Statement of The Constitution Project
Submitted to the Privacy and Civil Liberties Oversight Board
October 30, 2012

The Constitution Project (TCP) submits this statement for the record for the first public meeting of the Privacy and Civil Liberties Oversight Board (PCLOB). TCP has long urged that Congress and the President create and staff an independent board to review the privacy and civil liberties implications of national security programs. TCP welcomes the convening of this Board, whose creation is long overdue, and appreciates the opportunity to share our recommendations for issues on which the PCLOB should focus its attention.

TCP is a constitutional watchdog based in Washington, DC that brings together respected leaders from across the political spectrum and works with them to develop consensus recommendations for policy reforms that promote constitutional safeguards. We then conduct strategic public education campaigns and advocacy efforts to further these policy recommendations. Through our Liberty and Security Committee, which was created in the aftermath of the 9/11 attacks, TCP works to ensure that our nation protects both our national security and our civil liberties. As part of these efforts, TCP has continued to advocate in favor of establishing an independent board with meaningful oversight authority over national security policies and programs to ensure that they incorporate robust safeguards for privacy and civil liberties.

Now that four members have been confirmed to serve on the PCLOB, TCP urges the Board to begin this important work. The statute creating the PCLOB as an independent entity provides that the Board shall review proposed "legislation, regulations, and policies related to

efforts to protect the Nation from terrorism" and provide advice to ensure that privacy and civil liberties are properly safeguarded. The statute also provides the PCLOB with authority to conduct oversight of the implementation of programs, and instructs that the Board "shall continually review" programs that relate to "efforts to protect the Nation from terrorism to ensure that privacy and civil liberties are protected."

The issues worthy of the Board's attention are numerous, and we do not attempt to provide an exhaustive list. Rather, TCP suggests that the PCLOB should begin by focusing on the following three priority areas where independent review and oversight are most urgently needed: (1) programs whose very existence is classified and that remain largely if not entirely unknown to the public; (2) the targeted killing or drone program; and (3) programs that involve intelligence collection on, and government monitoring of, U.S. persons and their personal information. This final category is a broad one, ranging from surveillance conducted under the Foreign Intelligence Surveillance Act (FISA) Amendments Act to data mining programs.

National Security Programs Whose Existence is Classified

First and foremost, the PCLOB should examine classified national security programs whose existence has not been confirmed by the government and those that are completely unknown to the public. The members of the PCLOB have statutory authority to review classified information. The need for oversight and independent review of national security programs is greatest where the very existence of the program is considered classified, and where there has been no opportunity for public comment and debate, and at most, limited disclosure through the media. This category likely includes various government programs for conducting surveillance of potential terrorism suspects, such as the NSA warrantless

wiretapping program (or "Terrorist Surveillance Program") before its public disclosure in December 2005. Thus, the Board should begin its work by surveying all departments, agencies and other elements of the executive branch to identify all counter-terrorism programs being proposed or already in operation, and should prioritize review of programs whose very existence is considered classified. Where the public is not even aware of the existence of programs and is therefore unable to press for accountability – such as through Freedom Of Information Act requests and calls for action by Congress – the need for independent PCLOB review is particularly acute.

Targeted Killing or Drone Program

Second, it is critical that the PCLOB review the executive branch's "playbook" for its targeted killing or drone program. This program has now been publicly acknowledged and the guidelines and policies for the use of drones form a key component of U.S. counter-terrorism efforts. However, these policies are being developed by the administration in secret, making any meaningful public oversight impossible and effectively shielding the program from public accountability. Independent PCLOB review is especially important for the policy governing cases in which the targets may be U.S. persons, who clearly have constitutional rights. Although we do not know how many individuals targeted under the program have been U.S. persons, news accounts indicate that nearly 3,000 people have now been killed in drone attacks. In a speech last spring, Attorney General Holder asserted that the administration could satisfy due process in such cases – and in fact did – even without relying on judicial review. But those controversial claims have never been subject to adequate, independent review, judicial or otherwise. Indeed, a lawsuit seeking to challenge the placement of U.S. citizen Anwar al-

Awlaki on the list of individuals the CIA was authorized to kill under this program was dismissed on procedural grounds. Review of the targeted killing program should rank high on the PCLOB's priority list.

