

December 19, 2011

Mr. Edward H. Vazquez  
U.S. Department of State  
2201 C Street, NW  
SA-15, Room 3200  
Washington, D.C. 20520

VIA EMAIL: VazquezEH@State.gov

RE: Notice of Proposed Information Collection, Federal Register Vol. 76, No. 203, page 65317, Risk Analysis and Management, Form DS-4184

Dear Mr. Vazquez,

The comments provided herein are submitted in response to the announcement published in the Federal Register (Vol. 76, No. 203, page 65317) on October 20, 2011, by the Department of State (DOS) proposing to collect information from contractors, subcontractors, grantees and subgrantees in order to vet individuals against non-public U.S. government databases. This information collection effort, previously known as the Partner Vetting System, is now referred to in the announcement as the Risk Analysis and Management (RAM) program. In response to the four elements in the announcement, below please find our comments on DOS' RAM program and the information collection form DS-4184.

**Necessity of the proposed information collection for the proper performance of DOS functions**

As leading nongovernmental organizations working to support democracy worldwide, we are committed to ensuring that the funds we receive from donors, including the U.S. Department of State and USAID, are not provided to entities or individuals associated with terrorism and that we are otherwise in full compliance with Executive Order 13224 and other requirements. As such, we verify that individuals and entities to which we provide material or financial support do not appear on the U.S. Treasury Department's master list of Specially Designated Nationals and Blocked Persons, the United Nations Security Council (UNSC) sanctions committee list, and, as appropriate, other related lists of individuals designated as supporting terrorist activity. Since establishing relationships with respected local partners is a cornerstone of our programs, we also employ common practices beyond list checking to assess their integrity and reputation, such as site visits, one-on-one discussions, and prior experience with other groups. These efforts enable us and other international NGOs to have an in-depth understanding of the local partners with whom we work and to develop relationships of mutual trust. As noted in our previous comments

to similar Federal Register announcements on the Partner Vetting System,<sup>1</sup> we remain concerned that the collection of personal information on local partners for the specific purpose of vetting against U.S. government intelligence databases may jeopardize that trust and our neutrality since it could be perceived as intelligence gathering.

In accordance with the FY2010 Department of State, Foreign Operations and Related Programs Appropriations Act, we understand and appreciate the recent efforts of DOS and USAID to jointly pilot a Partner Vetting System in five countries to determine the risk of foreign assistance funds being diverted to terrorist entities. Although not yet implemented, the approach seems more methodical than the original design, appears to have taken into consideration several of the NGO community's previous comments and, importantly, allows for an evaluation of its effectiveness prior to any expansion outside the five pilot countries. However, the criteria by which awards would be subject to vetting requirements in a risk-based model remain unclear.

As the PVS/RAM pilot has been described as a joint effort by DOS and USAID, the NGO community's expectation is that the two agencies would use the same information collection form and mechanisms. The DOS information collection form, DS-4184, differs significantly from USAID's form for the pilot countries (AID 500-13, Partner Information Form). For example, the DS-4184 requires the collection of additional personal data (e.g., gender, phone numbers and social security numbers). This represents an increased and unnecessary burden on recipients, particularly those that receive funding from both Federal agencies in the same countries. In addition, the DS-4184 uses the term "key personnel" whereas USAID uses the term "key individual," which will lead to confusion since "key personnel" has a specific definition under USAID awards. This definition is not synonymous with "key individual." The form also references "technical assistance," and since the purpose of many of our programs is to provide technical assistance to local partners (groups) and beneficiaries (individuals), it is unclear if the recipients of such assistance are to be vetted as well.

Of particular note, the DS-4184 requires the collection of information for programs in Afghanistan, which is not one of the five pilot countries (Guatemala, Kenya, Lebanon, the Philippines and Ukraine). The statutory requirement limits the collection of information to the pilot countries.

Therefore, we believe that the level of detail required in DS-4184 and the specific inclusion of Afghanistan are not necessary for the proper performance of DOS functions with respect to the pilot vetting program. In addition, we remain concerned that since host country nationals would be vetted against a list/database maintained by U.S. Government intelligence agencies, the erroneous perception overseas then would be that U.S. NGOs are direct, intelligence-gathering sources for the U.S. Government. While the NGO community is willing to comply with all lawful conditions established on the receipt of federal funds and does not condone or support terrorism in any way, it must of necessity avoid becoming part of – or being perceived as to become a part of – the U.S. Government's national security/intelligence apparatus. The trust-

---

<sup>1</sup> See comments submitted on: August 27, 2007, September 18, 2007, September 21, 2007, November 30, 2007, March 3, 2009 and August 16, 2011

building process is central to our work as are the basic principles of NGOs and their programs – neutrality, impartiality and independence. In this regard, we are most troubled that personal information provided by organizations for the purpose of vetting could be used to supplement the data contained in the U.S. government intelligence database. This supports the concern that the vetting process is being used as an intelligence-gathering effort and could jeopardize the safety and security of our employees and local partners, particularly in politically sensitive environments.

### **Accuracy of burden estimate**

Given the level of detail required in the DS-4184, the burden estimate of 75 minutes for completion seems underestimated. However, it is not possible to fully assess the burden estimate since the parameters of the pilot program have not yet been made public. It is unclear, for example, whether the risk-based model of the pilot program will require vetting for all awards or only certain types of programs and the criteria by which the risk will be assessed. Further, the burden estimate focuses solely on the number of hours to complete the form. In order to collect, retain and manage the vast amount of personal data in a secure manner would require significant resources (human and financial). The financial and administrative burden this would place on non-profit organizations has not been considered to date or reflected in the burden estimates.

### **Quality, utility and clarity of the information to be collected**

Comments on the quality, utility and clarity of the information are noted under the section on necessity. In sum, the format of the DS-4184 is confusing; it introduces another form for the collection of information for the joint pilot program with USAID; utilizes different terminology than USAID for the joint pilot program; and it include references to provision of “technical assistance,” implying the vetting of and disclosure of personal information on program beneficiaries to DOS.

### **Reporting burden is minimized for respondents, including use of automated collection techniques**

Two distinct information collection forms for the joint DOS/USAID pilot program increases, rather than minimizes, the reporting burden on respondents. With respect to automated collection techniques, the announcement states that the information will be collected through mail, fax or electric submission. It does not specify whether DOS has identified or developed a universal, secure method by which organizations can transmit the information, thereby placing the burden of (and cost for) safeguarding and transmitting personal information on recipients. In an era of cyber attacks from foreign governments, hacking and identity theft, the safeguarding of sensitive personal information must be a priority for DOS prior to the implementation of the information collection system.

Thank you for your consideration of our comments. We look forward to further dialogue on a system that will contribute to ensuring U.S. government funds are not provided to terrorists and,

at the same time, that will enable us to maintain the critical principles of neutrality, trust and independence of our work and to minimize risk to our local partners and employees.

Sincerely,



Shawna Bader-Blau  
Executive Director  
American Center for International Labor  
Solidarity AFL-CIO (Solidarity Center)



John D. Sullivan  
Executive Director  
Center for International Private Enterprise



David J. Kramer  
President  
Freedom House



Lorne W. Craner  
President  
International Republican Institute



Kenneth D. Wollack  
President  
National Democratic Institute