



US **PRIVACY AND
CIVIL LIBERTIES**
OVERSIGHT BOARD

Congressional Budget Justification

Fiscal Year 2027

Privacy and Civil Liberties Oversight Board

Congressional Budget Justification

FISCAL YEAR 2027

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD
800 N. CAPITOL STREET, NW
WASHINGTON, DC 20002

This report is available at <https://www.pclob.gov/BudgetJustifications>
Send comments or questions to info@pclob.gov or to the mailing address above.

TABLE OF CONTENTS

PROPOSED FISCAL YEAR 2027 APPROPRIATIONS LANGUAGE	1
EXECUTIVE SUMMARY	2
MISSION AND VALUES	4
BOARD HISTORY AND AUTHORITIES	5
FY 2027 BUDGET JUSTIFICATION SUMMARY	8
FUNDING HIGHLIGHTS	8
ADDRESSING PRESIDENTIAL PRIORITIES.....	8
FY 2027 JUSTIFICATION FOR RESOURCES AND ANTICIPATED PERFORMANCE	12
ACCOMPLISHMENTS AND ONGOING ACTIVITIES	13
FY 2027 BUDGET EXHIBIT.....	19

PROPOSED FISCAL YEAR 2027 APPROPRIATIONS LANGUAGE

“For necessary expenses of the Privacy and Civil Liberties Oversight Board, as authorized by section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee), \$14,436,000, to remain available until September 30, 2028 (*Financial Services and General Government Appropriations Act, The Consolidated Appropriations Act*).”

EXECUTIVE SUMMARY

The Privacy and Civil Liberties Oversight Board (PCLOB) requests \$14.436 million for its Fiscal Year (FY) 2027 Budget Request. The FY 2027 Budget Request, which includes an increase of \$736,000 (or 5%) over the FY 2026 enacted appropriation of \$13.7 million, would allow PCLOB to continue its significant mission-related and operational accomplishments.

PCLOB is an independent agency within the executive branch, established in its current form by the Implementing Recommendations of the 9/11 Commission Act of 2007,¹ with a mission to ensure that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties. The agency is headed by a bipartisan, five-Member Board, whose Members are selected based on their expertise in counterterrorism, intelligence, privacy, civil liberties, and technology. PCLOB conducts oversight and provides advice regarding executive branch regulations, policies, procedures, and activities related to efforts to protect the nation from terrorism.

PCLOB continued to undertake a vigorous agenda to carry out its statutory responsibilities in FY 2025, releasing an unprecedented number of five advice and oversight reports by the end of the fiscal year. In FY 2026, the agency's open projects included the following:

- Oversight of the government's implementation of Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence Activities;
- Oversight of the surveillance program operated pursuant to Section 702 of the Foreign Intelligence Surveillance Act (FISA);
- Oversight of the government's actions to combat domestic terrorism;
- Oversight of the use of open-source information by the Federal Bureau of Investigation (FBI); and
- A review of the use of Tactical Terrorism Response Teams (TTRTs) by U.S. Customs and Border Protection (CBP).

¹ Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 801, 121 Stat. 266, 352-358, codified at 42 U.S.C. § 2000ee.

CURRENT MEMBERS OF THE BOARD

Board Member Beth A. Williams, appointed to a term ending January 29, 2026.²

² The James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, § 6801, 136 Stat. 2395, 3586 (extending a Member's term of office for up to one year after the date of expiration, at the election of the Member, either during the period preceding reappointment or until the member's successor has been appointed and qualified).

MISSION AND VALUES

MISSION

PCLOB provides advice and conducts oversight 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.

VALUES

Four key values guide PCLOB's work:

Integrity – As an agency whose power lies in its persuasiveness, PCLOB strives to preserve its reputation for independence, integrity, and credibility. The agency approaches its activities with objectivity and good faith. PCLOB strives to treat executive branch agencies and other outside parties with evenhandedness and respect and to evaluate a wide range of data, viewpoints, and considerations.

