BRENNAN
CENTER
FOR JUSTICE

Brennan Center for Justice
at New York University School of Law

161 Avenue of the Americas
12th Floor
New York, New York 10013
212.998.6730 Fax 212.995.4550
www.brennancenter.org

August 28, 2014

Re: Notice PCLOB 2014-04, Sunshine Act Meeting

To the members of the Privacy and Civil Liberties Oversight Board:

The Brennan Center for Justice previously submitted comments on the NSA's surveillance activities under both Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act (FISA), part of the FISA Amendments Act of 2008 (FAA). We also provided both written and oral testimony for the PCLOB's March 19, 2014 public hearing focused on Section 702, and offered further written commentary on April 11, 2014. The following comments are offered on the mid-term and long-term agenda of the Privacy and Civil Liberties Oversight Board.

Attorney General Guidelines and DIOG

As discussed in detail in our 2011 report, *Domestic Intelligence: New Powers, New Risks*, the Brennan Center has serious concerns about overbroad and unnecessary investigative authorities given to the FBI through the Attorney General's Guidelines. The Guidelines, which set out the basic rules under which the FBI initiates and runs domestic investigations, are promulgated and revised by the Attorney General. Successive Bush administration revisions to the Guidelines increased the FBI's latitude. In particular, the last and most far-reaching of these changes, issued by Attorney General Mukasey in 2008, authorizes FBI agents to initiate "assessments" of individuals and organizations without any factual predicate – meaning that a person can be investigated even when there is no objective evidentiary basis to suspect him or her of wrongdoing. FBI agents need only a subjective belief that the investigation will serve a legitimate law enforcement or national security purpose in order to justify an assessment.

FBI agents are permitted to use a number of highly intrusive investigative techniques during assessments, such as recruiting and tasking informants; conducting physical surveillance, as well as overt and covert FBI interviews; and issuing Grand Jury subpoenas for telephone subscriber information. The Guidelines impose no time limits on such investigations, and even allow agents to conduct assessments of individuals simply to determine if they could be turned into FBI informants.

The vast majority of assessments uncover no evidence of wrongdoing. Of more than 82,000 assessments opened in the first two years that the FBI had this authority, less than 3,400 found information worth pursuing in preliminary or full investigations.

The FBI retains all information collected during assessments for decades, even where the subjects are found to be innocent of any crime or threatening behavior. Given the FBI's focus on counterterrorism as its predominant mission, it is likely that a significant portion of these assessments are justified as counterterrorism efforts. The FBI's eGuardian program, implemented shortly after the 2008 amendments to the Guidelines, also encourages law enforcement and public reporting of harmless and commonplace activities like photography as potential indicators of terrorism. And the FBI's "no terrorism lead goes uncovered" policy ensures that even the most specious reports will be investigated as potential terrorism assessments.

Authorizing tens of thousands of investigations of individuals and organizations not suspected of wrongdoing unjustifiably and unnecessarily casts a cloud of suspicion over innocent people, violates their privacy and wastes security resources. It also opens the door to civil rights and civil liberties abuses. When agents are not required to adhere to objective evidentiary standards before opening assessments, they are far more likely to target individuals based on racial, ethnic, or religious bias, or to suppress First Amendment activity, just as they did until the 1970s when Attorney General Edward Levi issued the first set of Guidelines to prevent such practices.

There is evidence such abuse already has occurred. The FBI's Domestic Investigations and Operations Guide (DIOG), which implements the Guidelines, specifically authorizes FBI agents to collect and track racial and ethnic "behaviors" and map racial and ethnic communities. There would be no need for the FBI to identify or map these communities unless it intends to treat them differently. The Justice Department Guidance Regarding the Use of Race by Federal Law Enforcement Agencies, which the Guidelines incorporate by reference, serves as no barrier to race-based counterterrorism investigations, because it specifically exempts national security and border integrity investigations from its prohibitions. Many believe, with good reason, that the national security exemption to the Justice Department's racial profiling restrictions tacitly authorizes law enforcement to target Arab, Middle Eastern, Muslim, Sikh, and Asian communities for disparate treatment in investigations and intelligence gathering.

