September 30, 2013

M/OAA/P
USAID/Washington
1300 Pennsylvania Avenue, NW
Washington, DC  20523
M.OAA.RuleMaking@usaid.gov

RE: RIN 0412-AA71—Partner Vetting in USAID Assistance

To whom it may concern:

The ACLU is a non-profit, non-partisan organization committed to protecting the civil liberties guaranteed by the United States Constitution. We are writing to respond to the United States Agency for International Development’s (USAID) request for comments on proposed amendments to the regulations governing the administration of USAID assistance awards to implement a Partner Vetting System (PVS) pilot program.

The ACLU has submitted public comments to USAID and the Department of State six times since 2007, raising concerns with the PVS and the Risk Analysis and Management (RAM) program (see copies attached). While some of our comments have been addressed, the ACLU continues to have fundamental concerns with aspects of these programs.

The proposed PVS rule raises significant privacy and due process issues, with serious consequences for the associational rights of applicants and the individuals and organizations with whom they work. The standards employed by the program are wholly undefined. Moreover, whether the program is necessary in the first place remains an unanswered question, especially given that we are aware of no public reports of USAID resources being diverted to terrorist organizations or individuals.

PVS Puts Individuals’ Privacy at Risk

The information USAID is seeking under PVS is highly personal and confidential—including individuals’ social security and government-issued identification numbers, mailing and email addresses, and information concerning national origin and citizenship. The Background on the proposed rule notes that the process will “protect sensitive information from disclosure,” but the proposed rule does not specify what those measures may be and how they will protect against disclosure or misuse.

---

This is a very real concern. PVS has been designed to enable USAID to use the Terrorist Screening Center (TSC) to determine whether “key individuals” associated with an award applicant are “terrorists, supporters of terrorists or affiliated with terrorists.” The Background on the proposed rule also states that the program is concerned with identifying those “linked to terrorist activities.” The TSC, administered by the FBI, houses the Terrorist Screening Database (TSDB, known as the Watchlist), the U.S. government’s consolidated terrorist list. The names on the list are secret and are not limited to individuals and entities designated as terrorists by the U.S. government, which are already identified on lists that are made public by the Departments of Treasury and State. It also includes unpublished, secret intelligence databases that are centralized at the TSC.

The TSC shares information in the TSDB with thousands of law enforcement officers at every level of government and with 22 foreign governments. In some cases the information is shared with private-sector individuals.

Congress has expressed that USAID must disclose what will happen to the information it collects. The Senate Committee on Appropriations report accompanying the Fiscal Year 2014 State and Foreign Operations Appropriations Bill from July 2013 states: “All individuals and organizations being vetted should be provided with full disclosure of how information will be stored and used by the U.S. Government, including how information regarding a ‘positive match’ will be handled and how to appeal such a match.”

This month the ACLU released a report, Unleashed and Unaccountable: The FBI’s Unchecked Abuse of Authority, that documents abuse of surveillance powers. This includes the collection of vast amounts of personal information in various databases, including the TSDB, for data-mining programs. And in light of the ongoing revelations about the abuse of power of the National Security Agency and its sweeping collection of data, these concerns are more acute.

Yet, despite concerns expressed by Congress and evidence of data-mining misuse, the rulemaking is not clear about how the privacy of the highly personal and confidential data submitted to USAID during the vetting process will be treated and protected. There is no information on how long USAID will store the information, whether the data will be scrubbed, and under what criteria and timeline.

Even more worrisome, there is no assurance that the TSDB (or other government entities) will not store information about individuals whom USAID vets. Since TSC shares information with

---

2 “Key individuals” is a very broad category: “principal officers of the organization’s governing body,” “the principal officer and deputy principal officer of the organization,” “the program manager or chief of party,” and “any other person with significant responsibilities for administration of the USG-financed activities or resources.” Id. Based on USAID estimates of 44,000 applications for awards during the pilot program alone, a massive number of people will be subject to this screening. See id. at 53378.

3 Id. at 53376. The ACLU objects to this practice just as it objects to any requirement that non-governmental organizations that are USAID applicants must screen their own employees against such lists.

4 Id.


other agencies and foreign governments, individuals who submit their personal data have reason to be concerned about the privacy of their information. If the PVS pilot program is to go forward, USAID must spell out how the personal data will be secured and the very real possibility of abuse will be prevented.

Finally, by requiring all applicants to submit data for vetting, USAID will be collecting much more information than it needs to meet the program’s purpose. By collecting what amounts to bulk data on the designated applicant pool, USAID will create concern about the actual purpose of the information collection and could create the appearance of intelligence gathering in communities USAID serves.

**PVS Fails to Meet Due Process Requirements**

If an applicant does not pass vetting, it will be ineligible for a USAID award. Yet at a fundamental level, the PVS process lacks transparency and fails to provide notice—required by due process—of what association or activity may result in denial of a USAID award. For example, there is no definition for what is considered an “affiliation” or “linkage” to terrorism or who is considered a “supporter” that would trigger negative vetting result and result in serious harms to the applicant and key individuals.