Transparency – PCLOB aims to foster understanding of the ways that efforts to protect the nation from terrorism may impact privacy and civil liberties. In addition, the agency conducts its own activities responsibly and transparently to foster confidence in its management of authorities, resources, and information. PCLOB promotes transparency by holding public hearings and issuing public reports, to the greatest extent possible, consistent with the protection of classified information and applicable law, and by soliciting input from the public and outside experts.

Rigor – PCLOB strives for the highest standard of quality in its analysis and recommendations. When examining government programs, the agency takes care to understand those efforts in all their complexity. In assessing whether such efforts are consistent with the law and appropriately protect privacy and civil liberties, PCLOB strives to be thorough and accurate, and to account for the impact of new and emerging technologies and institutional reforms. When recommending changes to those efforts, the agency seeks to fully consider the foreseeable impact of its recommendations.

Equality Under the Law – PCLOB is committed to helping ensure that all persons are treated equally under the law, both as a component of protecting privacy and civil liberties, and in its own internal operations.

BOARD HISTORY AND AUTHORITIES

PCLOB was created at the recommendation of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission). Through the Intelligence Reform and Terrorism Prevention Act of 2004, Congress created a Privacy and Civil Liberties Oversight Board within the Executive Office of the President.³ In 2007, through the Implementing Recommendations of the 9/11 Commission Act, Congress established PCLOB in its current form as an independent agency within the executive branch.

The Board is composed of a full-time Chair and four part-time Members, each appointed by the President, with the advice and consent of the Senate, to staggered six-year terms. PCLOB's statute requires that no more than three Members come from the same political party. All Members are to be selected "on the basis of their professional qualifications, achievements, public stature, expertise in civil liberties and privacy, and relevant experience."⁴ At present, the Board has one Member and is operating in sub-quorum status. Our Sub-Quorum Policy permits the agency to continue significant work in the absence of a quorum.

PCLOB's mission is to ensure that the executive branch's efforts to protect the nation from terrorism are balanced with the need to protect privacy and civil liberties. Specifically, the agency's enabling statute, 42 U.S.C. § 2000ee, authorizes it 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 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 from terrorism."

These purposes encompass two core functions: providing advice and conducting oversight.

Under PCLOB's advice function, executive branch agencies can consult with the agency at an early stage in the development of legislation, policies, programs, guidelines, or regulations to ensure that privacy and civil liberties protections are appropriately considered in their design.⁵

³ Intelligence Reform and Terrorism Prevention Act, Pub. L. No. 108-458, § 1061, 118 Stat. 3638, 3684-3688 (2004).

⁴ 42 U.S.C. § 2000ee(h)(2).

⁵ *Id.* § 2000ee(d)(1).

In its oversight role, PCLOB is charged with continually reviewing (1) regulations, policies, procedures, and practices within the agency's jurisdiction to ensure that privacy and civil liberties are protected; and (2) other actions within PCLOB's jurisdiction to ensure that those actions appropriately protect privacy and civil liberties and are consistent with governing laws, regulations, and policies regarding privacy and civil liberties.⁶

PCLOB's statute makes transparency an inherent part of its mission. Specifically, the agency is required to inform the public about its work by holding public hearings, issuing public reports to the extent consistent with the protection of classified information and applicable law, providing semi-annual reports to the Congress, and appearing and testifying before Congress upon request.⁷

PCLOB has additional functions, such as making recommendations, when appropriate, to other agencies' privacy and civil liberties officers regarding their activities and coordinating their activities on relevant interagency matters.⁸ Congress has also identified PCLOB as a source of recommendations for individuals to serve as amici curiae to the Foreign Intelligence Surveillance Court.⁹

PCLOB also has designated roles under the following authorities:

- **Executive Order 13636, *Improving Critical Infrastructure Cybersecurity***, issued in February 2013, calls upon multiple agencies to develop and implement a cybersecurity framework to minimize the risk of a cyberattack on critical infrastructure.¹⁰ Section 5 of the Executive Order requires the Department of Homeland Security (DHS) to consult with PCLOB in preparing a report recommending ways to mitigate the privacy and civil liberties risks created by cybersecurity measures adopted under the order. That report must be reviewed on an annual basis and revised, as necessary.

