Privacy and Civil Liberties Oversight Board

Fiscal Year 2016 Budget Justification

This page is intentionally left blank.

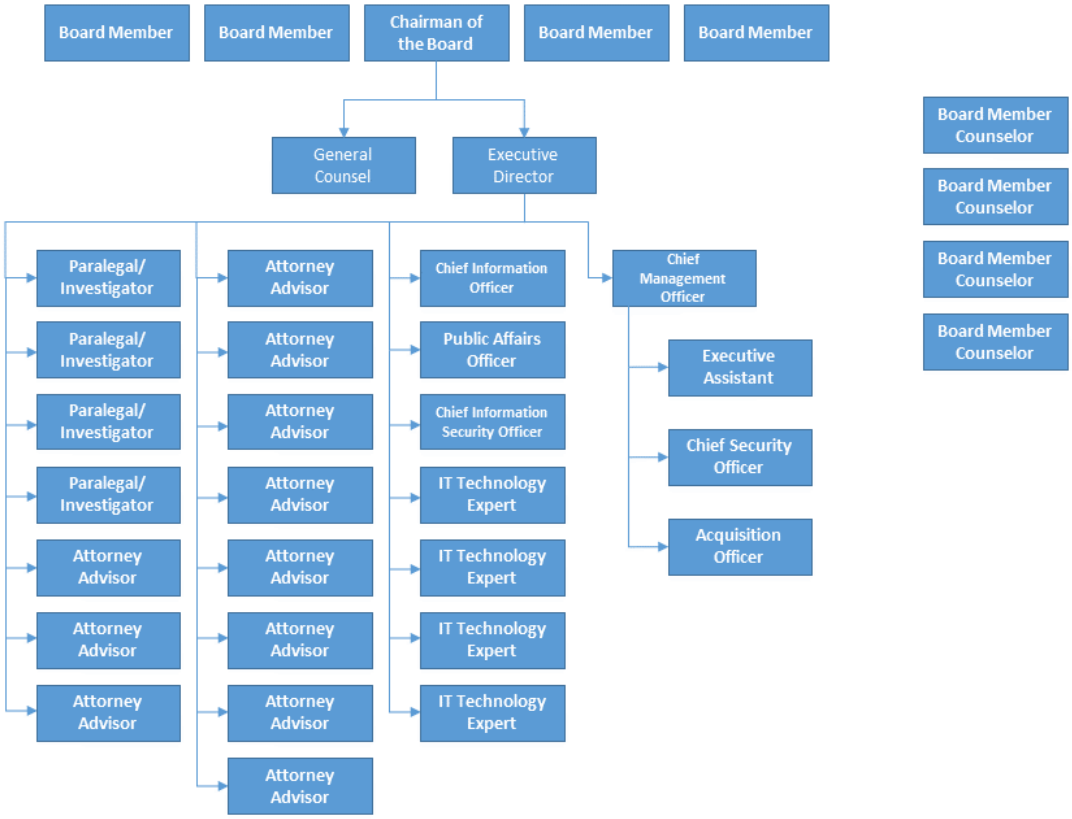
(UNCLASSIFIED)

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

FISCAL YEAR (FY) 2016 BUDGET JUSTIFICATION

TABLE OF CONTENTS

FY 2016 ORGANIZATIONAL CHART



Executive Summary

The Privacy and Civil Liberties Oversight Board (PCLOB) or "Board" requests $23,297 thousand and an increase of 12 positions for its fiscal year (FY) 2016 budget request. This request represents an increase of $15,797 thousand to the Board's FY 2015 budget. The change between FY 2015 and FY 2016 not only includes the increase of 12 positions, but is due primarily to a one-time increase of $13,216 thousand for the Board's required physical move in 2016. The funding requested for the 2016 move is a one-time expense required as the building housing the Board's current office is being torn down, and the Board must move to a new location where it can handle classified information and operate in a Sensitive Compartmented Information Facility (SCIF).

As an independent agency with a mandate to form its own independent views, the Board reviews both existing and proposed counterterrorism programs, making recommendations where appropriate, to ensure that those programs strike the right balance between protecting national security and respecting privacy and civil liberties.

In FY 2016, the Board plans to continue to expand its oversight role, as well as to further develop its role in providing advice to the Intelligence Community (IC) regarding the development of new counterterrorism (CT) initiatives, to ensure that privacy and civil liberties are appropriately considered at the outset as new programs are developed. This is the Board's second budget request since its inception in late 2012 and reflects the Board's continued efforts to reach a robust operational capability that will allow it to meet its statutory mission. The funding level requested, absent the one-time increase, is also consistent with the funding levels expressed in the legislation that created the Board in 2007.

The FY 2016 budget request will allow the Board to continue to hire staff and secure the supporting infrastructure necessary to carry out its mission on a sustained basis. The budget request is crucial to the Board's ability to perform its mission in FY 2016 as well as support the mandatory move of the agency in 2016 with the one-time increase. The budget request will assist in the completion of the Board's start-up activities and support its ongoing substantive operations.

The Board's FY 2016 budget requests the associated salaries and expense costs to support an effective staff

needed to maintain an efficient level of operations, enabling the Board to fulfill the role originally envisioned by the 9/11 Commission and Congress.

FISCAL YEAR 2014 ACCOMPLISHMENTS AND FISCAL YEAR 2016 CHALLENGES

In FY 2014, the Board made substantial progress in its efforts in achieving an effective operational capability as a fully independent agency within the Executive Branch. The Board is continuing to develop its understanding of critical government counterterrorism (CT) initiatives so that it can appropriately perform its oversight and advisory roles and promote public awareness and trust.

Of particular note was the January 2014 issuance of the Board's first substantive report, *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.* In a lengthy unclassified report, the Board provided a comprehensive description of the National Security Agency's (NSA) bulk telephone records program, its history, legal basis, its effectiveness in preventing terrorism, and its implications for privacy and civil liberties.

In addition to the Board's recommendations regarding operation of the Section 215 program, the report also contained an extensive discussion of the operations of the Foreign Intelligence Surveillance Court and included detailed recommendations for introducing a special advocate into that court, as well as a discussion and related recommendations geared toward increasing government transparency with respect to counterterrorism measures.

In preparing the report, the Board participated in numerous briefings with organizations involved in the operation of the program, reviewed a wealth of classified material, and conducted extensive legal and policy analysis. Consistent with its statutory mandate to operate publicly where possible, the Board held two public forums and solicited public comments.

The first was a day-long public workshop held in Washington, D.C., in July 2013, addressing different aspects of the government's surveillance programs operated under Section 215 of the Patriot Act and Section 702 of the Foreign Intelligence Surveillance Act (FISA). The second was a day-long public hearing in Washington, D.C., in November 2013, examining the value of these government programs, the operations of the Foreign Intelligence Surveillance Court, and potential reforms.

The Section 215 report was followed by the Board's issuance on July 2, 2014, of a report addressing the

surveillance program conducted under Section 702 of the FISA. Endeavoring once again to be transparent and accessible to a general audience, the Board provided an unclassified description of the highly complex Section 702 program, spanning over sixty pages and including over one hundred previously classified facts for which the Board successfully sought and obtained declassification.

The report fills key gaps in the public's knowledge about how the program operates, and it dispels misimpressions about the program that have circulated based upon press coverage. The report also discusses at length the legality and constitutionality of the program, its success in achieving counterterrorism and other foreign intelligence goals, and the privacy concerns that it raises. In particular, it examines 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 concluded 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.

To gather information for the report, the Board reviewed classified materials about the program and participated in numerous agency briefings. The Board also solicited public comments and held a day-long public hearing in March 2014, comprised of three panels that helped the board evaluate both legal and policy issues concerning operation of the program, and consider recommendations to ensure that U.S. government CT efforts properly balance the need to protect privacy and civil liberties.

Given its limited staff and resources, during fiscal year 2014 the Board primarily focused on the two reports described above. But during this period, the Board also initiated other efforts to promote privacy and civil liberties in the government's activities. As detailed in the Board's most recent semi-annual report, these efforts included:

- (1) Working with federal agencies to improve the quality of their "Section 803" reporting, which must detail the number and nature of the privacy and civil liberties complaints received by the agencies and a summary of the disposition of these complaints;
- (2) Prompting agencies to update their guidelines under Executive Order (E.O.) 12333 (which address the collection, retention, and dissemination of U.S. persons' information in the context of

intelligence-gathering), some of which have not comprehensively been updated in almost three decades, despite dramatic changes in information use and technology; and

- (3) Providing feedback on the Department of Homeland Security's report on the government's cybersecurity activities issued pursuant to E.O. 13636.

The Board's assessment includes a Fact Sheet, which provides a concise summary of the Board's conclusions about the implementation of its recommendations, and a table summarizing the Board's recommendations by subject matter.

The Board also engaged in informational sessions with federal agencies to better understand and discuss their CT programs and responsibilities. These sessions included:

- Meetings with the President, Vice President, their staffs, and other White House personnel about the Board's activities and recommendations;
- Meetings with staff for the House and Senate Judiciary Committees and staff for the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence;
- Briefings from the National Counterterrorism Center (NCTC) and the Department of Homeland Security (DHS) on the implementation of the 2012 *Guidelines for Access, Retention, Use and Dissemination by the National Counterterrorism Center and other Agencies of Information in Datasets Containing Non-Terrorism Information*;
- Programmatic updates from the Program Manager for the Information Sharing Environment (ISE). Consistent with the Board's statutory mandate, the Board provides advice and oversight on the implementation and administration of ISE programs including CT-related suspicious activity reporting;
- Meetings with industry representatives, members of privacy and civil liberties advocacy organizations, and open government advocates; and
- Introductory meeting with the President's Intelligence Advisory Board (PIAB) to identify areas of mutual interest and assistance.