Programs Involving Intelligence Collection on and/or Monitoring of U.S. Persons and Their Information

Finally, government programs that involve intelligence collection on, and monitoring of, U.S. persons and their private information should be a priority for PCLOB review. This is a broad category that includes surveillance conducted pursuant to both the FISA Amendments Act and the Patriot Act, cybersecurity programs, data mining programs, and the federal role in fusion centers. All of these programs – including their roles and the extent to which they are subject to meaningful oversight – should be independently reviewed to ensure that privacy and civil liberties are protected.

The surveillance program being conducted under the FISA Amendments Act (FAA) of 2008 is in urgent need of review by the PCLOB. The FAA vastly increased the government's powers to conduct surveillance of international communications without individualized judicial review, and severely limited the scope of review performed by the Foreign Intelligence Surveillance Court when the court's approval is actually required. The statute permits the collection of communications involving U.S. persons and people located within the United States so long as these individuals are not the targets of the surveillance. Earlier this year, in response to a request from Senators Wyden and Udall for the number of Americans whose communications have been intercepted under the Act's authority, the Inspector General of the Intelligence Community stated that "an estimate was beyond the capacity" of the NSA. If even

an *estimate* is impracticable, then Americans can and should be concerned about the scope of this electronic surveillance. The PCLOB should review the actual operation of this surveillance program and assess how many Americans have had their communications intercepted – lawfully and unlawfully. The Board should also examine the average number of communications involving any particular American that have been "incidentally" intercepted; the maximum number of such interceptions for any given U.S. person; and the number of communications to or from the United States that have been intercepted – all to demonstrate the extent to which large quantities of data may be collected on any particular U.S. person even if he or she is not a target.[1] PCLOB review can help determine whether and to what extent additional civil liberties safeguards should be incorporated into this program.

Similarly, the government's surveillance authorities under the Patriot Act should be reviewed by the PCLOB. This review should assess whether the Act – particularly the three sunsetting provisions and the national security letter (NSL) authority – incorporates adequate safeguards for privacy and civil liberties. In seeking reauthorization of the Patriot Act's business records, lone wolf and roving wiretap provisions, the executive branch has asserted that classified information demonstrates the continued need for these authorities. The PCLOB can and should review such classified information to determine whether increased safeguards for privacy rights and civil liberties can be incorporated without unduly jeopardizing the investigations being conducted.[2] In addition, as part of its oversight function, the PCLOB should review the actual classified operation of the surveillance authorities to assess the extent of

[1] *See* The Constitution Project, *Report on the FISA Amendments Act of 2008* (2012), http://constitutionproject.org/pdf/fisaamendmentsactreport_9612.pdf.
[2] *See* The Constitution Project, *Statement on Reforming the Patriot Act* (2009), http://www.constitutionproject.org/pdf/340.pdf.

compliance with existing rules. Previous reviews by the Inspector General for the FBI have found numerous instances in which such rules were not followed.

The PCLOB should also focus its attention on new cybersecurity programs being developed by the federal government. This includes programs that may be developed to implement potential legislation providing for information-sharing between the government and the private sector, those designed to carry out a potential executive order on cybersecurity, and any other government cybersecurity programs. The risks to privacy rights and civil liberties and the need for PCLOB review are greatest for programs in which the private sector may share individuals' personal information – including personally identifiable information and the content of private communications – with the government as part of cyber threat information. The PCLOB can and should play a critical role in assessing these risks and recommending safeguards to mitigate them.