⁶ *Id.* § 2000ee(d)(2). PCLOB is also charged with continually reviewing information-sharing practices within its jurisdiction.

⁷ *Id.* § 2000ee(d)(4), (f).

⁸ *Id.* § 2000ee(d)(3). In addition, PCLOB may designate new departments, agencies, or elements of the executive branch for coverage by the requirements of Section 803. *See id.* § 2000ee-1(a).

⁹ USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 401(i)(1), 129 Stat. 268, 279-281.

¹⁰ Exec. Order No. 13,636, 3 C.F.R. 13636 (Jan. 1, 2014).

- **Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Section 803)** requires certain executive branch departments, agencies, and elements to designate at least one senior official as a Civil Liberties and Privacy Officer (CLPO).¹¹ Each agency’s CLPO must issue semi-annual reports on the discharge of each of his or her functions under the statute.¹² These Section 803 Reports are to be submitted to the head of the CLPO’s agency, designated congressional committees, and PCLOB.¹³ These reports must be in unclassified form to the greatest extent possible
- **Executive Order 14086, *Enhancing Safeguards for United States Signals Intelligence Activities***, issued in October 2022, provides enhanced protection for privacy and civil liberties in signals intelligence as part of the new Data Privacy Framework to promote data transfers between the European Union (EU) and the United States. The Executive Order requires U.S. intelligence agencies to update their policies and procedures for signals intelligence activities in order to provide enhanced safeguards for privacy and civil liberties, and it establishes a redress mechanism for individuals from qualifying states alleging improper surveillance of their communications by the U.S. government. The order outlines roles for PCLOB in assessing implementation of these procedures, as well as in conducting annual reviews of the redress process.

¹¹ Implementing Recommendations of the 9/11 Commission Act of 2007, § 803, amended by FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, § 109, 132 Stat. 3, 15, codified at 42 U.S.C. § 2000ee-1(a). The entities covered are the Office of the Director of National Intelligence, the Central Intelligence Agency, the National Security Agency, the Federal Bureau of Investigation, and the Departments of Defense, Health and Human Services, Homeland Security, Justice, State and Treasury.

¹² 42 U.S.C. § 2000ee-1(f). Before its amendment in 2014, the statute required quarterly reports.

¹³ *Id.* § 2000ee-1(f)(1)(A).

FY 2027 BUDGET JUSTIFICATION SUMMARY

	FY 2023 Enacted	FY 2024 Enacted	FY 2025 Enacted	FY 2026 Enacted	FY 2027 (Requested)	FY26/FY27 (Delta %)
<i>(Dollars in Thousands)</i>						
Appropriation	\$ 10,600	\$ 13,700	\$ 13,700	\$ 13,700	\$ 14,436	5.4%
Carryover	\$ 1,700	\$ 1,300	\$ 3,400	\$ 3,200	\$ 1,000	-68.8%
Total Available	\$ 12,300	\$ 15,000	\$ 17,100	\$ 16,900	\$ 15,436	-8.7%
FTE Positions	37	43	43	43	37	-14.0%

FUNDING HIGHLIGHTS

PCLOB’s FY 2027 Budget Request is \$14.436 million and aligns with the agency’s projected expenses required to successfully achieve the agency’s mission. This request, paired with an anticipated carryover of approximately \$1 million from FY 2026’s Budget Request, would allow PCLOB to sufficiently fund the agency’s anticipated operational expenses of \$15.436 million, and accounts for the anticipated nomination and confirmation of new Board Members.

The number of the agency’s full-time employee (FTE) positions is shown as reduced from 43 to 37 in the exhibit above in FY 2027 to align with the Agency Reduction in Force and Reorganization Plan (ARRP) submitted to the Office of Management and Budget (OMB) and the U.S. Office of Personnel Management (OPM) in FY 2025. The ARRP called for position consolidation through OPM’s deferred resignation program, performance-based adjustments, and an agency-wide reduction in force (RIF).

While PCLOB’s salary expenses are projected to decrease as a result of the ARRP implementation, the agency’s funding requirements for critical goods and services are anticipated to increase in FY 2027. Along with the expected carryover from the FY 2026 appropriation, PCLOB’s requested FY 2027 funding will permit the agency to pursue its mission pursuant to the President’s direction for a more effective and efficient government.

