Archived Content

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

April 12, 2019

MEMORANDUM FOR: Christopher Logan
Acting Assistant Administrator for Grant Programs
Federal Emergency Management Agency

FROM: Jonathan R. Cantor
Acting Chief Privacy Officer

SUBJECT: Privacy Compliance Review of the Countering Violent Extremism Grant Program

Purpose

Beginning in 2016, the former Office of Community Partnerships and the Federal Emergency Management Agency (FEMA) managed the Countering Violent Extremism Grant Program (CVEGP) to fulfill a congressional mandate to help states and local communities prepare for, prevent, and respond to emergent threats from violent extremism. The CVEGP Privacy Impact Assessment[1] (PIA) discussed the privacy risks of the first iteration of this grant program. The PIA noted that the Department of Homeland Security's (DHS) Privacy Office (PRIV) would initiate a Privacy Compliance Review[2] (PCR) to provide recommendations for improving the privacy protections inherent in deploying a security review process as part of the grant application process. While the CVEGP was not renewed from its initial 2016 funding, the findings reflected in this report serve as lessons learned that the Office of Terrorism Prevention Partnerships should carefully consider for any future CVEGP iterations, if applicable. Further, the FEMA Grant Programs Directorate, as the administrator and manager of DHS grants, should fully implement PRIV recommendations to improve privacy protections for any future grant program that includes a security review.

Background

The CVEGP was the DHS mechanism for fulfilling a congressional mandate[3] to help states and local communities prepare for, prevent, and respond to emergent threats from violent extremism. To properly execute the grant program and help adhere to congressional intent, DHS sought to

---

[1] DHS/ALL/PIA-057 *available at*: https://www.dhs.gov/sites/default/files/publications/privacy-pia-all-057-cve-december2016.pdf.

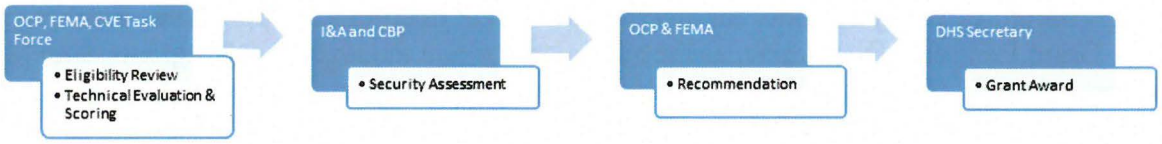
[2] DHS Privacy Policy Instruction 047-01-004 for Privacy Compliance Reviews, *available at*: https://www.dhs.gov/publication/dhs-privacy-policy-instruction-047-01-004-privacy-compliance-reviews.

[3] Section 543 of the 2016 Consolidated Appropriations Act provides DHS $50 million to counter emergent threats from violent extremism and from complex, coordinated terrorist attacks (*see*: https://www.congress.gov/bill/114th-congress/house-bill/2029/text). The Joint Explanatory Statement provides $10 million for a DHS CVE Initiative to help states and local communities prepare for, prevent, and respond to emergent threats from violent extremism (*see*: 161 Cong. Rec. H10162 (2015), https://www.congress.gov/crec/2015/12/17/CREC-2015-12-17-bk3.pdf).

ensure that grant recipients did not use Countering Violent Extremism (CVE) grant funding to support terrorism, engage in other criminal activities, or otherwise conduct or support activities that were contrary to the intent of the program.

DHS issued a Notice of Funding Opportunity[4] (NOFO) on July 6, 2016, that outlined the Department's objectives to develop new efforts and expand existing efforts at the community level to counter violet extremist recruitment and radicalization to violence. The NOFO clearly articulated eligibility criteria as well as information on how applications would be evaluated, selected for funding, and managed after the award. The NOFO also noted that as the principal senior official overseeing the application of the CVEGP, the DHS Secretary had the discretion to consider any necessary factors, such as applicant screening and other mission criteria, in the awarding of funding and the full execution of the grant program. The DHS Secretary was the final approval authority regarding the issuance of CVE Grant awards.