The Board established and maintains a website and "*info@pclob.gov*" email as communication tools between the Board and the public to address

inquiries and facilitate exchanges of information about Board activities and documents produced.

Having completed its report on the Section 702 program, the Board will continue to have follow-up discussions on its priorities, including issues identified by the Board or suggested by the public, such as intelligence activities conducted under E.O. 12333, an assessment of operations under Presidential Policy Directive 28 (PPD-28), and the Nationwide Suspicious Activity Reporting Initiative.

More recently, on January 29, 2015, the Board marked the one-year anniversary of the Board's report on the Section 215 telephone records program and the six-month anniversary of its report on the Section 702 surveillance program by releasing an assessment of the implementation of its recommendations. In its two reports, the Board made a total of 22 recommendations directed at the Executive Branch, Congress, and the Foreign Intelligence Surveillance Court. In its assessment, the Board discusses the status of each recommendation's implementation.

Key findings include:

- Overall, the Administration has accepted virtually all recommendations in the Board's Section 702 report and has made substantial progress toward implementing many of them, while also accepting most of the recommendations in the Board's Section 215 report;

- The Administration has not implemented the Board's recommendation to halt the NSA's telephone records program, which it could do at any time without congressional involvement. Instead, the Administration has continued the program, with modifications, while seeking legislation to create a new system for government access to telephone records under Section 215;

- The Administration has made substantial progress in implementing some of the Board's recommendations regarding transparency; and

- The Administration has not yet developed, as the Board recommended, a methodology for gauging the value of its counterterrorism programs.

The Board continues to make significant progress in establishing itself as an independent bipartisan federal agency, but it continues to face significant challenges as it strives to reach full operational capability. As a new agency, the Board continues to work closely with the Office of Management and Budget (OMB) in the formulation of its plans and has established and maintained contact with its appropriations committees in Congress, as well as with the Intelligence and Judiciary Committees, and individual

members of Congress who have expressed interest in the Board.

PROPOSED FISCAL YEAR 2016 FOCUS AREAS

The Board expects the following four priorities to guide its activities for FY 2016:

- Continuation of standing-up the Board to ensure full operational capability, particularly the hiring of personnel for the purposes of "right-sizing" the organization so it may effectively and efficiently exercise its authorities and carrying out the agency's office move;
- Integration into the ongoing business of the federal government and its structure;
- Identification and examination of priority issues within the Board's mandate; and
- Provision of advice and guidance to the federal government and transparency to the public.

Many of the issues already identified by the Board for its "short term" agenda will continue as areas of examination beyond FY 2015 and well into FY 2016. In addition, the Board will continue to identify additional programs and issues to consider in the upcoming years. More specifically, the Board anticipates that during FY 2016 it will be focusing on these areas:

- Reviewing CT activities conducted under E.O. 12333;
- Reviewing cybersecurity issues as they relate to terrorism pursuant to the cybersecurity Executive Order;
- Reviewing additional CT programs to be identified by the Board and its expanded staff; and
- Support to federal partners and privacy civil rights/civil liberties officers as they exercise oversight of CT programs within the United States Government.

PROPOSED FISCAL YEAR 2016 MISSION FOCUS

- Coordinate and consult with federal and non-federal partners to identify and examine privacy and civil liberties issues of concern;
- Develop and implement an issue-and-process methodology for use by the Board as a framework for analyzing the development, implementation, and operation of executive branch policies and programs related to efforts to protect the nation against terrorism;

- Conduct oversight of existing CT programs identified by the Board as priority areas and issue public reports as appropriate;
- Exercise the Board's advice function and consult with agencies developing new CT programs to ensure that these programs include appropriate safeguards for privacy and civil liberties;
- Advise federal agency privacy, civil rights, and civil liberties officers as they exercise oversight of government efforts to protect the nation against terrorism;
- 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
- Develop 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, as needed.

PROPOSED FY 2016 MANAGEMENT FOCUS

- Keep key congressional committees apprised of the Board's progress, including committees on Appropriations, Judiciary, Intelligence, and Homeland Security, as appropriate;
- Identify new office space for a required move in late FY 2016. The Board is currently occupying a leased space through the General Services Administration (GSA) in northwest D.C. The lease agreement is set to expire in late 2016 due to the current owner's plans to tear down the building by the end of that calendar year. The 2016 move has already proven to be a challenge for the Board as there is no existing SCIF space in the downtown Washington, D.C., area where the Board would need to operate. Consequently, the Board is requesting a one-time increase of funds in its FY 2016 budget request to build out a secure facility as part of a new lease;
- Manage and maintain information technology infrastructure and solutions that advance the Board's mission and improve overall operating efficiency, and permanently move its IT infrastructure and staff to a new SCIF location;

- Enhance and promote greater public access and participation in the Board's activities through the use of internet technologies and services;
- Ensure the security of PCLOB information and information systems through annual assessment of information security and related program policies, procedures, and monitoring practices;
- Continue to recruit staff to the required level of strength and desired skills, establishing a workforce planning process that takes into consideration workload analysis, employee competency, and skill assessments; and
- Work with the GSA to continue to strengthen PCLOB financial management through the recurring review and refinement of internal controls and procurement processes.

MEMBERS OF THE BOARD

Chairman of the Board, David Medine, confirmed and sworn in during May 2013 for a term ending January 29, 2018;

Board Member, Rachel L. Brand, confirmed and sworn in during August 2012 for a term ending January 29, 2017;

Board Member, Elisebeth Collins Cook, reconfirmed and sworn in during May 2014 for a term ending January 29, 2020;

Board Member, James X. Dempsey, confirmed and sworn in during August 2012 for a term ending January 29, 2016; and

Board Member, Patricia M. Wald, reconfirmed and sworn in during December 2013 for a term ending January 29, 2019.

FUNCTIONS AND RESPONSIBILITIES

The Board is comprised of four part-time members and a full-time chairman. Board members are appointed by the President and confirmed by the Senate to serve staggered six-year terms.

The Board has two primary purposes:

(1) To analyze and review actions the executive branch takes to protect the United States from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties; and

(2) 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.

VISION, MISSION, AND VALUES

VISION

The Privacy and Civil Liberties Oversight Board is driven by the belief that it is possible and imperative to achieve the goal of countering terrorism while simultaneously protecting privacy and safeguarding liberties. The Board seeks, in the words of the 9/11 Commission, to "find ways of reconciling security with liberty, since the success of one helps protect the other." By providing advice to the executive branch, oversight of counterterrorism measures, and transparency to Congress and the public, the Board helps the nation to reconcile security with liberty and enhances public trust in the government's actions.

MISSION

The mission of the Board is to ensure that efforts by the executive branch to protect the nation from terrorism are balanced with the need to protect privacy and civil liberties. The Board carries out this mission in two primary ways:

(1) Conducting oversight of executive branch actions and policies relating to terrorism prevention, to ensure that privacy and civil liberties are protected and that these efforts are consistent with governing law, and

(2) Advising the President and the executive branch to ensure that privacy and civil liberties are appropriately considered in the development and implementation of legislation, regulations, and policies related to efforts to protect the nation from terrorism.

VALUES

The Board's work reflects a special commitment to three key values:

Rigor - The Board strives for the highest standard of quality in the analysis that supports its oversight and advice. When examining the operation, value, and privacy or civil liberties impact of efforts to prevent terrorism, the Board takes scrupulous care to understand those efforts in all of their manifold complexity.

In assessing whether such counterterrorism efforts are consistent with governing law, the Board devotes the most exacting scrutiny to the question. And when recommending changes to these efforts, the Board seeks to ensure that it has fully considered all foreseeable ramifications of those changes.

Integrity - As an independent, bipartisan agency whose power lies in the persuasiveness of its recommendations, the Board regards the preservation of its own institutional integrity as paramount. The Board thus approaches all of its activities with the honesty and good faith demanded by the difficult challenge it faces: properly balancing national security with the preservation of liberties. To this end, the Board especially strives to demonstrate that, in carrying out investigations and reaching its conclusions, it conducts itself in a manner beyond reproach and gives due weight to a wide range of viewpoints and considerations.

Transparency - By informing Congress and the public, to the greatest extent possible, about the executive branch's counterterrorism efforts and their impact on privacy and civil liberties, the Board promotes understanding about these efforts, helping to inform debate about their proper scope. In addition, by making its own operations as transparent as possible, the Board fosters confidence that it is approaching its mission with the thoroughness and care that this mission deserves.

HISTORY AND PURPOSE

The mission of the Privacy and Civil Liberties Oversight Board (PCLOB) is to ensure that efforts undertaken by our government to protect the United States from terrorism also respect and preserve the freedoms that define our nation.

The Board was created upon the recommendation of the 9/11 Commission, whose 2004 report declared that preventing terrorism does not require sacrificing the values that make us strong. Liberty and security, the Commission wrote, need not be in opposition but instead can be mutually reinforcing:

> We must find ways of reconciling security with liberty, since the success of one helps protect the other. The choice between security and liberty is a false choice, as nothing is more likely to endanger America's liberties than the success of a terrorist attack at home. Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend.[1]

Legal changes adopted after the September 11 attacks, the Commission noted, "vested substantial new powers" in the government's investigative agencies, prompting "concerns regarding the shifting balance of power to the government."[2] The Commission found, however, that "there is no office within the government whose job it is to look across the government at the actions we are taking to protect ourselves to ensure that liberty concerns are appropriately considered."[3]

To fill that gap, the 9/11 Commission unanimously recommended the creation of what is now the Privacy and Civil Liberties Oversight Board. In the words of the Commission: "At this time of increased and consolidated government authority, there should be a board within the executive branch to oversee adherence to the guidelines we recommend and the commitment the government makes to defend our civil liberties."[4]

In 2007, Congress responded to this proposal through the Implementing Recommendations of the 9/11 Commission Act, which established the Board as an independent agency within

---

1 THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, at 395 (2004).

2 *Id*. at 394.

