General Support System

Does the PCLOB use the information to benefit or make a determination about an individual?	No.
What is the purpose?	Store and transmit data required to carry out the mission and operational activities of the PCLOB.
Are there controls to enforce accountability?	Yes, all standard PCLOB privacy protections and security controls apply.
What opportunities do I have for participation?	Opportunities generally include appropriate opportunities for notice, consent, access, and redress.

OVERVIEW

The Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law No. 110-53, Title VIII, established the Privacy and Civil Liberties Oversight Board ("PCLOB" or "Board"). The mission of the PCLOB is to ensure that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties.

In pursuing its mission, the PCLOB uses a networked infrastructure to provide the data processing needs to employees, contractors, and partners. This infrastructure includes both hardware and software to support both mission and daily operations. This general support system ("GSS") contains or connects to other GSSs, including cloud environments and major and minor applications, such as the PCLOB Active Directory and file and printer services.

The information that is contained on, or is transported over, the Infrastructure GSS includes every type of information that the PCLOB uses in support of its mission, including human resources data for personnel purposes, background investigation data for personnel security purposes, and other types of data required for meeting mission objectives and operational activities. This data at times contains Personally Identifiable Information ("PII") of employees and contractors, and others. This could range from PII of low sensitivity such as the type of contact information found on business cards (e.g., name, email, address, and phone number) to highly sensitive information such as individual's Social Security number and financial account numbers.

The Infrastructure GSS Privacy Impact Assessment ("PIA") is meant to cover all these types of information that exist on or traverses the PCLOB's technical infrastructure. For additional information and analysis related to specific systems, applications, and data collections, program-specific privacy impact assessments are available at pclob.gov/Legal/Privacy.

The main components of the infrastructure include:

- Client devices,
- Servers,
- Wide Area Network (WAN),
- Local Area Networks (LANs),
- Virtual Networks,
- Network Perimeter Devices and Boundary Protections,
- Remote Access Devices,
- Active Directory,
- File and Print Servers,
- Database Management Systems,
- Messaging Servers and Systems,
- Identity, Credentialing, and Access Control Management Systems, and
- Video Conferencing and Web Conferencing Systems.

The components of the Infrastructure GSS make up the fundamental hardware and software that provide connectivity, security, storage, and data access for PCLOB employees and contractors. These range from client devices where employees and contractors can perform daily work to central

data storage and management devices. Many of the components of the Infrastructure GSS are the physical tools or systems used to implement the security controls: access control systems provide a mechanism for moderating access requests to information, remote access devices appropriately limit access to systems to a distributed workforce, boundary protection devices protect internal systems from unauthorized access.

The establishment of the Infrastructure GSS is authorized by the Board's enabling statute, codified at 42 U.S.C. § 2000ee. Information in the Infrastructure GSS is collected in accordance with and is compliant with applicable federal laws, including the Privacy Act of 1974.[1]

Much of the information in the Infrastructure GSS does not constitute a system of records because it is not retrieved or retrievable by personal identifier. However, where it does constitute a system of records, the information is addressed in one or more of the PCLOB's System of Records Notices ("SORNs"). A complete list of applicable SORNs can be found at https://www.pclob.gov/Legal/Privacy.

PRIVACY RISK ANALYSIS

The primary privacy risks associated with data covered by the Infrastructure GSS PIA are risks related to:

- Purpose of Collection,
- Confidentiality,
- Data Quality and Integrity, and
- Data Minimization.

Purpose of Collection: Because the information included in the Infrastructure GSS covers nearly all the information that is collected and used by the PCLOB, it is important that the collections and uses of all data be reviewed to ensure that the data is only collected and used for appropriate purposes. A number of the components of the Infrastructure GSS place limitations on collection and use capabilities. For example, data may be contained in a role-based access-controlled file system. There are also administrative procedures requiring new collections or new uses of existing data to be reviewed to ensure that they fall within existing, approved frameworks for the collection and use of data.

Confidentiality: Because information of all types, including sensitive personal information, is either stored on or traverses the Infrastructure GSS, it is important that the controls exist to protect the confidentiality of the information. In the event of a breach of confidentiality, there is a risk of embarrassment or loss of reputation to both individuals and the PCLOB. In the case of sensitive PII, a breach of confidentiality could result in employees and contractors suffering financial harm or even identity theft. The PCLOB minimizes this risk by enforcing access controls to minimize the number of individuals who have access to the data and by storing data on systems that have been accredited as secure.