Moreover, flawed FBI training materials make it more likely that Muslims will continue to be inappropriately targeted for investigation. As detailed in the Brennan Center's report, *Rethinking Radicalization*, the FBI's operating philosophy identifies normal Muslim religious behavior - like growing a beard, wearing traditional Islamic clothing and frequent attendance at a mosque – as grounds for suspicion.

In 2010 the Justice Department Inspector General issued a report criticizing the FBI for characterizing non-violent civil disobedience as terrorism, and for opening and continuing investigations against domestic advocacy groups based on "factually weak" predicates and "speculative, after-the-fact rationalizations." These investigations took

place prior to the 2008 Guidelines changes, and the IG made the troubling observation that "some of the violations of policy we found in this review would not be violations if they occurred today." The IG suggested that Congress might wish to examine this issue.

The Brennan Center urges the PCLOB to recommend that the Attorney General's Guidelines be revised to prohibit the FBI from using intrusive investigative techniques against individuals or organizations unless there is a reasonable factual basis to suspect they are engaging, or preparing to engage in criminal activity, including espionage or terrorist activities. Investigations should be limited to the least intrusive means necessary, based on the seriousness of the crime or threat suspected, and the weight of the evidence establishing suspicion. Further, the PCLOB should recommend the Justice Department amend its Guidance Regarding the Use of Race by prohibiting federal law enforcement from using race, ethnicity, religion, national origin or First Amendment-protected activity as a factor in initiating investigations, assessments, or surveillance, absent a specific suspect description.

Fusion Centers and Suspicious Activity Reporting

In December 2013, the Brennan Center published a report on *National Security and Local Police* that identified serious problems with the national information sharing system designed for fusion centers and Suspicious Activity Reporting (SAR) programs. These programs were encouraged and funded by the Departments of Justice and Homeland Security as part of its efforts to ensure that information relevant to terrorism is shared between local police and federal law enforcement agencies. While better sharing of relevant information can assist counterterrorism efforts, we found that the current setup allows state and local agencies to collect and share troves of information without any connection to criminal activity. Vague and expansive definitions of "suspicious activity" lead officers to fall back on their own biases and preconceptions and open the door to a flood of irrelevant information. Unsurprisingly, a 2012 bipartisan Senate report that reviewed 13 months of fusion center reporting concluded that such reporting has endangered citizens' civil rights and Privacy Act protections while yielding little, if any, counterterrorism benefit.

Standard for Reporting "Suspicious Activity"

Police departments collect suspicious activity reports (SARs), which are shared through state or regional "fusion centers" on a federally administered computer network (the Information Sharing Environment or ISE) managed by the Office of the Director of National Intelligence. State and local police officers determine which SARS to place on the ISE according to federal guidance (the "Functional Standard"). A 2009 revision to the standards for information included in the ISE made some important changes, including a ban on using religion and ethnicity as factors that create suspicion and an acknowledgment that First Amendment protected activities, such as photography, should not be reported unless they have some connection to terrorism. But the revised policy also explicitly instructed state and local law enforcement to share reports of suspicious activity even if there is no reasonable suspicion of criminal activity. The absence of a

reasonable suspicion requirement substantially undermines the prohibitions on improper reporting. Recent SARs filed by fusion centers in Boston, California, and Washington, DC, demonstrate that despite the 2009 changes, many fusion centers are still reporting on innocent First Amendment activity and singling out Middle Eastern men for scrutiny without suspicion of criminal activity.

The FBI has developed its own system for compiling suspicious activity reports, known as eGuardian. The repository functions like the ISE, but the Bureau follows its own rules for acquiring and retaining information. The FBI rules are even more permissive than the low standard for the ISE. According to the Government Accountability Office, the FBI's definition of "suspicious activity" is notably broader than the ISE standard and the FBI permits longer data retention. The Bureau may keep a SAR for up to five years, after which it may be retained for another 30 years in the FBI's case management system.