Some have questioned whether cybersecurity falls within the jurisdiction of the PCLOB, because the Board's authorizing statute speaks in terms of programs designed "to protect the Nation from terrorism," and the term "cybersecurity" encompasses a wide variety of threats and potential aggressors beyond terrorists. However, as Secretary of Defense Panetta made clear in his speech in New York City earlier this month, terrorist groups pose cybersecurity threats, and our nation is now preparing for a "cyber-terrorist attack" as a critical part of efforts to safeguard our nation's cyber networks. Thus, counter-terrorism is a key part of newly developing cybersecurity programs, and therefore such programs should easily fall within the PCLOB's jurisdiction. Moreover, both of the lead cybersecurity bills currently pending in the Senate would clarify the PCLOB's authority to provide oversight of such programs. Thus, in its

recent report *Recommendations for the Implementation of a Comprehensive and Constitutional Cybersecurity Policy*,[3] TCP's Liberty and Security Committee specifically called for PCLOB oversight of government cybersecurity programs "to ensure that constitutional safeguards are implemented and followed across federal agencies and private industry."

Another area in which the PCLOB can play a valuable role is in assessing government data mining programs that are used for counter-terrorism investigations. These are programs that rely upon computing technology to examine large amounts of data to reveal patterns and identify potential wrongdoing. While data mining may be able to provide a valuable investigative tool in some contexts, the benefits for counter-terrorism are unclear because of the particular difficulties of developing a predictive model or algorithm to identify potential terrorist suspects. Data mining also poses real threats to Americans' privacy rights and civil liberties due to the risks of "false positives." As TCP's Liberty and Security Committee urged in our 2010 report *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age*,[4] once established, the PCLOB "would have the independence and authority to effectively review data mining Plans – particularly highly sensitive Plans – where Congress cannot do so, and to oversee their execution, for instance by reviewing and approving data acquisitions and data mining activities."

A final program in this category that merits PCLOB review is the fusion center program. There are now 77 fusion centers, information-sharing hubs designed to pool the knowledge and

[3] The Constitution Project, *Recommendations for the Implementation of a Comprehensive and Constitutional Cybersecurity Policy* (2012), http://www.constitutionproject.org/pdf/TCPCybersecurityReport.pdf.
[4] The Constitution Project, *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age* (2010), http://www.constitutionproject.org/pdf/DataMiningPublication.pdf.

expertise of federal, state and local law enforcement. As demonstrated in TCP's recent report, *Recommendations for Fusion Centers: Preserving Privacy & Civil Liberties While Protecting Against Crime & Terrorism*,[5] the fusion center system, as currently run, enhances the risk that Americans might be deemed suspicious simply because of their race, religion, or political views. The report released earlier this month by the Permanent Subcommittee on Investigations of the Senate Committee on Homeland Security and Governmental Affairs further demonstrates the real risks to privacy and civil liberties posed by fusion center operations. Among the 25 recommendations in TCP's report, we urge that the federal government should conduct an independent study of fusion center performance and of the centers' impact on civil liberties. Now that it has come into existence, the PCLOB can and should perform this critical task.

Conclusion

There are, of course, numerous additional national security and counter-terrorism programs that fall within the PCLOB's jurisdiction and would benefit from its independent review. TCP outlines the categories above to highlight the areas we believe should be priorities for the Board's focus. In large part this is because the programs described above have not been subject to rigorous oversight or public accountability. With the Board's access to classified information, it can play a critical role in assessing these programs.

[5] The Constitution Project, *Recommendations for Fusion Centers: Preserving Privacy & Civil Liberties While Protecting Against Crime & Terrorism* (2012), http://constitutionproject.org/pdf/fusioncenterreport.pdf.

TCP appreciates this opportunity to provide comments on areas upon which the Board will focus its attention.

Respectfully submitted,

Sharon Bradford Franklin
Senior Counsel
The Constitution Project
1200 18th Street, NW
Suite 1000
Washington, DC 20036
202-580-6920
www.constitutionproject.org