February 16, 2012

Department of State Desk Officer
Office of Information and Regulatory Affairs
Office of Management and Budget

Re: Department of State Notice of Proposed Information Collection: DS-4184, OMB Control #1405-XXXX, Risk Analysis and Management, Vol. 77 Fed. Reg. No. 11, page 2601

To Whom It May Concern:

The Constitution Project ("TCP") respectfully submits the following written comments regarding the State Department's (the "Department") proposed information collection. TCP is a national, bipartisan think tank that develops consensus-based solutions to some of the most difficult constitutional challenges of our time. TCP works on criminal justice and rule of law issues by undertaking scholarship, policy reform, and public education initiatives. TCP creates committees of experts and practitioners from across the political spectrum and works with them to promote and safeguard America's founding charter. TCP's Liberty and Security Committee, formed in the aftermath of September 11th, works to ensure that we promote both our national security and Americans' civil liberties. In September 2009, TCP's Liberty and Security Committee released its report, *Reforming the Material Support Laws: Constitutional Concerns Presented by Prohibitions on Material Support to "Terrorist Organizations,"*[1] which contains a series of recommendations for reform of the material support laws. TCP appreciates the opportunity to comment on the Department's proposed information collection.

On December 19, 2011, TCP submitted a comment letter, which we have attached as an Appendix, to the Department in response to its October 20, 2011 "60-Day Notice of Proposed Information Collection: DS-4184, Risk Management and Analysis (RAM)."[2] TCP expressed its concerns over the Department's proposed information collection, or Partner Vetting System ("PVS"), and urged that the constitutional standards of due process and privacy be applied throughout the PVS process. As we noted in *Reforming the Material Support Laws: Constitutional Concerns Presented by*

[1] The Constitution Project's Liberty and Security Committee, *Reforming the Material Support Laws: Constitutional Concerns Presented by Prohibitions on Material Support to "Terrorist Organizations"* (Nov. 17, 2009), http://www.constitutionproject.org/pdf/355.pdf.
[2] 60-Day Notice of Proposed Information Collection: DS-4184, Risk Management and Analysis (RAM), 76 Fed. Reg. 65317 (Oct. 20, 2011).

Prohibitions on Material Support to "Terrorist Organizations," cutting off support of terrorist activity is an important and legitimate part of the United States' counter-terrorism strategy, but this must be done consistently with constitutional safeguards.[3] Thus, while it may be appropriate for the government to investigate key players receiving government humanitarian aid to prevent the diversion of these resources to terrorist groups, it is critical to incorporate adequate processes and controls to safeguard constitutional rights and values, including due process and privacy. This must include meaningful procedures for challenges as well as robust safeguards for collected personally identifiable information ("PII").

The Department's "Supporting Statement for Paperwork Reduction Act Submission — Risk Analysis and Management: OMB Number 1405-XXXX" makes the following responses to the comments filed by organizations including TCP:

- The Department plans on incorporating due process procedures into the program "to the extent that it is possible consistent with the handling and protection of classified information. Organizations will be given a reason of denial of contract or grant due to vetting, with the maximum amount of detail allowed by the nature and source of the information that led to the decision, and they will be allowed to challenge the decision."[4]
- The Department will not use the collected data to create a "'blacklist' of organizations and/or individuals who will be barred from seeking U.S. government contracts and grants . . . . [T]he PII collected will be used for screening the key personnel of a particular contract or grant and will not prejudice an organization's eligibility to bid on other projects."[5]
- The Department states that the "only information about any individual being vetted that would be retained by other agencies beyond USAID would be if those individuals were already identified in the data holdings of the other agency."[6]

The Department's response to TCP's concerns is inadequate and unhelpful. No details are provided on the extent and nature of due process procedures that the Department plans to incorporate or on the methods by which the use of PII will be limited. As TCP expressed in its December 19, 2011 letter, the Department and the U.S. Agency for International Development ("USAID") have yet to publish any details about their respective PVS pilot programs. This is contrary to the provision in the House of Representatives' Committee Report for the appropriation authorizing the pilot. It said that USAID would "work constructively with implementing organizations, including contractors and nongovernmental organizations, to frame a commonsense system, without undermining foreign policy and development goals."[7] As the appropriation[8] itself requires that the pilot apply equally to USAID and the Department, it is incumbent on the Department to engage in this dialog *before* proposing to collect the personal information of NGO workers and officials. This position was endorsed in 2010 by the President's Advisory Council on Faith-Based and Neighborhood Partnerships, which said, "PVS as currently designed would significantly harm partnerships with local communities and compromises the safety of U.S. PVO [private voluntary organizations] personnel."[9] This lack of information on how the PVS pilot program will be run makes it extremely difficult to comment on whether the