3 *Id*. at 395.

4 *Id*. at 395.

the executive branch.[5] The agency is led by a bipartisan, five-member Board, comprised of a full-time chairman and four part-time Board members, all of whom are appointed by the President, with the advice and consent of the Senate, for staggered six-year terms. No more than three of the five Board members may be from the same political party, and the President must consult with the congressional leadership of the opposing party before appointing members who are not from the President's political party.[6]

Although the PCLOB was formally created as an independent agency in 2007, it did not come into existence until August 2012 when the Board's four part-time members were confirmed by the Senate, providing the Board with a quorum to begin activity. The Board did not have the ability to become fully functioning until 2013. The Board's chairman, who is vested by statute with the exclusive power to hire staff, was confirmed in May 2013, enabling the Board to become truly operational for the first time.[7]

Since then, the Board has been establishing itself as a functioning independent agency while simultaneously pursuing its statutory mission — most notably playing a lead role in confronting pressing questions about the scope of government surveillance carried out by the Intelligence Community.

The Board has two fundamental responsibilities under its authorizing statute:

(1) To analyze and review 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) 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.[8]

---

5 *See* Pub. L. No. 110-53, § 801(a), 121 Stat. 266, 352-58 (2007). Under the Act, the new PCLOB replaced an earlier agency with the same name that was situated within the Executive Office of the President. *See* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1061(b), 118 Stat. 3638, 3684 (2004).

6 *See* 42 U.S.C. § 2000ee(h)(2).

7 *See* 42 U.S.C. § 2000ee(j)(1). Before the chairman's Senate confirmation, the Board relied on a small number of detailees from other federal agencies to begin standing up the Board as a functioning agency. *See* 42 U.S.C. § 2000ee(j)(2).

8 *See* 42 U.S.C. § 2000ee(c).

These responsibilities encompass two distinct functions: providing oversight and providing advice.

In its oversight role, the Board is authorized to continually review the substance and implementation of executive branch regulations, policies, procedures, and information sharing practices relating to efforts to protect the nation from terrorism, in order to ensure that privacy and civil liberties are protected. The Board also is authorized to continually review any other actions of the executive branch relating to efforts to protect the nation from terrorism, in order to determine whether such actions appropriately protect privacy and civil liberties and whether they are consistent with governing laws, regulations, and policies regarding privacy and civil liberties.[9]

In its advice role, the Board is authorized to review proposed legislation, regulations, and policies related to efforts to protect the nation from terrorism (as well as the implementation of new and existing policies and legal authorities), in order to advise the President and the elements of the executive branch on ensuring that privacy and civil liberties are appropriately considered in the development and implementation of such legislation, regulations, and policies.[10]

When necessary to carry out its statutory duties, the Board is authorized to access all relevant executive agency records, documents, or other materials, including classified information, and to interview, take statements from, or take public testimony from any executive branch officer or employee. In addition, the Board may, by written request to the Attorney General if approved, require by subpoena that persons outside of the executive branch produce relevant information to the Board.[11]

In short, as a bipartisan oversight board that has access to classified information but is independent from the White House and the Intelligence Community, the PCLOB is uniquely positioned to ensure that Americans' civil liberties and privacy are not sacrificed in the government's efforts to prevent terrorism. By offering its independent but informed views and analyses, the Board assists the executive branch in formulating

9 *See* 42 U.S.C. § 2000ee(d)(2).

10 *See* 42 U.S.C. § 2000ee(d)(1).

11 *See* 42 U.S.C. § 2000ee(g)(1)(D).

policy regarding counterterrorism efforts, and it adds an important voice to broader discussions involving lawmakers and the public about striking the right balance between liberty and security in those efforts.

In furtherance of these goals, the Board is also authorized, when appropriate, to make recommendations to the privacy and civil liberties officers of certain agencies with counterterrorism functions, and to coordinate the activities of those officers on relevant interagency matters.[12]

In addition to these responsibilities, the Board has been directed by executive order to consult with the Department of Homeland Security as the Department assesses (and makes recommendations regarding) the privacy and civil liberties risks associated with cybersecurity activities undertaken by federal agencies pursuant to the executive order.[13]

To keep Congress and the President apprised of its activities, the Board is required to produce semiannual reports describing its major activities during the reporting period, as well as the Board's findings, conclusions, and recommendations resulting from its advice and oversight functions.[14]

To promote transparency, the Board is directed to make its reports available to the public to the greatest extent possible, and to hold public hearings and otherwise inform the public of its activities.[15] The Board is subject to the Freedom of Information Act, and it must conduct official business in accordance with the Government in the Sunshine Act, which requires that the public be provided notice of any meetings at which the Board deliberates to determine official action.[16] These requirements help ensure that the Board remains accessible to the public, as well as to Congress and the President, as it pursues its mission of safeguarding civil liberties and privacy in the nation's counterterrorism efforts.

---

12 *See* 42 U.S.C. § 2000ee(d)(3).

13 *See* Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity, § 5 (Feb. 12, 2013).

14 *See* 42 U.S.C. § 2000ee(e).

15 *See* 42 U.S.C. § 2000ee(f).

16 *See* 5 U.S.C. § 552(a)(2); 5 U.S.C. § 552b; 42 U.S.C. § 2000ee(l)(1).

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

FY 2016 BUDGET REQUEST SUMMARY

(Funding in Thousands)

	FY 2014 Enacted Budget	FY 2015 Enacted Budget	[1]FY 2016 Budget Request	FY 2015 FY 2016 (Delta)	[2]FY 2015 FY 2016 (Delta %)
Funding	$3,100	$7,500	23,297	$15,797	311%
Positions	17	25	37	12	148%
FTE	12	18	35	17	194%

Footnote: [1]The Board is requesting $10,081 thousand for its FY 2016 budget request and a one-time increase of $13,216 thousand for its required 2016 physical move. [2]The large delta percentage between FY 2015 and FY 2016 FTE wil decrease once adjusted for actual FTEs in FY 2015.

The Privacy and Civil Liberties Oversight Board's (PCLOB) budget request is $23,297 thousand for FY 2016. The Board requests $10,081 thousand to support mission-related activities exercised through the Board's authorities and planned growth; as well as a one-time increase of $13,216 thousand for the Board's physical relocation in 2016.

The Board recognizes the state of the current fiscally constrained environments, and has therefore, focused its resources on priority initiatives. The FY 2016 budget request outlines spending priorities for continued efforts on the stand up of the organization and other critical mission areas, including the mandatory 2016 physical move.

The budget and accompanying staffing plan demonstrate a continued focus on the following priorities:

- Board stand-up to ensure full operational capability, with a focus on sufficient staffing and a strong information technology infrastructure and carrying out the agency's 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;
- Identification and examination of issues within the Board's mandate through inquiry, investigation and public debate; and
- Providing advice and guidance to the federal government and ensuring transparency to the public through outreach, public hearings and meetings, to include access to the Board through its public website.

More specifically, the Board anticipates that during FY 2016 it will be focusing on issues related to Executive Order (E.O.) 12333; the Information Sharing Environment, cybersecurity issues as they relate to terrorism; and support to federal agency privacy and civil rights/civil liberties officers as they exercise oversight of terrorism related programs of the U.S. Government. In

addition, the Board will assessing further issues for its review in FY 2016, such as implementation of the 2012 Attorney General (AG) Guidelines for the National Counterterrorism Center (NCTC), and operation of the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) domestic intelligence activities as they relate to terrorism.

In order to build a baseline capability to support these important programs, the Board needs sufficient funding and personnel to address the priorities of personnel, facilities/IT support, de-commissioning of secure space, and the required 2016 physical move of the Board.

THE FY 2016 BUDGET WOULD ALLOW THE BOARD TO:

- Move from being a reactive, single-issue agency to one with sufficient staff to delve into a variety of issues simultaneously. The Board has begun this transition with the issues already identified for its short term agenda – such as cybersecurity, operations under E.O. 12333, and aspects of the Information Sharing Environment. As described below, the Board is working to identify additional issues to add to its longer term agenda, such as data handling at the National Counterterrorism Center (NCTC);

- Permit the Board to develop and exercise its advice function, serving as a key resource for other agencies developing new counterterrorism (CT) programs and seeking input on how to incorporate adequate safeguards for privacy and civil liberties;

- Enable the Board to increase its outreach to all agencies conducting counterterrorism programs as well as public stakeholders such as industry groups and advocacy organizations, to assist the Board in identifying new programs and issues for review;

- Allow the Board to conduct one or more open to the public hearings a year to promote transparency and public engagement, as well as further engage with the international community;

- Ensure that agency personnel have appropriate access to career-related training and development as employees in the federal government;

- As a non-Title 50 agency, to have the capability to address the various security and support requirements needed to operate within a Sensitive Compartmented Information Facility (SCIF);

- Simultaneously pay its current lease while addressing future SCIF space requirements for 2016; and

- Support its own IT capabilities required for an existing federal government agency infrastructure.