[1] The authorities for specific information collections are addressed in applicable System of Records Notices and program-specific privacy impact assessments, available at https://www.pclob.gov/Legal/Privacy.

Data Quality and Integrity: On occasion, the PCLOB may collect information that is out-of-date or incorrect. Because the interactions that result in information collection are often voluntary and because the PCLOB does not use any information collected through these types of interactions to deprive an individual of a right or benefit, the privacy risks associated with these collections are minimal. Finally, to minimize any residual impact on individuals, the PCLOB has implemented appropriate technical, physical, and administrative controls relative to the risks presented to confidentiality, information quality, and information uses. These controls are discussed in more detail in the subsequent sections of this PIA.

Data Minimization: The PCLOB reviews collections of data in an effort to try and minimize the collection of directly identifying PII to the greatest extent possible, while still allowing the PCLOB to complete its objectives in furtherance of its mission. This may be done by stripping collections of direct identifying PII, aggregating data, or other means of minimizing such collection. When the PCLOB does collect PII, it utilizes appropriate technical, physical, and administrative controls relative to the risk of the data. These controls are discussed below and in the appropriate PIA and SORN associated the particular collection.

PRIVACY RISK MANAGEMENT

1. Describe what information the PCLOB collects, how the information is collected, and the sources from which the information is collected.

The information that resides on or traverses the PCLOB infrastructure supports the Board's mission and operational activities. It may include either PII or non-PII as needed to support these objectives. The PCLOB takes steps to limit its intake to PII necessary for the purpose of its collection. PII could include:

- Name,
- Address (business or personal),
- Phone number (business or personal),
- E-Mail address (business or personal),
- Social Security number,
- Financial account numbers,
- Birth date or place,
- Demographic information,
- Income information,
- Employment information, and
- Personnel security information.

The information may be collected directly from individuals, when possible and appropriate, or it may be collected from third-party partners, public sources, and others. Most commonly information is collected from:

- Employees and contractors for personnel and clearance information,
- Individuals or organizations who are interested in receiving information from the PCLOB about public events,
- Members of the public submitting formal public comments on PCLOB-published notices or rulemaking,
- Representatives of industry,
- Federal government representatives, and
- Other individuals who interact with, or whose activities pertain to the mission of, the PCLOB.

In cases where the information is derived from non-public sources, such as other Federal agencies, the PCLOB obtains such information using contracts, information sharing agreements, or other similar agreements or processes, and in accordance with applicable law.

For additional information and analysis related to specific systems, applications, and data collections, program-specific privacy impact assessments are available at https://www.pclob.gov/Legal/Privacy.

2. Describe the PCLOB's objective for the information.

The information covered by this PIA is used to support all PCLOB mission and operational activities. The objectives for specific collections of information are described in the PCLOB's SORNs and program-specific privacy impact assessments, available at https://www.pclob.gov/Legal/Privacy.

3. Describe how the PCLOB shares, for compatible purposes, any of the information with third parties.

The PCLOB shares information that transverses or resides on the Infrastructure GSS for a number of purposes. The extent of information shared, with whom the information is shared, and the method of sharing will vary based on the specific mission or operational use. For example, the PCLOB may share employee information with Federal agencies to carry out background and suitability investigations as part of the employment process. The PCLOB also shares employee information with other Federal agencies to support the provision of employees' salaries and benefits.

Where applicable, the PCLOB may share information as outlined in the Routine Uses of the relevant SORNs and as described in program-specific privacy impact assessments, available at https://www.pclob.gov/Legal/Privacy.

4. Describe what opportunities, if any, individuals to whom the information pertains have to (a) receive notice regarding the PCLOB's use of the information; (b) consent to such use; (c) access the information that pertains to them; or (d) obtain redress.

Some information that transverses or resides on the Infrastructure GSS is collected directly from individuals (e.g., employment applications and FOIA and Privacy Act requests). Other information is not collected directly from individuals (e.g., technical information about user devices in order to provide technical support for web conferencing platforms).