---

[3] TCP, *Reforming the Material Support Laws*: supra note 1.
[4] Department of State, Supporting Statement for Paperwork Reduction Act Submission — Risk Analysis and Management: OMB Number 1405-XXXX at 5 (2012).
[5] *Id.* at 4.
[6] *Id.*
[7] H.R. Rep. No. 111-187 (2010).
[8] Consolidated Appropriations Act, 2010, Pub. L. No. 111-117, 123 Stat. 3034 (2009).
[9] President's Advisory Council on Faith-Based and Neighborhood Partnerships, A New Era of Partnerships: Report of Recommendations to the President at 100 (2010), http://www.whitehouse.gov/sites/default/files/microsites/ofbnp-council-final-report.pdf.

Department's program may be expected to include adequate privacy and due process protections. The Department has not yet made a proposal that can be considered adequate.

First, given the lack of specifics in the Department's filings it is unclear whether an applicant will receive adequate due process if his or her application is denied. To satisfy constitutional due process, an applicant who is denied access to the Department's funds because of a match to a U.S. government database should (1) receive an explanation stating the reason for denial and (2) have a meaningful opportunity to challenge the findings of his or her presence in the database. While the Department states that it will provide due process, it qualifies this by (1) limiting it "to the extent possible consistent with the handling and protection of classified information," and (2) limiting the explanation of denial by the "nature and source of information." As TCP noted in its December 19, 2011 letter and the report *Promoting Accuracy and Fairness in the Use of Government Watch Lists*,[10] many individuals are placed on watch lists due to mistaken identity or inadequate justification for inclusion. Although we recognize that it would defeat the purpose of watch lists to provide individuals notice that they have been placed on such a list, individuals should still have a meaningful opportunity for redress when they are harmed as a result of an erroneous listing.[11] Moreover, the potential involvement of classified information should not prevent the Department from establishing procedures that provide meaningful due process. As TCP has explained repeatedly in seeking reform of the state secrets privilege and in combatting the problem of overclassification of government documents, there are many options available to provide substitutes for classified documents. For example, the government may be able to provide a redacted version of a document or a summary, thereby enabling the information to be presented in an unclassified manner that would still permit a robust and meaningful opportunity to challenge. The Department can — and should — develop alternatives to work around classified documents.

Second, although the Department states that the collected data will not be used to create a "blacklist" of organizations and individuals who will be barred from seeking U.S. government contracts and grants, if the Department does not provide adequate due process for challenging a grant denial or the finding of his or her presence in a U.S. government database, the Department will be in effect blacklisting these applicants. Though the Department states that a denial in one instance does not bar an applicant from bidding on other projects, if that applicant cannot effectively challenge the initial denial, then he or she is likely to be denied on any future application. For a system to be fair, it must include a meaningful mechanism for redressing errors.

Third, the Department's response to TCP's privacy concerns completely ignores our suggestions that the PVS pilot program should (1) impose use restrictions on personal data obtained by the government and (2) properly encrypt and secure this data. Although the Department states that the only information that will be retained by other agencies beyond USAID would be data regarding individuals who were already present in other agency databases, the Department did not assuage our concerns that this data would not be used for any other purpose than to verify that government grant recipients are not funneling money to terrorist organizations. As TCP noted in its December 19, 2011 letter and the report *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age*, government access to or use of personal information in databases can violate privacy rights.[12] Private parties and other government agencies should not receive access to this information. Also, data from approved applicants should not be retained and stored in intelligence databases, and investigative files should not be

---

[10] The Constitution Project's Liberty and Security Committee, *Promoting Accuracy and Fairness in the Use of Government Watch Lists* (Mar. 6, 2007), http://www.constitutionproject.org/pdf/53.pdf.
[11] *See id.* at 5.
[12] The Constitution Project's Liberty and Security Committee, *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age* (Dec. 12, 2010), http://www.constitutionproject.org/pdf/DataMiningPublication.pdf.

opened on any approved applicant without reasonable suspicion. Applicants seeking to provide humanitarian aid should not have to worry about how the U.S. government uses their personal and private data.

Furthermore, the Department ignored TCP's concerns regarding the encryption and security of data collected under the PVS pilot program. This is particularly troubling due to the handling of data security during the West Bank and Gaza PVS program. As TCP noted in its December 19, 2011 letter, the Government Accountability Office and the State Department Office of the Inspector General found that personal information submitted by applicants was vulnerable to security breaches.[13] Had those data been accessed, applicants' privacy rights would have been violated.