A REDUCTION IN FUNDS WOULD HAVE A NEGATIVE IMPACT ON THE FOLLOWING:

- The Board's ability to achieve a baseline capability and completion of successful stand-up of the agency;
- The Board's ability to conduct oversight of multiple programs simultaneously as well as to exercise its advice function;
- The Board's ability to address the need for a more stable and effective IT infrastructure;
- The Board's ability to attract and hire key talent required in executing the Board's authorities, resulting in a static mission; and
- The Board's ability to fund its pending 2016 physical move requirement.

FUNDING HIGHLIGHTS

INCREASES FOR FUNDING (THIS REPRESENTS AN INCREASE OF $15,797 THOUSAND FOR THE BOARD'S FY 2016 BUDGET REQUEST, WHICH INCLUDES $13,216 THOUSAND FOR A ONE-TIME INCREASE TO SUPPORT THE BOARD'S PHYSICAL MOVE IN 2016)

Program increases are requested for pertinent targeted investments, as outlined below.

- Maintaining current services;
- Continuing efforts in establishing an effective IT infrastructure;
- The Board's Relocation/2016 Move: Moving into permanent SCIF office space;
- Procuring information technology and telecommunications support;
- Maintaining required shared service agreements, to include finance, accounting, payroll, human resources, recruiting, the Federal Register, eRulemaking, transcription services, acquisition, and guard services;
- Rental payments that, for certain periods of time, would cover two spaces due to the Board's required physical move in 2016;
- Increased personnel services (Pay and Benefits) for positions necessary to effectively execute its mission and authorities;
- Decommissioning of current SCIF space and the accreditation of the Board's new SCIF space.

INCREASES FOR POSITIONS (THIS REPRESENTS AN INCREASE OF 12 POSITIONS):

- Building the Board's staff with experts in law, technology and intelligence[17];
- Advisory and assistance services from non-government experts (e.g., scholars in residence), especially on technological issues;
- Administrative and acquisition expertise for the purposes of managing agency contracts, interagency agreements, etc.;
- Paralegal/Investigative Analysts for the purposes of conducting required legal analysis for producing and disseminating investigative reports; and
- Counselors, each of whom works directly for one of the part-time Board members and also works on Board projects/tasks.

JUSTIFICATION FOR REQUIREMENTS

The Board has made significant progress over the past year in modernizing its technological systems, however, it is imperative the Board continue its efforts in order to keep pace with the technologies of those agencies over which it has oversight.

[17] This includes the need to increase the part-time Board members' days worked from 60 to 130 days, the maximum allowed by current law.

The Board's unclassified IT support contract provides two contractor full-time equivalents (FTE), to include management support. This support is essential for the Board's operations. Board staff members with technical expertise serve dual roles in managing the Board's own IT infrastructure and providing technical analysis in connection with the Board's investigation of counterterrorism programs.

Consequently, the Board has only devoted a combined one FTE to their roles of Chief Information Officer and Chief Information Security Officer.

E.O. 13556, Controlled Unclassified Information, the Federal Information Protection Standards (FIPS), and the Board's involvement in matters of national security combine to create a requirement that the Board maintain a higher standard of information security. The Board's oversight mission requires accessibility to all necessary classified information from U.S. Government agencies to review classified data. The Board also prepares classified and unclassified reports on programs, which requires access to the Joint Worldwide Intelligence Communications System (JWICS) and use of its connected workstations.

The outdated infrastructure at the Board 's current location creates an environment where it has to pay several hundred thousand dollars per fiscal year to ensure adequate support for its classified systems and cabling for all network connectivity. The Board is

currently occupying space in a building that is scheduled for demolition in late 2016. Consequently the Board will incur additional costs to include establishing an IT infrastructure and support related to a required move of the Board to another Sensitive Compartmented Information Facility (SCIF) location in 2016.

In order to meet the government requirements for network security and protection of sensitive information, the Board must procure a more robust set of services. OMB Memorandum M-08-05 directs all agencies to move their internet connectivity to a Trusted Internet Connection (TIC) that will provide sufficient scanning, firewalls, and proxy services to reduce the risk of network breaches or compromises. The Board is able to purchase Managed Trusted Internet Protocol Services through the Networx vehicle to obtain this level of protection at a reasonable price. The Networx vehicle will be utilized to acquire telephony services and mobile phone services.

In compliance with Homeland Security Presidential Directive (HSPD) 12, the Board has moved to two-factor authentication architecture for network access utilizing a Personal Identity Verification (PIV) card as the second factor. The Board will contract for the card management services from the General Services Administration (GSA) through the USAccess program vehicle.

The Board will continue to upgrade and modernize both network hardware and workstations to ensure devices are compatible and ensure its security tools and processes keep pace with a growing and increasingly complex infrastructure as it continues to develop and train analytical staff to monitor, respond to, and remediate risks.

In FY 2016, the Board will begin purchasing new desktop computers for one-third of users to begin a regular cycle of three-year refresh of technology. Upgrade and replacement of network devices will follow a similar schedule to space out replacement costs.

2016 RELOCATION/MOVE REQUEST

The Board's required physical move in 2016 will be significantly impacted if additional funds are not appropriated. The Board is currently occupying a SCIF in northwest Washington, D.C. which is scheduled for demolition in late 2016. The Board's requirements for a new space include:

- The building must meet the appropriate security requirements;
- The intended occupying space must be a SCIF, or be able to be remodeled to be accredited as a SCIF;
    - SCIF perimeters must include all walls that outline the SCIF confines, floors, ceilings, doors, windows and penetrations by ductwork, pipes, and conduit;

  - Noise must be controlled in the open space; and
  - The SCIF must be outfitted with classified and unclassified equipment at each workstation.
- Completed SCIF development and construction must be accredited by the appropriate authority;
- The space must offer 24/7 access to the Board's staff;
- The Board will require 24/7 guard and facility security, unless it receives a waiver from the appropriate authority;
- The Board must have access control and the appropriate Intrusion Detection Systems (IDS) alarming systems, closed circuit televisions (CCTV), and motion sensors;
- The Board staff must maintain access to the Joint Worldwide Intelligence Communications System (JWICS) for classified communications;
- Furniture, classified material, IT systems, and the Board (to include its staff) must be transported in a secure manner that will protect and safeguard throughout the relocation process;
- The Board's space must be outfitted with the appropriate IT connections; and
- The Board must cover decommissioning costs for its current classified space, and the associated costs with accrediting new SCIF space.

The one-time funding request for the Board's required physical move in 2016 is for approximately 13,000 square feet of "classified" or SCIF space, as well as 3,000 square feet of unclassified space to accommodate "open to the public" town halls, meetings, conferences, and/or symposiums. In doing so, the Board would yield a cost savings having its own unclassified space for interactions with the public, rather than having to expend large sums to a third party vendor when unclassified space is needed.

The classified space would accommodate approximately 50 FTEs, to include permanent staff, detailed personnel, experts, interns, and contract personnel. The Board seeks to acquire approximately 13,000 square feet of classified space, which would allow the Board room for growth, and ensure that it does not "outgrow" its new space in the near future.

The requirements for the 13,000 square feet of classified space follows:

- 6,925 square feet for individual work spaces and offices;

- 160 square feet for kiosks (for contractors and cleared interns);
- 250 square feet for a meeting/conference room that will accommodate 10 people and storage space;
- 1,000 square feet for a meeting/conference room that will accommodate 40 people and storage space;
- 27 square feet for lateral/safes files away from desks;
- 100 square feet copier, printer, HVAC control, and other storage;
- 90 square feet appropriately distributed within open work areas to minimize noise and foot traffic;
- 150 square feet for server room;
- 150 square feet for a break room/kitchenette;
- 150 square feet for the reception and access control point;
- 2,611 square feet for internal circulation (per the GSA calculations in there standard template); and
- 1,387 square feet for the rentable/usable factor (1.15 multiplier that converts usable areas to rentable area.)

OTHER REQUIREMENTS FOR INCREASED FUNDING

There are two specific duties that have been allocated to the Board not found in its authorizing statute. The first is under Executive Order (E.O.) 13636 on Improving Critical Infrastructure Cybersecurity, which calls on the Department of Homeland Security (DHS) to consult with the Board on its annual report. This report must assess the privacy and civil liberties risks of the functions and programs undertaken to address cybersecurity, and include recommendations regarding the ways to minimize or mitigate such risks.

The second, is found in Presidential Policy Directive (PPD) 28 on Signals Intelligence Activities, issued by President Obama on January 17, 2014. This directive encourages the Board to provide the President with a report that assesses the implementation of any matters contained within this directive that fall within the Board's mandate, which the Board has acknowledged and agreed to provide.

FY 2016 BUDGET EXHIBITS

RESOURCE EXHIBIT 1

(Funding in Thousands)

Budgetary Resources FY 2016	
FY 2014/2015 Carryover Funding	883
FY 2015 Enacted Budget	7,500
[1]FY 2016 Budget Request	23,297
$ Delta (FY 2015 Request over FY 2016 Request *(To Include the One-Time Increase*)	15,797
% Delta (FY 2015 Request over FY 2016 Request *(To Include the One-Time Increase)*	311%
Footnote: [1]The Board's FY 2016 request incldes a one-time increase of $13,216 thousand for ifor its required 2016 physical move.	