ADDRESSING PRESIDENTIAL PRIORITIES

This section of the FY 2027 Budget Request summarizes proposals in the areas of agency management tied to Presidential priorities around eliminating waste, fraud and abuse, the workforce, Federal procurement, financial management, and information technology. These priorities to advance the forthcoming President’s Management Agenda (PMA) and other Government-wide management efforts include:

- *Rightsizing the Federal Real Estate Footprint:* PCLOB’s real estate footprint is very small, consisting only of office space secured through an occupancy agreement with the U.S. General Services Administration (GSA). The agreement extends through April 2028 and affords the agency partial use of one floor of one building, with the majority of the square footage being a Sensitive Compartmented Information Facility (SCIF). Due to this unique real estate configuration, PCLOB is currently working with GSA to evaluate lease renewal options beyond FY 2028 that align with the PMA.

In addition to annual rent to GSA, PCLOB incurs other related operations and maintenance costs relating to required building security services, custodial services, and information technology (IT) data center rack space and associated infrastructure support.

Functional Area Identifier	Functional Area Code	RPM Asset Lifecycle Phase Name	RPM Asset Lifecycle Phase Code	RPM Asset Cost Category Name	RPM Asset Cost Category Code	Agency Subject 3 Digit Code	FY2026	FY2027	FY2028	FY2029	FY2030	Comments
							BY	BY+1	BY+2	BY+3	BY+4	
(in Thousands)												
Real Property Management	5	Rent and Related Expenses - Leased Properties	4	Rent to GSA	M	54M	1,058	1,070	TBD	TBD	TBD	Occupancy agreement expires in April 2028
				Other related O&M costs	O	540	377	386	TBD	TBD	TBD	Security, custodial, and data center

- *Establishing a Merit-Based Federal Workforce:* PCLOB supports fair and merit-based hiring practices, and, with the assistance of its shared services provider, adheres to OPM guidelines, ensuring fair and open competitive hiring based on qualifications, experience, and adherence to civil service rules, while working to eliminate discriminatory practices and streamlining processes consistent with the merit system principles established across federal agencies.
- *Efficient Government Systems:* PCLOB works with federal shared service providers for core functions, including Financial Management, Procurement, Human Resources and Payroll, and Travel. The agency will continue to collaborate with its shared service providers to comply with requirements that align with the President's priorities, as outlined in Executive Order 14249, *Protecting America's Bank Account Against Fraud, Waste, and Abuse* and Executive Order 14240, *Eliminating Waste and Protecting Taxpayer Dollars by Consolidating Procurement*.

- *Defending Against Sophisticated Cyber Adversaries*: PCLOB’s FY 2027 budget request would sufficiently fund necessary resources to effectively counter increasingly sophisticated cyber threats. Central to PCLOB’s proactive and strategic approach in its cybersecurity posture is a strong commitment to advancing along the Cybersecurity and Infrastructure Security Agency’s (CISA) Zero Trust Maturity Model. Integrating Zero Trust principles such as least privilege access, continuous authentication, and real-time threat detection into agency governance and decision-making frameworks is also essential. By embedding cybersecurity into core operations, PCLOB can maintain adaptive and resilient security postures.

A foundational aspect of this defense strategy involves comprehensive visibility and control over all agency assets. This includes traditional IT systems, Internet of Things (IoT) devices, operational technology (OT), and cloud-based infrastructure. Maintaining an up-to-date and accurate inventory of these assets is essential for identifying vulnerabilities and mitigating risk.

Additionally, building centralized data analytics environments is crucial. These platforms provide enterprise-wide visibility, enabling data-driven, risk-informed decisions. Leveraging advanced analytics and AI enhances threat detection, accelerates response, and supports accountability.