The Brennan Center urges the PCLOB to recommend that the collection and sharing of information through SAR programs like the ISE and eGuardian should be governed by a single, consistent standard that adequately protects privacy. In particular, data should only be collected and shared through SAR programs if it gives rise to a reasonable suspicion of criminal activity. Reasonable suspicion is the traditional bar for most investigatory activities. Cadets in every police academy in the country are familiar with it. It is also not a particularly high bar to clear – officers need only point to specific facts that evince more than an inchoate and unparticularized suspicion or hunch. Applying such a filter would be minimally burdensome to law enforcement and would go a long way toward preventing irrelevant, unfounded, and biased-based reports from coursing through government databases for years to come.

Lack of Oversight

The Brennan Center's research also reveals a profound lack of oversight and accountability for fusion center activities. There are very few mechanisms to ensure that even the lax rules that exist are followed. DHS formerly took the position that because fusion centers were state enterprises, anti-commandeering principles prevented it from dictating what they can and cannot do. In 2010, however, the Department required each fusion center to craft a privacy policy and designate a "privacy officer" as a condition of receiving DHS funds. But with few exceptions, there is no independent oversight or auditing for compliance with these policies (e.g., by auditing the SARs that police include in the ISE or eGuardian). State and local governments have rarely taken the initiative to fill the gap left by DHS. The result is that nobody is systematically ensuring that the loose rules for SARs are not being abused.

The Brennan Center encourages the PCLOB to draw attention to this oversight deficit and to recommend that the federal government, as a major funder and primary driver for the establishment of fusion centers, take responsibility for ensuring that they are properly overseen and to mitigate the privacy and civil rights concerns raised by their activities. As a condition of future federal funding, fusion centers should be required to fully

implement their privacy policies and demonstrate compliance through regular, independent audits available to the public.

Executive Order 12333

Compared to the legal regime governing NSA operations in the United States, the legal framework for the agency's overseas intelligence activities, which are regulated by Executive Order ("EO") 12333, have received relatively little attention. The scope of NSA activities under EO 12333 is less well understood than some of the other programs that have come to light in the past year, but appears to be of far greater magnitude than domestic programs.

While overseas surveillance operations have traditionally not been regulated by U.S. law, changes in technology and developments in the international legal framework make it imperative that the PCLOB pay close attention to these issues.

Implications for U.S. Persons

To begin with, the explosion in communications technology and international travel means that large quantities of American communications are almost inevitably picked up in foreign operations. Americans are vulnerable to the NSA's collection practices under EO 12333 as long as they communicate with a foreigner, or if their communications (even if purely domestic) are transmitted to or stored on a server overseas. As a result, the NSA potentially sweeps up the personal and sensitive information of millions of innocent Americans and, unlike the better-known operations under Section 215 of the PATRIOT Act and Section 702 of the FISA Amendments Act, there is absolutely no judicial involvement in these operations.

Americans' information collected under EO 12333 may be retained and disseminated by the government for a wide variety of purposes. While the Attorney General is required to promulgate procedures to minimize such retention and dissemination, these procedures are not public. They are, however, widely understood to be more permissive than those used to protect Americans from the exercise of other surveillance authorities such as Section 215 of the PATRIOT Act and Section 702 of the FAA. Indeed, it was recently reported that the NSA shares billions of phone, e-mail and internet records with nearly two dozen other government agencies.

There is little Congressional oversight of this broad swath of activities. Although Congress must be kept "fully and currently informed" about "significant" intelligence activities, the executive branch has wide latitude to determine what information it shares with Congress. Senator Dianne Feinstein, the Chair of the Senate Intelligence Committee, has admitted that her Committee exercises little oversight in this realm.