TCP appreciates the opportunity to offer our views on the PVS pilot program. We share the goal of protecting USAID and Department resources from diversion to terrorist groups. We urge the Office of Management and Budget ("OMB") to reject or modify the information collection proposed by the Department. Particularly because the State Department has not yet released any details on the PVS pilot program, they have not demonstrated that they plan to include adequate due process protections or privacy safeguards. In the alternative, we recommend that OMB conduct a "listening session" with representatives of the nonprofit sector before taking any action. In addition to heeding the wishes of Congress, this is needed because the Department's "Supporting Statement for Paperwork Reduction Act Submission—Risk Analysis and Management: OMB Number 1405-XXXX" made no changes or adjustments to address serious and legitimate concerns.

Sincerely,

Sharon Bradford Franklin
Senior Counsel

Jessica Neiterman
Fried Frank Fellow

The Constitution Project
1200 18th Street, NW, Suite 1000
Washington, DC 20036

[13] *See* David Gootnick, United States Government Accountability Office, *Foreign Assistance: Recent Improvements Made, but USAID Should Do More to Help Ensure Aid is Not Provided for Terrorist Activities in West Bank and Gaza* 17 (Sept. 29, 2006), http://www.gao.gov/new.items/d061062r.pdf.

THE CONSTITUTION PROJECT

Safeguarding Liberty, Justice and the Rule of Law

December 19, 2011

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

Re: Notice of Proposed Information Collection: DS-4184, Risk Management and Analysis (RAM), Vol. 76 Fed. Reg. No. 203, page 65317

Dear Mr. Vazquez,

The Constitution Project ("TCP") respectfully submits the following written comments regarding the State Department's (the "Department") proposed information collection. TCP is a national, bipartisan think tank that develops consensus-based solutions to some of the most difficult constitutional challenges of our time. TCP works on criminal justice and rule of law issues by undertaking scholarship, policy reform, and public education initiatives. TCP creates committees of experts and practitioners from across the political spectrum and works with them to promote and safeguard America's founding charter. TCP's Liberty and Security Committee, formed in the aftermath of September 11th, works to ensure that we promote both our national security and Americans' civil liberties. In September 2009, TCP's Liberty and Security Committee released its report *Reforming the Material Support Laws: Constitutional Concerns Presented by Prohibitions on Material Support to "Terrorist Organizations,"*[1] which contains a series of recommendations for reform of the material support laws. TCP appreciates the opportunity to comment on the Department's proposed information collection.

The Partner Vetting System ("PVS") will be used "to conduct screening to ensure that State funded activities do not provide support to entities or individuals deemed to be a risk to national security."[2] The Department proposes to collect information from contractors, subcontractors, grantees, and sub-grantees regarding their directors, officers, or key employees. The Department will compare this information to information stored in "commercial, public, and U.S. government databases to determine the risk that the applying organization, entity or individual might use Department funds or programs to benefit terrorist entities."[3]

---

[1] The Constitution Project's Liberty and Security Committee, *Reforming the Material Support Laws: Constitutional Concerns Presented by Prohibitions on Material Support to "Terrorist Organizations"* (Nov. 17, 2009), http://www.constitutionproject.org/pdf/355.pdf.

[2] 60-Day Notice of Proposed Information Collection: DS-4184, Risk Management and Analysis (RAM), 76 Fed. Reg. 65317 (Oct. 20, 2011).

[3] *Id.*

As we noted in *Reforming the Material Support Laws: Constitutional Concerns Presented by Prohibitions on Material Support to "Terrorist Organizations*, cutting off support of terrorist activity is an important and legitimate part of the United States' counter-terrorism strategy.[4] However, while it may be appropriate for the government to investigate key players receiving government humanitarian aid to prevent the diversion of these resources to terrorist groups, it is critical to incorporate adequate processes and controls to safeguard constitutional rights and values, including due process and privacy. While we recognize that the PVS pilot program will apply to both U.S. persons and non-U.S. persons[5] and that a non-U.S. person would not be entitled to the same protections under the United States' Constitution and laws, we urge that these constitutional standards be applied throughout the PVS process.

Due Process Concerns

The Fifth and Fourteenth Amendments to the U.S. Constitution provide that a person shall not be deprived of life, liberty, or property without due process of law.[6] For the PVS pilot program to provide adequate due process protections, the system must be transparent and curative. In other words, if an applicant is denied access to the Department's funds because of a match to a U.S. government database, the applicant should (1) receive an explanation stating the reason for denial and (2) have a meaningful opportunity to challenge the finding or his or her presence in the database. We note that the Department and USAID have not yet published any details about the PVS pilot program. We urge that robust due process safeguards be afforded to denied applicants.

