

## **Privacy Shield Ombudsperson Mechanism Unclassified Implementation Procedure**

(U) **PURPOSE:** The Privacy Shield Ombudsperson Mechanism Implementation Procedure (Procedure) governs the implementation of commitments undertaken by the Department of State (Department) pursuant to EU-U.S. Privacy Shield Ombudsperson Mechanism Regarding Signals Intelligence (Ombudsperson Mechanism) under the EU-U.S. Privacy Shield Framework (Framework) and other comparable arrangements extending the Privacy Shield Ombudsperson Mechanism. It assigns responsibilities for the review of allegations that the U.S. Intelligence Community has engaged in signals intelligence activities that do not comply with applicable restrictions affecting the personal privacy of unconsenting persons covered under the Ombudsperson Mechanism. The Department of State takes seriously allegations that U.S. signals intelligence activities have been conducted in a manner that fails to comply with applicable privacy protections and other restrictions. This Procedure is implemented consistent with applicable U.S. laws, policies, and procedures.

(U) **ROLES AND RESPONSIBILITIES:**

(U) **The Privacy Shield Ombudsperson (Ombudsperson)** oversees implementation of this Procedure and performs certain other specified functions contained herein. The Framework directs the Department's Senior Coordinator for International Information Technology Diplomacy under Presidential Policy Directive 28: Signals Intelligence to serve as the Ombudsperson. The Under Secretary of State for Economic Growth, Energy, and the Environment (E) has been designated as the Senior Coordinator for International Information Technology Diplomacy. The Under Secretary reports directly to the Secretary of State. To carry out the Ombudsperson duties, the Under Secretary will work closely with other U.S. government officials and agencies, including appropriate independent oversight bodies, to ensure that completed requests are processed and resolved in accordance with applicable laws and policies.

(U) **The Office of International Communications and Information Policy (EB/CIP)** performs chief implementation functions under this Procedure. EB/CIP will update the Bureau of European and Eurasian Affairs (EUR) on an at least monthly basis as to the number of requests and responses under the Mechanism.

(U) **The Bureau of Intelligence and Research (INR)** advises the Ombudsperson and EB/CIP concerning intelligence issues and coordinates as appropriate with Intelligence Community (IC) partners.

(U) **The Office of the Legal Adviser (L)** provides legal advice and coordinates as appropriate with IC partners.

(U) **The Bureau of Public Affairs (PA)** administers the public-facing Ombudsperson website.

(U) **The Bureau of Information Resource Management (IRM)** designs and provides technical support to the password-controlled Privacy Shield Ombudsperson Request Website.

(U) **PROCESS:**

(U) The EU Individual Complaint Handling Body (CHB)<sup>1</sup> submits perfected requests, consistent with paragraph 3.b. of the Ombudsperson Mechanism section of the Framework, for review to the Ombudsperson via a web portal that feeds into the Department's SharePoint site. The perfected request for review consists of the EU individual's request and a form completed by the CHB during its assessment.

(U) Initial Vetting and Disposition:

(U) Upon receiving each request for review, EB/CIP:

- ensures that the Sharepoint site has automatically generated an individual tracking number and sent a confirmation of receipt to the CHB (these functions should occur automatically); and
- reviews the request to confirm it contains all required elements under paragraph 3.b. of the Ombudsperson Mechanism, which are:
  - the request contains information that –
    - forms the basis of the request;
      - Note: such information must contain at least one unique identifier associated with the type(s) of communications that are the subject of the request (examples are a telephone number or email address); a request that does not contain a unique identifier is deficient
    - states the nature of information or relief sought;
    - identifies the U.S. government entities believed to be involved, if any; and
    - cites any other measures the individual has taken to obtain the information/relief requested and the response received, if any; and
  - the CHB has –
    - confirmed verification of the requestor's identity;
    - concluded that the request concerns data reasonably believed to have been transferred under a covered mechanism; and
    - determined that the request is not frivolous, vexatious, or made in bad faith.

---

<sup>1</sup> References to the CHB throughout are also intended to apply to similar bodies under comparable arrangements.

(U) In the course of this review, EB/CIP makes one of three determinations, in consultation with the Ombudsperson, INR, L, and other offices as necessary:

- the request does appropriately seek review under the Ombudsperson Mechanism but is deficient in one or more aspects (e.g., lack of identifier);
- the request does not appropriately seek review under the Ombudsperson Mechanism and is better understood as a request for records under the Freedom of Information Act (FOIA); or
- the request is sufficient

(U) *Deficient Requests:* Requests that either do not contain a unique identifier or state the nature of information or relief sought, or that may not have been sufficiently reviewed by the CHB will be returned to the CHB, via the Sharepoint portal, along with a letter signed by the Director of EB/CIP/BA, or his or her designee, that details the deficiencies to be remedied. This letter should refer to the request by its individual tracking number.