RESOURCE EXHIBIT 2

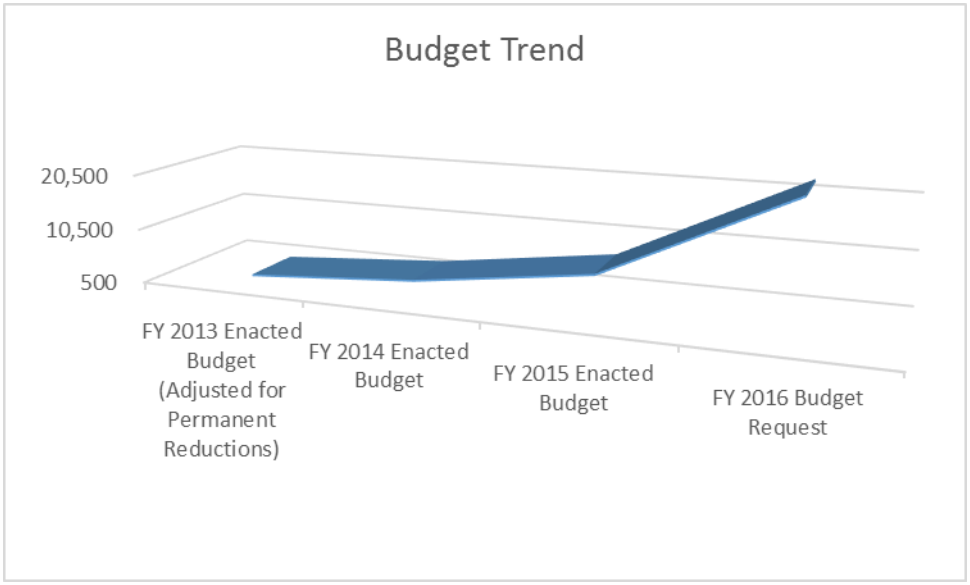
(Funding in Thousands)

Object Class	Total FY 2016 Budget Request
11.1	4,805
11.3	311
11.5	256
11.8	175
12.1	1,254
21	110
22	10
23.1	1,000
23.3	407
24	50
25.1	822
25.2	170
25.3	13,514
26	150
31	264
Total	**23,298**
Footnote: The object class breakout for Board's FY 2016 one-time increase of $13,216 for its required physical move follows: $12,946 thousand for Object Class (OC) 25.3, $20 thousand for OC 26, and $250 thousand for OC 31.	

SPENDING AUTHORITY – BUDGET TREND

RESOURCE EXHIBIT 3

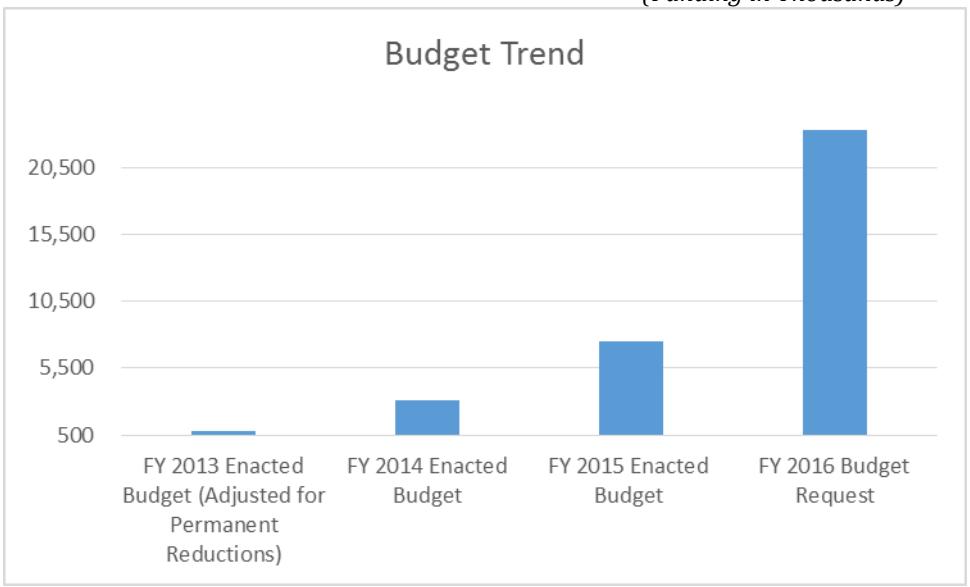
(Funding in Thousands)



Footnote: The Board's FY 2016 budget request includes a one-time increase of $13,216 thousand for its required 2016 physical move.

RESOURCE EXHIBIT 4

(Funding in Thousands)



Footnote: The Board's FY 2016 budget request includes a one-time increase of $13,216 thousand for its required 2016 physical move.

HILL INTERACTIONS

FY 2014 Congressional Meetings		
Date	**Meeting Participants**	**Purpose**
January 2014	Board members held briefing for staff of Senate Judiciary Committee, House Judiciary Committee, Senate Select Committee on Intelligence, House Permanent Select Committee on Intelligence and congressional leadership	To preview Board's findings and recommendations in 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
Feb-14	Chairman Medine testified before the House Judiciary Committee	Hearing: Recommendations to Reform Foreign Intelligence Programs.
Feb-14	All Board Members testify before the Senate Judiciary Committee	Hearing: The Report of the Privacy and Civil Liberties Oversight Board on Reforms to the Section 215 Telephone Records Program and the Foreign Intelligence Surveillance Court
Feb-14	Board Members and staff met with for staff for Senate Select Committee Intelligence	Operation of Section 702 program
Feb-14	Board Members and staff met with for staff for House Permanent Select Committee on Intelligence	Operation of Section 702 program
June 2014	Board Members and staff met with staff of Senate Judiciary Committee and House Judiciary Committee	The Board's potential recommendations for Section 702 program
June 2014	Board Members and staff met with staff of House Permanent Select Committee on Intelligence	The Board's potential recommendations for Section 702 program
June 2014	Board Members and staff met with staff of Senate Select Committee on Intelligence	The Board's potential recommendations for Section 702 program
September 2014	Chairman Medine and Board Member Brand spoke at the Intelligence Security Forum organized by Congressman Pittenger	To educate representatives of EU countries and others on U.S. surveillance policies

Footnote: This is a representative list of significant meetings and not a comprehensive list of all Hill interactions.

PUBLIC INTERACTIONS

FY 2014 P Public Meetings/Conferences		
Date	**Meeting Participants**	**Purpose**
October 2013	Board Members and staff met with representatives of privacy and civil liberties Non-Governmental Organizations (NGO)	The Board's study of Section 215 and 702 programs and the NGOs recommendations
November 2013	Board Public Hearing	The Board's study of Section 215 and 702 programs
January 2014	Board Public Meeting	The release of the Board's 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
February 2014	Chairman Medine and PCLOB staff met with members of the NGO Surveillance Coalition	The Board's study of the Section 702 program
February 2014	Chairman Medine and staff met with members of industry groups and NGO advocacy groups participating in the Data Privacy and Security Working Group	The Board's report on the Section 215 program and its study of the Section 702 program
February 2014	Board Members and staff met with representatives of groups representing Arab, Muslim and Sikh communities	Regarding the meeting representative's concerns with counterterrorism programs and recommendations for Board actions
February 2014	Board Members met with two technology companies	Regarding the Privacy & Civil Liberties Oversight Board's (PCLOB) role
March 2014	Board Members and staff met with epresentatives of privacy and civil liberties NGOs	The Board's study of Section 702 program and the NGOs recommendations
May 2014	Board Members and staff met with academics, government officials and advocates at forum organized by the American Society of International Law and the Center for Democracy and Technology	To discuss Presidential Policy Directive (PPD) 28
July 2014	Board Public Meeting	To release its Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act
July 2014	Board Public Meeting	To release its Semi-Annual Report and announce the Board's short term agenda
August 2014	Chairman Medine and staff met with representatives of open government NGOs	Regarding Board's Section 702 report and groups' recommendations for future Board work

Footnote: This is a representative list of significant meetings and not a comprehensive list of all interactions with members of the public.

PUBLIC INTERACTIONS - CONTINUED

FY 2014 Public Meetings/Conferences		
Date	**Meeting Participants**	**Purpose**
November 2014	Board Public Meeting	Board Public Meeting regarding the definition of "privacy" in the context of government counterterrorism programs, the conceptual interests involved in the protection of privacy, the impact of technology on privacy, and lessons from the private sector
December 2014	Board Members and staff met with representatives of privacy and civil liberties NGOs	The Board's study of activities conducted Under Executive Order 12333

Footnote: This is a representative list of significant meetings and not a comprehensive list of all interactions with members of the public.

STRATEGIC PLAN

The Privacy and Civil Liberties Oversight Board will develop a draft strategic plan in FY 2015 for fiscal years 2015 – 2018. The Board's strategic plan will outline the intended goals and strategies it will use in executing its oversight authorities and advice function, enabling the agency to ensure that counterterrorism programs include adequate safeguards to effectively protect privacy and civil liberties. In the absence of an official strategic plan, the Board has drafted the following to outline intended focus areas.

- The Board will develop a Continuity of Operations Plan (COOP) to ensure that the organization can respond to, and recover from, an emergency situation effectively. In addition, the Board is committed to effective and efficient management of information resources, and will develop a records management program. This transition will enable staff to perform their work more efficiently, maintain the Board's records, and protect sensitive information from inappropriate access.

- The Board will ensure it has an effective and secure information technology infrastructure, which will be essential to meeting the Board's strategic goals. The Chief Information Officer (CIO) will identify and provide critical high quality classified IT and low-risk unclassified IT services that are agile enough to meet the Board's business needs.

Additionally, the Board understands the importance of accountability and transparency, as shown through resource stewardship and oversight activities. This covers a wide range of administrative and operational efforts, such as formulating and executing the Board's budget, managing acquisition activities, spearheading audit resolution, and ensuring compliance with financial management laws and regulations.