When information is collected directly from individuals, they are given notice of the uses and the opportunity to consent to particular uses; the information will not be collected if individuals do not consent to a particular use. These individuals typically have opportunities to change or update information that is incorrect, out of date, or no longer relevant. Notice to individuals may be provided in the form of a Privacy Act Statement (when required by the Privacy Act of 1974), a privacy notice (when the Privacy Act of 1974 does not apply), or other methods such as an informed consent form, or instructions directing individuals to the privacy policy of a third-party partner or vendor, or to the PCLOB's own privacy policy for its website, pclob.gov. Finally, the PCLOB has published this and other PIAs and relies on a SORN (if applicable).

Where applicable, individuals may request access to or amendment of their information in accordance with the Privacy Act and the PCLOB's Privacy Act regulations, at 6 C.F.R. Parts 1001, 1002, and 1003 *et seq.* Individuals may sometimes be able to directly update their information—for example, by contacting the PCLOB directly to update contact or mailing information, or updating information provided for registration purposes for a PCLOB-sponsored event.

For additional information and analysis related to specific systems, applications, and data collections, applicable SORNs and program-specific privacy impact assessments are available at https://www.pclob.gov/Legal/Privacy.

5. Explain the standards and relevant controls that govern the PCLOB's—or any third party contractor(s) acting on behalf of the PCLOB—collection, use, disclosure, retention, or disposal of information.

The PCLOB complies with the Privacy Act of 1974, and E-Government Act of 2002; adopts Office of Management and Budget privacy-related guidance as best practices; and applies National Institute of Standards and Technology risk management processes for privacy.

The PCLOB uses the following technical and administrative controls to secure the information and create accountability for the Board's appropriate collection, use, disclosure, and retention of the information:

- Audit Logs and Reviews,
- PCLOB Personnel Privacy Training, including annual and role-based training,
- PCLOB Incident Response and Recovery Plan
- Compliance with PCLOB cybersecurity policy and procedures,
- Information Quality and Integrity Checks,
- Extract logging and 90-day reviews,
- Policy and Standard Operating Procedures,
- Role-based Access Controls,

- Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies,
- Records Schedule Submitted to/Approved by National Archives and Records Administration (NARA): Records will be disposed of according to the applicable records schedule. Information in the Infrastructure GSS is covered by PCLOB specific records schedules as well as general records schedules.
- Personnel Security supported through due diligence screening.

The PCLOB may use contractors to help support the collection, use, disclosure, or retention of information covered by this PIA, and those contractors are subject to similar controls.

Contractors with access to direct identifying PII are required to report suspected or confirmed privacy breaches to the PCLOB immediately and no later than one hour after discovery. Other requirements placed on contractors may include training on privacy, and compliance with federal privacy requirements and Federal Acquisition Regulations.

6. Discuss the role of third party(ies) that collaborate or partner with the PCLOB, if any. Identify any controls used to protect against inappropriate collection, use, disclosure, or retention of information. (This does not include third parties acting on behalf of the PCLOB, e.g., government contractors discussed in Question 5).

The PCLOB may at times collaborate with other federal agencies in limited number of ways. For example, the Board may partner with other federal government agencies to provision employees' salary and benefits and carry out other operational activities.

When the PCLOB does collaborate with federal agencies, controls are put in place to protect against inappropriate collection, use, disclosure, and retention depending on the type of sharing or data involved. Depending on the particular initiative, typical controls might include:

- Compliance with PCLOB cybersecurity policy and procedures,
- Agreements governing the sharing of information (e.g., contracts, Memorandum of Understanding, Memorandum of Agreement),
- Contracts,
- Policy and Standard Operating Procedures, and
- Role-based Access Controls.

DOCUMENT CONTROL

Approval

PRESTON MCGILL

C=US, O=U.S. Government, OU=PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD, CN=PRESTON MCGILL + OID.0.9.2342.19200300.100.1.1=9520100333258
I have reviewed this document
2020-06-19 09:19:33

Preston McGill

Chief Information Officer

Eric Broxmeyer

Digitally signed by Eric Broxmeyer
Date: 2020.06.22 12:16:32 -04'00'

Eric Broxmeyer

Senior Agency Official for Privacy

Change Control

Version	Summary of material changes	Pages affected	Date of change