(U) *FOIA Requests:* Requests that *exclusively* seek the production of or access to documents or other U.S. agency records may be best construed as FOIA requests. Uncertainty as to the nature of the request may require consultation with L and will be resolved in favor of processing the request under the Ombudsperson Mechanism. FOIA requests will be returned to the CHB, via the Sharepoint portal, along with a letter signed by the Director of EB/CIP/BA, or his or her designee, that explains the Department's assessment and provides information on how to submit FOIA requests.

(U) *Sufficient Requests:* Requests that contain the required information listed above are deemed sufficient. If a sufficient request also seeks the production of documents, it should be processed for review under the Ombudsperson Mechanism and the final response letter should both contain the Ombudsperson's substantive response and provide information on how to submit a FOIA request. Sufficient requests are further processed through interagency processes contemplated in Section 2 of the Ombudsperson Mechanism in accordance with applicable classified procedures.

(U) This initial vetting process is to be completed within fifteen (15) days of receiving the request, unless the volume of incoming requests requires additional resources. Should this occur, EB/CIP shall inform the Ombudsperson and seek her or his guidance, in consultation with INR and L as appropriate.

(U) Coordination:

(U) *Status Updates:* Should the CHB request information concerning the status of an individual request, EB/CIP will coordinate the preparation of a brief response confirming that the request is in process. Any such status updates will refer to the request by its

individual tracking number and are to be recorded in a mailbox associated with the Sharepoint system.

(U) Compliance Incidents: In the event that further processing pursuant to applicable classified procedures reveals a compliance incident, pertinent implementation processes pursuant to such procedures shall be followed to ensure the compliance incident is remedied.

- (U) Because the further processing discussed in the preceding paragraph might contain or indirectly reveal information that risks disclosure of sources and methods, it is critically important that any information associated with such processing be classified and treated as extremely sensitive.
- (U) If, after these procedures have been followed, the Ombudsperson assesses that further review is required, the Ombudsperson will pursue such review as contemplated in Section 2 of the Ombudsperson Mechanism, including its provision that when the request relates to the compatibility of surveillance with U.S. law, the Privacy Shield Ombudsperson will be able to cooperate with one of the independent oversight bodies with investigatory powers, in accordance with applicable classified procedures.

(U) Example of Coordination to Review Sufficient Requests: Sufficient requests are processed in accordance with applicable classified procedures. The following example of how coordination might occur is drawn from unclassified descriptions of applicable existing oversight processes and is included for illustrative purposes:

- Once a sufficient request received by the Ombudsperson is determined to pertain to a particular Intelligence Community agency or element, the request will be reviewed by that agency or element's Civil Liberties and Privacy Office and forwarded to relevant officials, such as compliance officials, to conduct further reviews and to report their findings. The Office of the Intelligence Community Inspector General will be informed of all such requests and can conduct an independent review of any allegation of improper signals intelligence activity at any time.

If a review finds a violation of law, executive order, or presidential directive, then appropriate measures would be taken to remedy the violation, including any required purge of data or recall of intelligence reporting. In addition, the incident would be reported through established incident reporting channels. Depending on the type of incident, this could include reporting to the Office of the Director of National Intelligence, the Department of Defense, the President's Intelligence Oversight Board, the Privacy and Civil Liberties' Oversight Board, the specific Inspector General for the agency or element in question, and intelligence oversight committees in Congress. If the incident involves a violation of any

authority or approval granted by the Foreign Intelligence Surveillance Court, including for example, a violation of FISA Section 702 targeting procedures or minimization procedures, the violation would be reported to the Court.

If the Ombudsperson determined an issue arose under the jurisdiction of another oversight authority, such as another Inspector General or the Privacy and Civil Liberties Oversight Board, the Ombudsperson can further refer the matter to them.

The Ombudsperson would engage this oversight structure to ensure the incident is remedied.

(U) Responding to Sufficient Requests:

(U) Where there is no compliance incident detected, or where any compliance incident discovered has been remedied, EB/CIP prepares a letter for the Ombudsperson's signature certifying that U.S. laws, statutes, executive orders, presidential directives, and agency policies/regulations described in the ODNI letters incorporated into the Framework have been complied with, or, in the event of non-compliance, that such non-compliance has been remedied. Once signed, EB/CIP transmits the response to the CHB via the Sharepoint portal.

(U) Improper Influence:

(U) Should the Ombudsperson have reason to believe an entity or individual inside or outside the Department is attempting to assert improper influence over the Ombudsperson Mechanism generally or over a specific request, the Ombudsperson will immediately report any and all such improper conduct to the Secretary, who will take any actions he deems appropriate to ensure that the Ombudsperson carries out its function objectively and free from improper influence that is liable to have an effect on the response to be provided. The Ombudsperson can also refer any such attempts to the appropriate Inspector General. Suspected criminal activity is reportable to Diplomatic Security and/or the Department of Justice, consistent with applicable Department guidance.

(U) Closing a File:

(U) Before marking a request as completed, EB/CIP ensures that all pertinent documentation is recorded in the appropriate system.