This transparency is evident in the Board's work to improve access to organizational documents and findings, as appropriate to the public. Public documents and findings approved or authorized by the Board will be posted as "text-searchable" on the Board's website in conjunction with applicable news releases. As resource levels permit, the Board will also post public documents generated prior to the establishment of the Board's website in 2012.

The intended objectives for the Board's FY 2015 strategic plan will include:

- Establishing the agency as a recognized critical partner in the development of new counterterrorism programs, such that agencies routinely confer with the Board in the exercise of its advice function, to ensure that new programs include adequate safeguards for privacy and civil liberties;

- Establishing methods for identifying counterterrorism programs to be reviewed by the Board through its oversight function;

- Increasing and establishing regular methods for the Board's outreach to agencies conducting counterterrorism programs as well as to public stakeholders such as industry groups and advocacy organizations, to assist the Board in identifying new programs and issues for review;

- Ensuring efficiency of financial management operations, managed by the General Services Administration (GSA) for the Board. In doing so, this will strengthen the agency's internal controls, improve efficiency of the procurement process, and provide agency staff with timely information regarding budget execution and the availability of funds;

- Improvement of the Board's IT services by building redundancy into the IT infrastructure to support vital services, creating computing environments to consolidate the management and utilization of IT resources, and investing in new technologies to further support the Board's mission;

- Develop a records management program and develop a governance policy. The policy will cover file structures for organizing information, developing document naming conventions, setting access restrictions, establishing retention rules and triggers, maintaining agency records in secure electronic formats for the required retention periods and a requirement to transfer permanent agency records to the National Archives Records Administration (NARA);

- Continue partnership with the General Services Administration (GSA), the Office of Management and Budget (OMB), the Office of the Director of National Intelligence (ODNI), and other federal entities in executing the coordinated relocation of the Board to a new location in 2016;

- Promote and expand the use of the Electronic Document Management System to store work product and official records;

- Identify and implement process improvements through effective

use of technology to facilitate the Board's decision-making processes and its management of priorities;

- Promote the use of web-based e-filing of public comments in Board's rule-makings and other proceedings, which would continue to solicit public comments, to facilitate public participation and web posting of comments;

- Introduce new systems and applications that will enhance the Board's user experience and further provide tools to achieve strategic goals and meet government-wide IT mandates, including the Federal Information Security Management Act (FISMA);

- Initiate the Board's mobile device platform and remote access telework portal and begin developing a mobile computing platform, all of which will improve employees' ability to access the network required data;

- Deploy a Single-Sign-On solution to support the implementation of HSPD-12 and further protect Board data and systems from unauthorized access.

CONGRESSIONAL REPROGRAMMING

There were no congressional reprogrammings during FY 2014.

SPECIAL TOPICS

The Board has completed its extensive studies of the government's surveillance programs operated under Section 215 of the Patriot Act and Section 702 of the Foreign Intelligence Surveillance Act (FISA); has identified eight issues for its short term agenda; and has begun exploring these new issues. In FY 2015, in addition to carrying forward its work on these eight issues – PPD-28, Executive Order (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.

From its current short-term agenda, the PCLOB can identify certain issues where the work will clearly continue into FY 2016. First, the Board's work on E.O. 12333 will certainly continue well into FY 2016 and beyond. This executive order governs the operations of the entire intelligence community (IC) and its coverage is vast. While the Board has begun to investigate operations conducted under E.O. 12333, its efforts to "scope" its work will extend well into FY 2015, and the Board's review of programs conducted under this authority will continue throughout FY 2016.

Another aspect of the Board's work related to E.O. 12333 that will extend into FY 2016 is its effort to work with intelligence agencies to update their Attorney General (AG) guidelines for collecting data pursuant to E.O. 12333. As noted above, some agencies are operating under guidelines that have not been updated in decades. The PCLOB expects that the work to update all agency guidelines will continue well into FY 2016. Similarly, the Board's work on cybersecurity will continue throughout FY 2016 and beyond. Not only does the Board have an ongoing annual obligation under E.O. 13636 on Improving Critical Infrastructure Cybersecurity to work with DHS on its annual report.

In addition, the Board has already identified certain issues that it will be evaluating during FY 2015 for possible inclusion on the Board's future agenda. Possible issues for the Board's future agenda include:

- The operation of the National Counterterrorism Center (NCTC) and its 2012 guidelines

for collecting information;

- The rules for conducting domestic counterterrorism;
- the operation of fusion centers;
- The government's watchlisting system; and
- AG guidelines on the Federal Bureau of Investigation's (FBI) domestic activities.

Staff will be exploring these issues and the Board will determine which will become projects for FY 2015 and FY 2016. With the expanded outreach the Board will be conducting to agencies, Hill staff, and public stakeholders, the PCLOB will identify many additional issues to evaluate for inclusion as part of the Board's future oversight work.

The Board also plans to increase activities under its advice function during FY 2016. As explained above, one of the Board's statutory purposes is to provide advice to agencies that are developing new counterterrorism programs to ensure that the programs include appropriate safeguards for privacy and civil liberties. Since, by definition, these will be new programs being developed by other agencies, the Board cannot identify what these new programs will be in advance. However, the outreach that the PCLOB will be conducting throughout FY 2015, will help establish the communication channels to ensure that agencies solicit advice and input from the Board going forward.

Finally, the Board recognizes the likelihood that some programs or issues will be added to the Board's FY 2016 agenda based on future developments that simply cannot be predicted at this point. This could be based on new legislation to be enacted by Congress, requests by Congress or the White House, whistleblowers, or public revelations regarding counterterrorism programs.

FY 2016 PLANNED PROJECTS DISCUSSED

INTELLIGENCE ACTIVITIES UNDER EXECUTIVE ORDER (E.O.) 12333

The range of intelligence activities conducted pursuant to E.O. 12333 is immense, covering a varied assortment of efforts by numerous intelligence agencies and elements, each with their own missions and unique sets of methods, priorities, and guidelines. These activities are not overseen by the Foreign Intelligence Surveillance Court and traditionally have received less scrutiny beyond the executive branch than have comparable activities governed by statute. Examining the activities under E.O. 12333 that have a counterterrorism nexus, to assess their lawfulness and whether they appropriately safeguard privacy and civil liberties, is a formidable task that will involve a multi-year effort and a number of discrete investigations or studies.

CYBERSECURITY

Cyber threats to critical infrastructure represent a serious national security challenge. Enhancing the security and resilience of critical infrastructure while promoting privacy and civil liberties will involve a joint effort between the government and private sector. The Board is dedicated to promoting privacy and civil liberties at the intersection of cybersecurity and counterterrorism efforts. The Board will engage with the Department of Homeland Security, advocacy groups, and industry regarding cybersecurity information sharing issues and activities undertaken in accordance with E.O. 13636 that raise privacy and civil liberties concerns. Should legislation be enacted that provides a clear role for the Board that fits within its mandate, the Board will be prepared to execute its responsibilities accordingly.

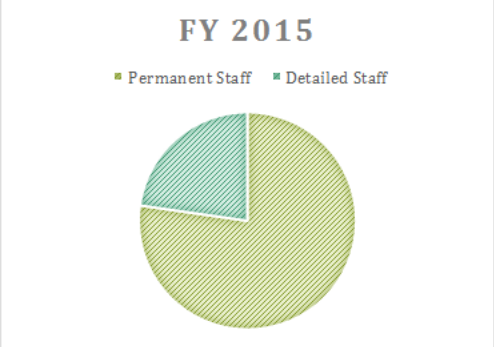
SUPPORTING AGENCY PRIVACY AND CIVIL LIBERTIES OFFICERS

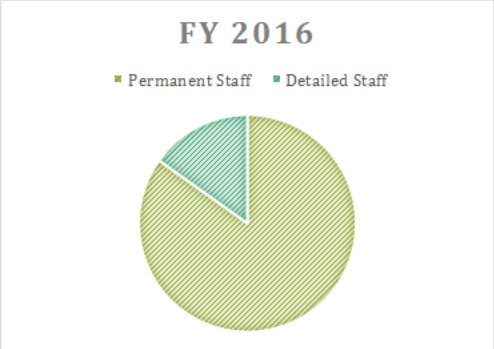
Many departments and agencies that contribute to the prevention of terrorism have their own privacy and civil liberties officers, whose roles have been established by statute, by the initiative of the department or agency, or by designation under Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007. These officers are best positioned to identify potential problems or areas for improvement within their own agencies where the protections for civil liberties and privacy could be enhanced. In the coming years, the PCLOB will work to support the efforts of these officers, give advice to them where appropriate, and develop partnerships with them that will facilitate a comprehensive initiative across the executive branch to safeguard privacy and civil liberties in the government's anti-terrorism efforts.