- *Leveraging the Buying Power of the Federal Government—Buying American*: PCLOB will prioritize the President’s Made in America agenda by maximizing the use of domestically-produced goods, products, and materials. Further, the agency will use all available tools and resources, consistent with existing laws, to reduce or eliminate the need for waivers.
- *Accelerating Federal Use of Artificial Intelligence (AI) through Innovation, Governance, and Public Trust*: In keeping with the Administration’s efforts to drive AI innovation within the Federal government and improve services to the public, PCLOB is initiating several efforts to assess opportunities and build capacity to incorporate AI into its work processes. Challenges include the appropriate protection of classified and controlled information in the agency’s statutory oversight and advice work. Foreseeable AI initiatives (with no expected increase to the FY 2027 budget request) include:

- Evaluation of commercially available AI tools and services for their potential effectiveness, accuracy, and efficiency in performing programmatic oversight activities. Oversight activities require extensive research and review of written material; success will be demonstrated by identifying AI tools or services that can extract significant findings at least as reliably and accurately as human reviewers.
- Scaling up use of AI requires expertise gained through additional training of staff. Proper consideration should be given to the identification of appropriate training resources and materials for optimal results.

FY 2027 JUSTIFICATION FOR RESOURCES AND ANTICIPATED PERFORMANCE

PCLOB's FY 2027 Budget Request focuses on key capabilities and anticipated performance in the following areas:

- Providing effective, timely, and relevant advice regarding the protection of privacy and civil liberties in the development and implementation of legislation, regulations, and policies related to efforts to protect the nation against terrorism;
- Conducting effective oversight of executive branch authorities, policies, and activities related to efforts to protect the nation against terrorism to ensure appropriate protection of privacy and civil liberties;
- Offering insight on the effects of new and emerging technologies on the balance between government counterterrorism activities and privacy and civil liberties;
- Promoting transparency regarding PCLOB's activities and issues within its jurisdiction to the extent consistent with the protection of classified information and applicable law;
- Building and strengthening relationships with agency CLPOs and coordinating the activities of those officers on relevant interagency matters;
- Strengthening PCLOB's institutional capacity. This includes a continued focus on retaining highly qualified staff; maintaining robust cybersecurity; exercising effective fiscal management to ensure that taxpayers' dollars are spent wisely; and pursuing the most efficient shared services provided by other federal agencies to make better use of taxpayer dollars; and
- Continued implementation of PCLOB's Strategic Plan.

ACCOMPLISHMENTS AND ONGOING ACTIVITIES

Advice, Oversight, and Other Mission Activities

PCLOB has continued to undertake a vigorous agenda to carry out its statutory responsibilities.

Advice – Since 2016, PCLOB has provided advice on every significant revision or issuance by an Intelligence Community element of its Attorney General-approved guidelines governing the handling of U.S. person information collected under Executive Order 12333, *United States Intelligence Activities*. Most recently, in FY 2023, consistent with Executive Order (EO) 14086, *Enhancing Safeguards for United States Signals Intelligence Activities*, PCLOB reviewed and provided advice regarding updated policies and procedures developed by intelligence agencies to ensure enhanced privacy and civil liberties protection in connection with signals intelligence activities. In FY 2024, PCLOB provided advice to the Department of Justice regarding candidates to serve as judges and special advocates for the new Data Protection Review Court created by the Executive Order. In addition, PCLOB participated along with U.S. government representatives in the European Union-U.S. Data Privacy Framework Review, which informed the Commission’s report on the adequacy of the Data Privacy Framework, as required by EU law.

Oversight – PCLOB continues its work on oversight projects related to efforts to protect the nation against terrorism and will continue its robust agenda in FY 2027. The agency’s oversight docket will evolve by FY 2027. In FY 2025, highlights included:

- PCLOB concluded its review of the government’s use of airline Passenger Name Records.¹⁴
- PCLOB released a report on the Terrorist Screening Database, commonly known as the Terrorist Watchlist. The report describes the standardized protocols employed by the government to determine the contents of the Terrorist Screening Database, explains redress processes available to individuals who believe they are inappropriately listed or have been inappropriately impacted due to watchlisting, and includes recommendations for program improvements to enhance privacy and civil liberties safeguards.

¹⁴ Further details concerning PCLOB’s review of this program remain classified.