Due process principles require transparency because the government only remains accountable to its people when the people know that the government follows its own rules and know how the government reaches its decisions. As TCP's Liberty and Security Committee noted in the report *Promoting Accuracy and Fairness in the Use of Government Watch Lists*,[7] many individuals are placed on watch lists due to mistaken identity or inadequate justification for inclusion. Although we recognize that it would defeat the purpose of watch lists to provide individuals notice that they have been placed on such a list, individuals should still have a meaningful opportunity for redress when they are harmed as a result of an erroneous listing.[8] For most watch lists there is currently no effective way to challenge one's inclusion or adverse decisions resulting from such listings.

During the PVS process, grant applicants' personal data will be compared with information contained in commercial, public, and U.S. government databases, including many of the aforementioned inaccurate and unreliable watch lists. Without a system in place to notify applicants of the reason why their grant requests have been denied and to challenge the Department's decision, many organizations will be unfairly denied humanitarian aid. For a system to be fair, it must have some mechanism for redressing errors. The PVS application process should not serve as a means to blacklist certain individuals or organizations from receiving USAID funds just because their names appear on a watch list.

Privacy Concerns

Under the PVS pilot program, the U.S. government will collect personal data – including name, government identification number, date of birth, country of citizenship, home address, email address, employer information, and job title – from applicants who wish to use federal money for humanitarian purposes overseas. Although this data collection may be appropriate to adequately investigate whether people receiving government funds funnel money to terrorist organizations, this data should not be used for any other purpose. The PVS pilot program should (1) impose use restrictions on personal data and (2) properly encrypt and secure this data.

First, use restrictions are essential to protect privacy rights. In TCP's Liberty and Security Committee's report, *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age*, we noted that

---

[4] TCP, *Reforming the Material Support Laws:* supra note 1.

[5] The term "U.S. person" refers to both United States citizens and legal residents of the United States.

[6] U.S. Const. amend. V and XIV.

[7] The Constitution Project's Liberty and Security Committee, *Promoting Accuracy and Fairness in the Use of Government Watch Lists* (Mar. 6, 2007), http://www.constitutionproject.org/pdf/53.pdf.

[8] *See id.* at 5.

government access to or use of personal information in databases can violate privacy rights.[9] Any program involving the collection or use of personal data should ensure privacy protection through use restrictions. Data collected during the PVS pilot program should not be used for any other purpose than to verify that USAID recipients are not funneling money to terrorist organizations. Private parties and other government agencies should not receive access to this information. Most importantly, data from approved applicants should not be retained and stored in intelligence databases; investigative files should not be opened on any approved applicant without reasonable suspicion. Humanitarian applicants should not have to worry about how the U.S. government uses their personal and private data.

Second, all data collected under the PVS pilot program should be properly encrypted and secured. As TCP's data mining report recommends, "[a]dministrative and technical measures should be employed together to reduce the potential for abuse or misuse of personal data."[10] The Government Accountability Office and the State Department Office of the Inspector General found that personal information submitted by applicants to the West Bank and Gaza PVS program had been kept in unlocked file cabinets and was otherwise vulnerable to security breaches.[11] Had those data been accessed, applicants' privacy rights would have been violated. The Department should take steps to prevent any future security lapses in the new PVS pilot program.

Conclusion

TCP appreciates the opportunity to offer our view on the PVS pilot program. We share the goal of protecting USAID and Department resources from diversion to terrorist groups. We encourage the Department to create a PVS pilot program that respects applicants' due process rights, provides transparency to the greatest extent possible, and protects applicants' personal and private data.

Sincerely,

Sharon Bradford Franklin
Senior Counsel

Jessica Neiterman
Legal Fellow

The Constitution Project
1200 18th Street, NW, Suite 1000
Washington, DC 20036

[9] The Constitution Project's Liberty and Security Committee, *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age* (Dec. 12, 2010), http://www.constitutionproject.org/pdf/DataMiningPublication.pdf.
[10] *See id.* at 26.
[11] *See* David Gootnick, United States Government Accountability Office, *Foreign Assistance: Recent Improvements Made, but USAID Should Do More to Help Ensure Aid Is Not Provided for Terrorist Activities in West Bank and Gaza* 17 (Sept. 29, 2006), http://www.gao.gov/new.items/d061062r.pdf.