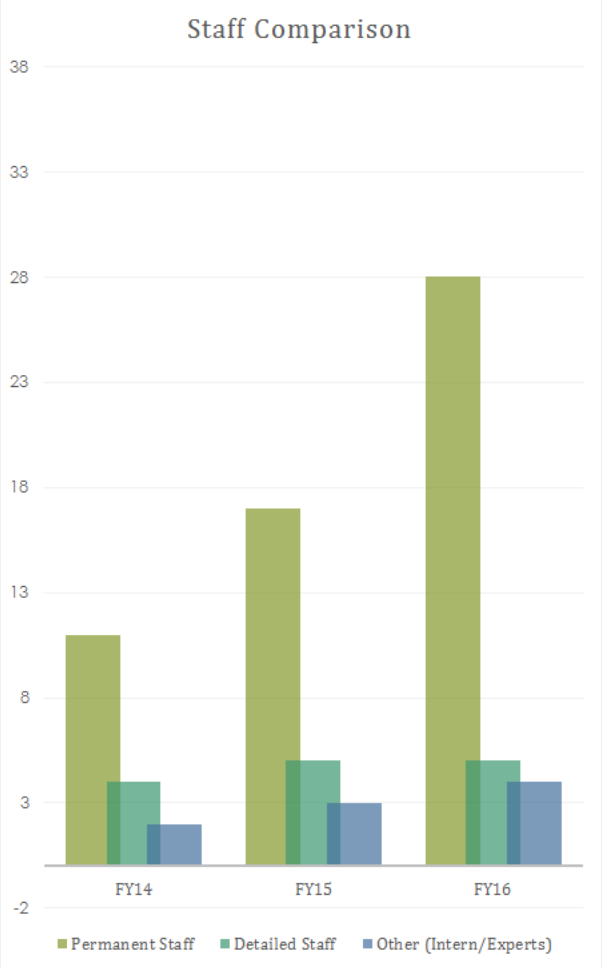
WORKFORCE COMPOSITION

Personnel Summary

	FY14	FY15	FY16
Permanent Staff	11	17	28
Detailed Staff	4	5	5
Other (Intern/Experts)	2	3	4







In fiscal year (FY) 2014, the Board made substantial progress in its efforts to achieve an effective operational capability as a fully independent agency within the executive branch. The Board continued efforts of increasing its workforce so that it can continue to appropriately perform its oversight and advisory roles and promote public awareness and trust.

The Board went from four full-time staff positions at the end of FY 2013 to 17 positions and 12 FTEs by the end of FY 2014. The Board will continue its recruiting efforts for the purposes of "right-sizing" the Board in order to

effectively address its mission requirements and execute its authorities.

The Board requests a total of 37 positions and 35 FTEs in FY 2016, an increase of 12 positions and 17 FTEs from FY 2015. The positions requested will allow the Board to:

- Continue to stand-up a full operational capability;
- Expand its reach and ability to oversee programs across the federal government;
- Identify and examine priority issues within the Board's mandate; and
- Provide advice and guidance to the federal government and transparency to the public.

STRATEGIES FOR ATTRACTING AND RETAINING TALENT

The Board developed a work-force plan to identify required skill sets and fulfill current and future human capital needs to carry out the Board's mission. The Board continues to progress and refine its processes to enhance its recruiting efforts, and retain a highly qualified and diverse workforce.

The Board strives to create an agency-wide performance culture that focuses on individual and organizational accountability toward achieving the Board's programmatic goals and priorities. The Board will seek to achieve this by providing quality training and staff development.

Brief descriptions of the Board's key personnel include:

BOARD MEMBERS

The Board members and Chairman of the Board are responsible for ensuring the effective and efficient execution of the Board's congressionally mandated responsibilities. The Board formulates policy that guides and directs the organization's work, and allocates required resources. The Board also monitors the agency's progress in accomplishing its stated goals and objectives.

GENERAL COUNSEL

The General Counsel (GC) was established as the Board's chief legal officer and adviser. The GC's major functions are representing the Board and providing legal counsel and policy advice to the Board to ensure compliance with all legal requirements for the Board's operation as an independent federal agency. The GC advises Board members and staff on such issues as ethics and Freedom of Information Act matters.

EXECUTIVE DIRECTOR

The Executive Director (ED) serves as the managerial and administrative arm of the Privacy and Civil Liberties Oversight Board, with responsibility for the overall operation of the agency. The

ED works closely with the Board on strategic planning and assessing the management and resource implications of any proposed action. The ED supervises and directs the work of agency staff in pursuit of the Board's mission, conducting its oversight and advice functions.

The ED also directs preparation of the Board's reports on counterterrorism programs, responses to formal congressional requests, briefings for congressional committees and subcommittees, drafting of testimony for congressional hearings, analysis of proposed legislation affecting the Board, and reviews Board comments to the President, the Office of Management and Budget (OMB), and Congress.

CHIEF MANAGEMENT OFFICER

The Chief Management Officer (CMO) is responsible for enabling the Board to accomplish its goals through workforce planning, recruitment, employee development, retention, compensation, and performance management. Activities include paralegal recruitment; attorney and non-attorney hiring; obtaining reimbursable and non-reimbursable detailed positions, contractors, interns, and scholars in residence.

The CMO provides advice and guidance on benefits, retirement, awards, training, position descriptions, labor relations, administration of performance management, and payroll. The CMO ensures that the Board complies with laws and regulations governing budget and human resources, and maintains a core staff of highly-trained professionals to aid the Board in carrying out its mandated responsibilities. The CMO assists the Board on budget development, justification, execution, and review. This includes working with OMB, and congressional staff to obtain appropriations and subsequent apportionment authority, distribute enacted and Board-approved resources to organizational projects, and track the use of agency resources.

CHIEF INFORMATION OFFICER

The Chief Information Officer (CIO) is responsible for providing the Board with a robust, reliable, rapidly scalable and interoperable infrastructure, providing connectivity and computing capabilities. The CIO also directly supports critical mission area IT development, modernization, the enhancement of applications and systems, and business services and related office automation systems.

The CIO's IT responsibilities align with and support two agency services: access to classified systems and services as well as the vital, secure, and stable technology infrastructure that forms the basis for specific Board transparency organizational activities. Some key activities performed by the CIO include:

- Procuring and ensuring the implementation of classified IT systems and services that are critical to the Board's oversight activities;

- Supporting the Board and staff through services provided by our Enterprise Services Desk, including PC installation and repair; training and support in the use of information technology resources;

- Providing a vital, secure, and stable technology infrastructure for a multitude of mission-supporting applications, systems, and services;

- Securing Board data and information technology systems against current and emerging cyber-security threats by using sophisticated network security technologies; and

- Ensuring that organizational applications, processes, and internal policies, procedures, and guidelines align with all federal mandates, legislation, and guidance.

CHIEF SECURITY OFFICER

The Chief Security Officer (CSO) performs tasks related to risk assessment, crisis management, personnel safety and facility security. The CSO is responsible for strengthening security initiatives; creating digital security management programs; prioritizing security initiatives and issues; and creating security policy and education awareness program for employees. The CSO manages the Board's "security" function, which includes physical security, facilities, and assets.

The CSO maintains productive working relationships with other security colleagues and the Intelligence Community (IC) to share information of interest, explain the specifics of security programs and procedures, and, when appropriate, present, justify, defend, negotiate and/or settle matters involving significant or controversial issues. The CSO provides guidance and support regarding personnel security to include initiating and/or crossing over clearances; ensuring physical security guidelines are in place for the Board and its staff, assignees, detailees, interns, and contract personnel.

PERFORMANCE MANAGEMENT

The Board believes that advancing organizational performance at all levels creates a strong foundation for overall organizational success. The Board's work and ongoing efforts to advance organizational performance enhances its ability to focus on protecting privacy and civil liberties.

Advancing organizational performance is inherently collaborative, and primarily encompasses key management areas of the Board: human capital, infrastructure and security, information technology resources, finance and acquisition, and equality of opportunity in employment. These efforts foster leadership and accountability across the Board and establish a culture of constituent responsiveness, and effective planning, administration, and management.

The Board's staff is expected to display leadership in their areas of expertise by exhibiting a willingness to develop and mentor others, a commitment to teamwork, and a drive to find innovative solutions.

In addition, the Board will perform targeted review of internal controls. The areas targeted for review will be determined by several factors, including risk assessment, management input, prior audits and reviews results and external (regulatory) environment. The Board will evaluate the results from internal control reviews to determine what processes should be modified to strengthen controls and/or improve efficiency.

With respect to the information technology and data security arena, the Board will be undergoing its first annual Federal Information Security Management Act (FISMA) review, and will act on any areas identified as needed improvement.

In the tables below, the Board has outlined its FY 2014 accomplishments and its FY 2015 anticipated accomplishments. Planned Board projects for FY 2016 are outlined under the "Special Topics" section of this request.

PERFORMANCE MANAGEMENT (FY 2014)

FY 2014 Accomplishments		
Item	**Description**	**Accomplishment**
Section 215 Report	January 2014 issuance of the Board's first substantive report, 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.	In a lengthy unclassified report, the Board provided a comprehensive description of the National Security Agency's (NSA) bulk telephone records program, its history, legal basis, its effectiveness in preventing terrorism, and its implications for privacy and civil liberties. In addition to the Board's recommendations regarding operation of the Section 215 program, the report also contained an extensive discussion of the operations of the Foreign Intelligence Surveillance Court and included detailed recommendations for introducing a special advocate into that court, as well as a discussion and related recommendations geared toward increasing government transparency with respect to counterterrorism measures.
Section 702 Report	July 2014 issuance of the Board's Report on the Surveillance Program Conducted under Section 702 of the Foreing Intelligence Surveillance Act	The Board provided an unclassified description of the highly complex Section 702 program, spanning over sixty pages and including over one hundred previously classified facts for which the Board successfully sought declassification. The report fills key gaps in the public's knowledge about how the program operates, and it dispels misimpressions about the program. The report also discusses at length the legality and constitutionality of the program, its success in achieving counterterrorism and other foreign intelligence goals, and the privacy concerns that it raises. The Board's report concluded 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.
Information Sharing Environment (ISE)	The Board provided input to the Program manager for the Information Sharing Environment (PM-ISE) on two major projects.	The Board reviewed an update to the Suspicious Activity Reporting Functional Standard, the standard that governs the entry of information into the Information Sharing Environment. As a result of its review, the Board submitted comments addressing the use of race as a cause for suspicion, as well as the use of First Amendment protected activity as a cause for suspicion. The Board also reviewed a proposed Framework for Information Sharing Access Agreements, which promotes privacy-centric development of ISAAs. The Board will submit comments related to the framework on October 1. The intended outcome for the feedback on both documents is for the PM-ISE to incorporate the Board's comments into its final guidance on both issues.