- PCLOB released a report, per Section 824 of the Consolidated Appropriations Act of 2022, assessing the impacts on the privacy and civil liberties of Americans concerning the use or recommended use of any federal laws, regulations, and policies used to address significant threats to the United States and Americans associated with foreign racially motivated violent extremist organizations. The report includes recommendations on options to develop protections to mitigate such impacts.
- PCLOB released a report on the National Counterterrorism Center’s (NCTC’s) access to and handling of datasets containing non-terrorism information. The report assesses whether NCTC’s policies and practices concerning such materials are consistent with governing laws, regulations, and policies and appropriately balance privacy and civil liberties interests with national security interests relating to counterterrorism.
- PCLOB released a comprehensive report evaluating the use of facial recognition technology for aviation security. The report reviews how facial recognition technology is used to verify the identity of passengers at airport security checkpoints, considering both operational benefits and privacy and civil liberties concerns.
- PCLOB continued to examine executive branch policies and activities to counter domestic terrorism, with a focus on two simultaneous and distinct workstreams: the impact on First Amendment rights, including as a result of efforts to counter mis-, dis-, and mal-information; and the impact on privacy and civil liberties of particular groups, such as those with shared racial, religious, political, or ideological affiliations.
- PCLOB opened a new project on the surveillance program that the executive branch operates pursuant to FISA Section 702. PCLOB published its *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* in September 2023, to inform public and congressional debate regarding reauthorization of the program, which occurred in April 2024. The new project updates that report in advance of expiration of the authority in April 2026.

- PCLOB conducted oversight to carry out the roles envisioned for it in [Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence Activities](#). Specifically, the Board reviewed implementation of the updated policies and procedures adopted by the intelligence agencies pursuant to the executive order to ensure that they are consistent with the enhanced safeguards contained in the order.

Other Mission Activities –

- PCLOB’s authorizing statute instructs the agency to advise covered agencies on their efforts to protect privacy and civil liberties and to coordinate those activities on relevant interagency matters. For example:
 - Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 requires agencies’ CLPOs to issue periodic reports about their activities to their respective agency heads, Congress, and PCLOB. The agency has received Section 803 reports from federal departments and agencies, which are available on the PCLOB website.
 - PCLOB is committed to ensuring that its work is available, relevant, and informative for the public, Congress, and other federal agencies. To foster a better understanding of PCLOB’s mission and work, Board Members speak at events sponsored by professional organizations and other stakeholders in the national security and privacy and civil liberties space.
- PCLOB continued to track developments regarding advanced and emerging technologies through an AI and machine learning working group and is considering various areas for possible oversight and advice.

Operational Support

PCLOB must work diligently to maintain strong administrative, managerial, and organization capabilities, enabling the small agency to operate efficiently while recognizing solid accomplishments over its human resources and financial management, information technology, and security of agency data, personnel, and assets.

Workforce – PCLOB seeks to ensure that its staff encompasses a broad range of professional backgrounds, including experience in intelligence, counterterrorism, privacy and civil liberties, oversight and investigations, and technology. At the end of FY 2025, PCLOB had a total of 27 employees (1 Board Member and 26 staff members).

PCLOB’s workforce continues to support the President’s efforts to restore the values of individual dignity, hard work, and excellence.

In FY 2027, PCLOB will continue the following workforce initiatives:

- Sustain a positive and professional workplace;
- Focus on merit-based hiring and retention practices;
- Improve human capital assessments and guidance, including reviewing how to improve assessments of employee performance and recognition;
- Implement a thorough succession plan that is responsive and adaptive to agency operations; and
- Continue to encourage and facilitate staff participation in high-quality training programs to ensure the ongoing professional development of PCLOB’s workforce.

Information Technology Systems and Cybersecurity – In FY 2025, PCLOB’s IT team focused on strengthening the agency’s cybersecurity posture. To that end, PCLOB’s IT staff executed solutions to address and implement multiple key directives:

- **CISA Binding Operational Emergency Directive (BOD) 25-02, *Mitigate Microsoft Exchange Vulnerability***, to remediate configurations that may allow an attacker to move laterally across MS Exchange Infrastructure.
- **CISA Binding Operational Directive 25-01, *Implementing Secure Practices for Cloud Services*** to align PCLOB’s Microsoft 365 and other cloud tenants to CISA’s Secure Cloud Business Applications (SCuBA) secure configuration baselines, enroll in continuous monitoring via SCuBA assessment tools, and report compliance.