International Law Constraints

Surveillance operations conducted under EO 12333 also implicate the privacy rights of

non-Americans. The order authorizes signals intelligence operations aimed at collecting information for a broad range of "foreign intelligence" purposes. "Foreign intelligence" is defined as any "information relating to the capabilities, intentions and activities of foreign powers, organizations or persons." This definition could encompass *all* the communications and personal data of a foreign national living anywhere outside the U.S., since they contain information relating to the "activities of … foreign persons." The broad power to spy on the ordinary citizens of foreign countries potentially violates the U.S.'s human rights obligations, including the prohibition against "arbitrary and unlawful interference" with a person's privacy under Article 17 of the International Covenant on Civil and Political Rights.

The Brennan Center recommends that the PCLOB investigate and report on the scope of operations carried out under EO 12333 in order to provide a public with a properly unclassified description of such programs. As part of the effort to increase transparency, the Board should facilitate the declassification of any internal executive memoranda or documents that contain significant legal interpretations of EO 12333, including minimization procedures. The PCLOB should also scrutinize whether EO 12333 is consistent with the Fourth Amendment and widely accepted understandings of the International Covenant on Civil and Political Rights, to which the U.S. is a party. In particular, the Board should make recommendations for narrowing the definition of "foreign intelligence" to ensure that the government only collects, retains and shares information that is likely to significantly implicate national security. With regard to the international human rights issues, the Brennan Center recommends that the Board review whether the NSA's large scale collection practices constitute "arbitrary or unlawful" interferences with the right to privacy under Article 17 of the ICCPR. Finally, the Brennan Center recommends that the PCLOB provide suggestions for how EO 12333 programs may be brought under congressional and judicial oversight.

PPD-28

In January 2014, the President issued Presidential Policy Directive ("PPD") 28 in an attempt to address criticisms about the NSA's surveillance programs. While the Directive is long on privacy rhetoric, a close examination of its provisions raises serious questions about whether it reflects any real change in U.S. policy and practice.

PPD-28 conspicuously fails to limit the scope of foreign intelligence collection. The Directive reiterates the government's authority to collect communications and personal data for "foreign intelligence" and "counterintelligence" purposes, and adopts the extremely broad definitions of these purposes under EO 12333.

The Directive purports to restrict the *use* of "signals intelligence collected in bulk" to detecting and countering: (1) threats of espionage and other activities directed by foreign powers against the U.S.; (2) terrorist threats to U.S.; (3) threats to U.S. posed by weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied armed forces; and (6) transnational criminal threats. However, the Directive adopts a narrow definition of bulk collection, effectively exempting a range of large scale surveillance programs

from these restrictions.[1]

Finally, PPD-28 extends restrictions on the sharing and dissemination of personal information under EO 12333 to non-U.S. persons. However, EO 12333's minimization rules are extremely permissive, and their privacy value may be even more illusory to non-U.S. persons. For example, EO 12333 allows the NSA to retain and share "information that constitutes foreign intelligence," which in turn refers to "information relating to the capabilities, intentions or activities of foreign … persons." As explained above, such a definition effectively allows the NSA to retain and share *all* information linked to a non-U.S. person.

PPD-28 encourages the Board to provide the President with a report on the Directive which focuses on strengthening it to place meaningful limits on the collection of signals intelligence to protect the rights of both U.S. and non-U.S. persons. At a minimum, the PCLOB should recommend that PPD-28's restrictions on the *use* of information should also apply to how such information is *collected* in the first place. The Board should also suggest that such limits be extended to *all* large scale programmatic surveillance activities, including those that collect signals intelligence with the use of discriminants.

[1] Surveillance programs that collect large quantities of signals intelligence data with the use of "discriminants" like specific identifiers and selection terms fall outside PPD-28's definition of bulk collection. Presidential Policy Directive/PPD-28, §2(5), 2014 WL 187435 (January 17, 2014), *available at* *http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities*. However, the NSA is permitted to use extremely broad selectors, effectively sweeping up reams of information about Americans and non-Americans. For example, a selector such as "Pakistani Taliban" would result in the collection of a huge amount of communications - the overwhelming majority of which would have no legitimate intelligence value.