PERFORMANCE MANAGEMENT (FY 2014)

FY 2014 Accomplishments		
Item	**Description**	**Accomplishment**
Executive Order 13636, Improving Critical Infrastructure Cybersecurity	Executive Order 13636, Improving Critical Infrastructure Cybersecurity, provides that the Department of Homeland Security ("DHS") shall consult with the Board in producing a report that assesses the privacy and civil liberties risks associated with the activities undertaken by federal agencies under the Order.	Although the PCLOB was not consulted early enough to be able to play a significant role in the first DHS report, the Board provided feedback to the DHS by letter of March 21, 2014. The letter outlined areas of concern for the Board and made a series of recommendations for the work of DHS and other agencies conducting cybersecurity activities under the Executive Order. The intended outcome for this letter is for the agencies to address the Board's concerns and follow its recommendations as they develop their next annual cybersecurity report. In an effort to start the consultation process earlier this cycle, members of the PCLOB were briefed by DHS leadership regarding DHS's major cybersecurity initiatives on August 14, 2014. The staff maintains regular contact with the DHS' Office of Civil Rights and Civil Liberties as part of this endeavor. In addition, the PCLOB is currently tracking cybersecurity legislation that provides an oversight role for the Board. As part of this process, the Board responded to two legislative referral memoranda regarding the Senate's Cybersecurity Information Sharing Act of 2014.
E.O. 12333 Project	Updates to the various Intelligence Community agencies' Attorney General-approved guidelines, and beginning assessment of intelligence agency operations pursuant to E.O. 12333	The Board followed up on its FY 13 letter to the Attorney General and the Director of National Intelligence, urging updates to the various Intelligence Community agencies' Attorney General-approved guidelines, by meeting with representatives from the Department of Justice and the Office of the Director of National Intelligence to discuss the process for updating these guidelines. In addition, the Board began to scope the issues within Executive Order 12333 that it will focus its attention upon in the upcoming fiscal years. The Board received a joint overview briefing regarding Executive Order 12333 from several Intelligence Community agencies on September 24, 2014.

PERFORMANCE MANAGEMENT (FY 2015)

FY 2015 Anticipated Accomplishments		
Item	**Description**	**Anticipated Accomplishment**
Efficacy of Counterterrorism Programs	In Recommendation 10 of the Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (Report on Section 702), the Board stated that the government should develop a comprehensive methodology for assessing the efficacy and relative value of counterterrorism programs in order to assist policy makers in making informed, data-driven decisions about governmental activities that have the potential to impact the privacy and civil liberties of the public.	In FY 2015 - 2016, the Board will focus efforts on researching what metrics the Federal government currently compiles to assess the efficacy of its counterterrorism programs. Specifically, the Board will be looking to work with all major components of the intelligence and national security community, to determine what - if any - programs exist to assess the outcome and effectiveness of its intelligence collection programs and how those efforts, either individually or collectively, contribute to the government's broader counterterrorism mission. The Board will be looking to assess, and possibly advise agencies on the development and utilization of, methodologies that gauge and assign value to the government's counterterrorism activities. Further, the Board is looking to examine how agencies might use metrics to ensure counterterrorism programs are meeting their stated goals, and how those goals are balanced against the potential of those programs to invade the privacy and civil liberties of the public.
803 Reports	In partnership with the White House Office of Science and Technology Policy ("OSTP"), the PCLOB has initiated an interagency process to improve the consistency and usefulness of the so-called "Section 803 reports" issued by certain designated agencies. These semiannual reports, which are mandated by statute, require agencies to describe the activities of their civil liberties and privacy officers ("CLPOs") during the reporting period as well as the complaints received by those agencies for alleged violations of privacy and civil liberties. Some agencies' reports currently lack critical information as well as contextual explanations of the information they do provide. In an effort to improve the reports, PCLOB staff have undertaken a detailed examination of the existing reports and have analyzed the statutory requirements that govern them. Staff also have consulted with the CLPOs from a number of agencies and with OSTP, and have developed a technological model to consolidate the quantitative data in the reports for statistical and trend analysis.	The Board will continue to coordinate with agency CLPOs and with the OSTP on improving the usefulness of Section 803 reports over the next year. The Board anticipates that initial steps will involve collaborating with CLPOs to reach consensus on the statutory requirements for such reports, followed by development of a model structure for the reports, with the goal of enhancing both the narrative descriptions of CLPOs' activities and the accessibility of the quantitative data provided. The ultimate intent is to make the reports more helpful to Congress, the public, and the PCLOB in identifying the privacy and civil liberties challenges faced by the designated agencies and how their CLPOs are addressing those challenges.

PERFORMANCE MANAGEMENT (FY 2015)

FY 2015 Anticipated Accomplishments		
Item	**Description**	**Anticipated Accomplishment**
Information Sharing	The Board has provided input to the Program Manager for the Information Sharing Environment (PM-ISE) on two major projects. The Board reviewed an update to the Suspicious Activity Reporting Functional Standard, the standard that governs the entry of information into the Information Sharing Environment as well as a proposed Framework for Information Sharing Access Agreements.	The Board plans to continue to evaluate work of the Information Sharing Environment, and to conduct oversight of the ISE's work as required under the PCLOB's enabling statute.
PPD-28	As described above, Presidential Policy Directive (PPD) 28 on Signals Intelligence Activities encourages the Board to provide the President with a report that assesses the implementation of any matters contained within this directive that fall within the Board's mandate. The Board has agreed to provide such input.	The Board will work with intelligence agencies to evaluate the policies being developed under PPD-28. The Board will assess the appropriate protections to be provided to non-U.S. persons, and will make recommendations to ensure that privacy and civil liberties are adequately protected. Pursuant to the instructions to the PCLOB in PPD-28, the planned outcome of this project is to provide review and assessment of the actions the intelligence community takes in response to the new directive.
Executive Order 13636, Improving Critical Infrastructure Cybersecurity	Executive Order 13636, Improving Critical Infrastructure Cybersecurity, provides that the Department of Homeland Security ("DHS") shall consult with the Board in producing a report that assesses the privacy and civil liberties risks associated with the activities undertaken by federal agencies under the Order.	The Board will coordinate and consult with the DHS in connection with its second cybersecurity report over the coming year. While cybersecurity is a vast field, the Board's work on cybersecurity will focus on the intersection of cybersecurity, counterterrorism, and privacy and civil liberties. Therefore, the staff anticipates increased interactions with the DHS, advocacy groups, and industry regarding cybersecurity information sharing issues that raise privacy and civil liberties concerns. Lastly, the PCLOB will continue to monitor cybersecurity bills that propose a role for the Board. And, should legislation be enacted that provides a role for PCLOB, the Board will be prepared to execute its responsibilities accordingly.
E.O. 12333 Project	This work includes two components: (1) updates to the various Intelligence Community agencies' Attorney General-approved guidelines; and (2) assessment of programs and activities undertaken pursuant to E.O. 12333.	The Board will continue to encourage the updating of the Attorney General-approved guidelines and offer its advice on how those guidelines should be updated. In addition, the PCLOB will be briefed by the various Intelligence Community agencies regarding the activities that each agency conducts pursuant to Executive Order 12333. During FY 15 and FY 16, the Board will produce reports designed to provide the public with a better understanding of Executive Order 12333 and address the privacy and civil liberties issues that arise from actions taken pursuant to the Executive Order.
Defining Privacy	The Board held a one day public event in November 2014, hosting a set of panels that examined different views of privacy, how it can be affected by technological changes, and what alternative approaches to protect privacy are being examined by industry and government.	The panels were moderated by Board members and drew speakers from the information technology industry, academic research centers, advocacy groups, and current and former government officials to offer their perspectives. The objective of the event was to educate Board members and the public on the diversity of views on the topic. The results of the forum will also inform future Board deliberations on other specific projects planned for FY 2015 and beyond.

ACRONYMS

AG – Attorney General.

CCTV- Closed Circuit Television.

CIO – Chief Information Officer.

CMO – Chief Management Officer.

COOP – Continuity of Operations Plan.

CSO – Chief Security Officer.

CT – Counterterrorism.

DHS – Department of Homeland Security.

E.O. – Executive Order.

ED – Executive Director.

FBI – Federal Bureau of Investigation.

FIPS – Federal Information Protection Standards.

FISA – Foreign Intelligence Surveillance Act of 1978.

FISMA - Federal Information Security Management Act.

FTE – Full-time Equivalents.

FY – Fiscal Year.

GC – General Counsel.

GSA – General Services Administration.

HSPD – Homeland Security Presidential Directive.

IC – Intelligence Community.

IDS – Intrusion Detection Systems.

ISE – Information Sharing Environment.

IT – Information Technology.

JWICS – Joint Worldwide Intelligence Communications System.

NARA – National Archives Records Administration.

NCTC – National Counterterrorism Center.

NSA – National Security Agency.

ODNI – Office of the Director of National Intelligence.

OMB – Office of Management and Budget.

PCLOB – The Privacy and Civil Liberties Oversight Board.

PIAB – President's Intelligence Advisory Board.

PPD – Presidential Policy Directive.

SCIF – Sensitive Compartmented Information Facility.

TIC – Trusted Internet Connection.

INDEX

This page is intentionally left blank.

Privacy and Civil Liberties Oversight Board
www.pclob.gov
202.331.1986