarding the Information Sharing Environment and the work of the PM-ISE office to identify additional opportunities for the Board to assess the information sharing practices of the executive branch related to counterterrorism.

Training – The Board continued its work related to privacy and civil liberties trainings in the context of counterterrorism programs. The Board has completed its assessment of the training materials provided by IC elements with a counterterrorism mission. Throughout this assessment process, Board staff participated in an interagency training-focused working group of the Privacy and Civil Liberties Subcommittee of the Information Sharing and Access Interagency Policy Committee. Board staff provided input to the working group on best practices in designing training content and delivery methods to

⁹ *Id.* § 2000ee-1(f). The statute originally required quarterly reports, but was amended in 2014 to make those reports semiannual.

safeguard privacy and civil liberties.

The Board will continue to participate in the working group's efforts related to privacy and civil liberties trainings. Beyond this participation, the Board will incorporate its assessment of training programs into its ongoing work regarding specific counterterrorism activities, rather than continuing this effort as a separate Board project.

PUBLIC, CONGRESSIONAL, AND FEDERAL AGENCY OUTREACH

As the Board executes its statutory mission, it continues to ensure, to the extent possible consistent with the protection of classified information, that its work and reports be transparent to the public. The Board fulfills its statutory mandate through extensive outreach and Board meetings, hearings, and events that are open to the public, and by disseminating its findings to the public, as appropriate. Board Members and staff frequently participate in events hosted by other government agencies and a variety of groups and organizations, including bar associations, business organizations,

educational institutions, and non-governmental organizations, to foster a better understanding of its mission and role.

Board Members and staff have also met periodically with Members of Congress and congressional staff. These meetings have covered issues ranging from the impact of the continuing resolution in the fall of 2015 on the Board's operations to the Board's work examining counterterrorism activities under E.O. 12333. The Board works closely with a variety of other government agencies including seeking their input as the Board develops its priorities, and to promote productive working relationships. The Board also conducts outreach and receives input from a variety of private sector stakeholders on their concerns. These engagements both within government and outside the government assist the Board in making informed decisions as it develops its agenda.

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.¹⁰ 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.¹¹

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.¹²

A. Findings, Conclusions, and Recommendations

During the Reporting Period, the Board released its Recommendations Assessment Report. As described above, in that report, the Board found that overall, the Administration had been responsive to the Board's input, although many recommendations were still in the process of being acted upon and that certain recommendations had not been implemented. The Board individually

assessed the status of each of the twenty-two recommendations made in the Board's Section 215 and Section 702 reports. There were no minority views for this report. The Board's complete report can be found on the Board's website at: https://www.pcllob.gov/library/Recommendations_Assessment-Report.pdf and a chart summarizing those findings is available at: https://www.pcllob.gov/library/Recommendations_Assessment-FactSheet.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.

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.

NEXT STEPS

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

¹⁰ *Id.* § 2000ee(e)(2).

¹¹ *Id.* § 2000ee(e)(2)(D).

¹² *Id.* § 2000ee(e)(2)(E).

ORGANIZATION, ADMINISTRATION AND BUDGET

- Developing the Board's 2016-2018 strategic plan;
- Continuing to develop, update, and apply internal policies and procedures governing the Board's operations;
- Continuing to integrate the Board into the ongoing business of the federal government as a full participant in interagency processes;
- Enhancing and promoting public access and participation in the Board's activities to the extent possible consistent with the protection of classified information;
- Working with the executive and legislative branch to ensure the Board's budgets for FY 2016 and FY 2017 are sufficient to support the Board's operations and to hire necessary staff to ensure operational success;
- Identifying and procuring new office space for a required physical move in late FY 2016 and ensuring that the new location meets SCIF requirements;
- Continuing to recruit and hire staff with the required skill sets in order to balance workload requirements against available resources;
- Managing and continuing to develop the Board's IT infrastructure and solutions that will advance the Board's mission and improve the overall operating efficiency;
- Ensuring the security of classified information and information systems through annual assessment of information security and related program policies, procedures, and monitoring practices; and
- Continuing to build, secure, and maintain the Board's information systems to ensure seamless support to the Board's mission while ensuring implementation of the Federal Information Security Management Act ("FISMA")¹³ mandates throughout the infrastructure relocation.

OUTREACH

- Supporting and providing guidance to federal agencies and, in particular, privacy civil rights/civil liberties officers to promote appropriate consideration of privacy and civil liberties in counterterrorism activities and authorities;
- Continuing to maintain lines of communication with non-governmental organizations and private sector stakeholders, including holding additional public meetings or forums;

¹³ Pub. L. No. 107-347 (2002).

- 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;
- Developing a capability to respond to the media and general public regarding specific plans and projects pending before the Board, and to execute public outreach programs that advance Board goals; and
- Engaging with Congress to discuss the Board's work examining the privacy and civil liberties implications of counterterrorism activities.

OVERSIGHT AND ADVICE ACTIVITIES

In July 2014, the Board identified eight issues as part of its short term agenda: PPD-28, E.O. 12333, training, cybersecurity, defining privacy, Suspicious Activity Reports, Section 803 reports, and Efficacy. As described above, the Board's initial phase of work on two of these issues – the review of training and the public forum on defining privacy – has been completed. Going forward, the Board's efforts on these two issues will continue, but will be incorporated into the Board's work on other ongoing projects.

Over the next Reporting Period, the Board will continue its work on the other six issues identified in July 2014 for its short term agenda. This will include continuing the Board's review of

counterterrorism activities conducted under E.O.12333 and consulting with DHS and other participating agencies pursuant to E.O. 13636 on critical infrastructure cybersecurity.

The Board will also continue to identify additional programs and issues for review, and will refine its system for prioritizing which issues to address. The process for identifying new programs and issues includes outreach to federal agencies, Congress, non-governmental organizations, and private sector stakeholders. As the Board's staff identify issues and conduct background research, the Board will evaluate the various proposals and assess which ones to prioritize. Thereafter, the Board will conduct oversight of the counterterrorism programs identified by the Board as priority areas, and issue reports as appropriate.

The Board, in exercising its advice function, will continue to consult with the appropriate agencies who are developing new counterterrorism programs, or modifying existing ones, to ensure that these programs include appropriate safeguards for privacy and civil liberties.

CONCLUSION

During the Reporting Period, the Board continued work on several projects, detailed in this report, as well as fulfilling its advice and oversight responsibilities under 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 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 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.



Privacy and Civil Liberties Oversight Board (PCLOB)