Additionally, the PCLOB IT staff began onboarding solutions and strategies aimed at addressing the focus areas identified in the CISA Zero Trust Maturity Model tenets.

Information security remained a top priority: an independent FY 2025 audit found PCLOB’s information security controls to be effective; the annual FISMA audit confirmed that internal controls sufficiently protected information resources; and the Office of the Chief

Information Officer mitigated all identified vulnerabilities through independent penetration testing.

PCLOB also continued leveraging shared-service providers and contractor support to enhance boundary-protection mechanisms. The IT team implemented, maintained, and documented technical controls in compliance with federal standards and CISA Cross-Agency Priority Goals for cybersecurity, including asset management, network and data protection, and least-privilege access. Looking ahead into FY 2026 and through FY 2027, PCLOB will maintain its focus on Zero Trust Tenets while continuing to meet current and evolving CISA BOD requirements.

Financial Management – Sound fiscal management is integral to the execution of PCLOB’s mission and remains a top priority for the agency. PCLOB has maintained its positive momentum in improving its financial management. In November 2025, PCLOB issued its annual Agency Financial Report (AFR), which included an unmodified (“clean”) audit opinion of the FY 2025 financial statements, with no material weaknesses or significant deficiencies noted, as well as a report on an internal controls assessment, which found no waste, fraud, or abuse. Through the agency’s diligence and dedication to successful issuance of the AFR each year, PCLOB continues to meet statutory reporting requirements and demonstrates its responsible stewardship of funds and sound financial management.

Protecting Classified and Sensitive Information – PCLOB’s Chief Security Officer (CSO) is actively involved in government-wide initiatives aimed at modernizing the security clearance process. This includes the rollout of Trusted Workforce (TW) 2.0 and adherence to the National Security Presidential Memorandum (NSPM) 28, which mandates that agencies establish an Operations Security program aligned with the standards set forth in Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*. EO 13587 enhances the security of classified networks and ensures the responsible sharing and protection of classified information.

Additionally, PCLOB has transitioned certain security responsibilities to the Defense Counterintelligence and Security Agency (DCSA), leading to enhanced services for the agency. The CSO, serving as the Senior Implementation Officer (SIO) for TW 2.0, remains focused on enrolling all PCLOB staff in the updated Continuous Evaluation process. This initiative involves collaboration with the ODNI, DCSA, and the FBI Rap Back Service as part of a concerted effort to reform the personnel security clearance system.

The CSO, serving as the SAO under Executive Order 13526, *Classified National Security Information*, guarantees PCLOB's compliance with annual requirements set by the National Security Information Oversight Office. PCLOB remains committed to the modernization of security education and awareness, reporting, and compliance initiatives.

FY 2027 BUDGET EXHIBIT

FY 2027 Budget Request by Object Class		
<i>(Dollars in Thousands)</i>		
Object Class		FY 2027 Request
<i>Personnel Services</i>		
11.1	Full-Time Permanent	\$ 5,966
11.3	Other than Full-Time Permanent	\$ 480
11.5	Other Personnel Compensation	\$ 149
12.1	Civilian Personnel Benefits	\$ 2,256
<i>Operation and Mission Services</i>		
21.0	Travel and Transportation of Persons	\$ 50
23.1	Rental Payments to GSA	\$ 1,103
23.2	Rental Payments to Others	\$ 22
23.3	Communications, Utilities, and Misc. Charges	\$ 422
24.0	Printing and Reproduction	\$ 8
25.1	Advisory and Assistance Services	\$ 2,627
25.2	Other Services from Non-Federal Sources	\$ 188
25.3	Other Goods and Services from Federal Sources	\$ 342
25.4	Operation and Maintenance	\$ 77
26.0	Supplies and Materials	\$ 134
31.0	Equipment	\$ 612
Total		\$ 14,436