The Fifth Amendment’s due process protections also require notice of the basis for an adverse determination and an opportunity to contest that determination in a meaningful way. The proposed rule’s broad discretion to restrict information released on why an applicant does not pass vetting and the very limited appeals process it provides violate this basic standard.

The proposed rule does not provide adequate notice of the basis for an adverse finding. Instead, an applicant will only be notified that it has failed vetting and the vetting official will only inform the applicant of information that USAID decides is “releasable,” “consistent with applicable law and Executive Orders, and with the concurrence of relevant agencies.”

7 This is no assurance that an applicant will receive any explanation stating the reason it has not passed vetting. In fact, the applicant may not even be informed about which key individual caused it to fail vetting, which would make it impossible to effectively seek reconsideration, because the applicant would have to guess what error or misconstruction of evidence may be the basis for an adverse determination, and thus what evidence it should submit in its defense. Without meaningful notice and an explanation, an applicant cannot clear up misunderstandings or rebut erroneous inferences. Giving applicants the specific reasons for a decision increases the likelihood of error correction.

The proposed regulations allow for an appeals process of sorts, in which a denied applicant can ask for the decision to be reconsidered and provide more information.

---

7 78 Fed. Reg. at 53379.
8 This would be similar to the government’s policy to refuse to confirm or deny information about a person’s status on the No Fly List. We have argued that the policy is not constitutional in the context of the No Fly List, and similar concerns apply to USAID vetting. See Press Release, American Civil Liberties Union, Federal Court Sides with ACLU in No Fly List Lawsuit (Aug. 29, 2013), https://www.aclu.org/national-security/federal-court-sides-aclu-no-fly-list-lawsuit.
is unlikely to provide for a meaningful opportunity to challenge the vetting results and in fact, does not even comport with the more robust, but still insufficient, notice and procedures required in the national security context for organizations the government designates as terrorists.

These problems are exacerbated by the fact that there are significant concerns about the accuracy and management of the TSDB. A May 2009 audit by the Department of Justice’s Office of Inspector General (OIG) documented the high error rate and dysfunction of the TSDB. The audit revealed a process so disorganized that “the actual number of individuals the FBI nominated to the terrorist watchlist since its inception is unknown.” Many entries contained information “unrelated to terrorism.” The audit also found that the FBI:

- Failed to timely remove closed cases from the records in 72 percent of cases;
- Failed to appropriately modify outdated records in 67 percent of cases; and
- Failed to remove terrorism classification in 35 percent of cases, even though many of these should have been removed from the Watchlist entirely.

The known high error rate for listings in the TSDB (with no effective means for challenging the fact that one is on the list) means that USAID vetting has a high risk of erroneous outcomes, and therefore erroneous deprivation of rights.

The fact that classified or sensitive national security information may be involved is not enough to deny applicants notice of the reasons for a negative vetting finding, or an adequate opportunity to respond, given the enormity of the issues at stake for applicants and the humanitarian goals they seek to fulfill.

**Inadequate Due Process Harms Applicants’ and Individuals’ Associational Rights**

Not only does PVS threaten privacy rights, but it may harm applicants’ and individuals’ interest in freedom from false government stigmatization. Being denied a USAID award on the basis of alleged association with terrorism (no matter how attenuated or unsupported) can seriously damage applicants’ standing with the public and associations in their community and the communities they seek to serve. This can have a secondary effect of discouraging private donors, depriving the organization of the resources it needs to carry out non-USAID activities. These problems are in addition to the fact that the organization cannot legally partner with USAID. The key individual whose name matches the TSDB (if that information is released by USAID) may lose his or her job or contract and face an inability to conduct similar work in the future, all without a meaningful opportunity to clear his or her name.

---


11 *Id.* at 1.

12 *Id.* at vi.

13 *Id.* at 36.

14 *Id.* at 23.

15 *Id.* at 54.
PVS Lacks Demonstrated Need

Finally, the ACLU continues to believe that USAID and the Department of State have failed to demonstrate that implementing PVS or RAM is necessary and that the government’s goals of assuring that grantee organizations will abide by the law cannot be achieved through much less burdensome means, such as by requiring recipients to abide by anti-terrorism financing and asset-control laws, statutes, and executive orders, in their use of grant funds.

* * *

We hope these comments are useful in your continued review of the proposed rule and we strongly urge you not to go forward with the PVS pilot program. Please contact Legislative Counsel Dena Sher at 202-715-0829 or dsher@dcaclu.org if you have questions or comments about our concerns.

Sincerely,

Laura W. Murphy
Director, Washington Legislative Office

Dena Sher
Legislative Counsel

Hina Shamsi
Director, National Security Project