The DHS Office for Community Partnerships[5] (OCP), together with the Federal Emergency Management Agency (FEMA), administered the CVEGP application process. Final award decision authority rested with the DHS Secretary. The CVEGP application process was (and continues to be) managed through FEMA's Non-Disaster Grants System (ND Grants),[6] in accordance with standard procedures. Management of roles and responsibilities for this program is partially addressed in a December 6, 2016, FEMA memorandum from the Deputy Administrator, Protection and National Preparedness. In the memorandum, FEMA's Grant Programs Directorate had financial responsibilities and OCP had programmatic responsibilities. Responses received during the PCR clarify that OCP responsibilities included general management and oversight, as well as reviewing grant applications for eligibility and considering information and analysis contained in security assessments. Security assessments were coordinated and produced by DHS's Office of Intelligence and Analysis (I&A), with the assistance of U.S. Customs and Border Protection (CBP).



The CVE grant program's NOFO formally announced the program in July 2016, and solicited applications from state, local, and tribal governments; non-profit organizations; and institutions of higher education. The NOFO explained that the program seeks to:

---

[4] DHS-16-OCP-132-00-01, FY 2016 Countering Violent Extremism Grants, *available at*: https://www.grants.gov/web/grants/view-opportunity.html?oppId=285773.

[5] On November 30, 2017, Acting Secretary of Homeland Security Elaine Duke announced the transition of the Office for Community Partnerships (OCP) to the Office of Terrorism Prevention Partnerships (OTPP). This report addresses OCP as that was the responsible office during the course of this PCR. However, any action items or best practice recommendations from this PCR should be addressed by OTPP.

[6] Privacy compliance documentation for this system includes DHS/FEMA/PIA-013 Grant Management Program (*see*: https://www.dhs.gov/sites/default/files/publications/privacy_pia_FEMA_GrantManagementPrograms_February2015.pdf) and DHS/FEMA-004 Non-Disaster Grant Management Information Files, 80 Fed. Reg. 13404 (Mar. 13, 2015) (*see*: https://www.gpo.gov/fdsys/pkg/FR-2015-03-13/html/2015-05799.htm).

> "…develop new efforts and expand existing efforts at the community level to counter violent extremist recruitment and radicalization to violence by funding activities that enhance the resilience of communities being targeted by violent extremists for recruitment, provide alternatives to individuals who have started down a road to violent extremism, and that create or amplify alternative messages to terrorist/violent extremist recruitment and radicalization efforts. In addition, the CVE Grant Program seeks to develop and support efforts by U.S.-based entities that are broadly countering violent extremists' on-line recruitment efforts aimed at U.S.-based individuals".[7]

The NOFO clearly defined the process to complete the application, as well as eligibility criteria and the application selection process. The NOFO also stated that the "Secretary retains the discretion to consider other factors and information in addition to those included in the recommendations" developed by OCP and FEMA.[8]

The application process for the CVEGP is managed through FEMA's Non-Disaster Grants System[9] (ND Grants), which maintains grant applicant information that FEMA uses to manage and administer the grant application process. Applicants provided information to DHS through ND Grants when applying for a grant under the CVEGP. The information provided by grant applicants was used to both determine eligibility and quality, as well as to conduct security reviews of eligible grant applications from non-governmental and non-academic grant applications that were recommended for selection to the Secretary. OCP and FEMA presented the Secretary with recommendations of eligible and quality applications, including those that underwent a security review. The totality of each application was considered by the Secretary in making award decisions.

Due to privacy sensitivities involved in administering and managing the security review process, OCP and FEMA, in coordination with the DHS Privacy Office (PRIV), published the CVEGP Privacy Impact Assessment[10] (PIA) in December 2016. The PIA outlines the unique and heightened privacy risks associated with DHS reviewing and vetting grant applicants for security concerns. This risk-based review process considered information and analysis resulting from security assessments conducted by DHS I&A, with assistance from CBP, in an effort to gauge the likelihood that applicants would use CVE grant funding to, either directly or indirectly, engage in or support terrorism or other criminal behavior. Due to this security review process, the PIA noted that the DHS Privacy Office would initiate a Privacy Compliance Review (PCR) ninety days from the start of the grant application review period to assess the program's compliance with established privacy protections, as well as provide recommendations for improving the privacy protections inherent in deploying a security review process.

---

[7] NOFO, page 2.
[8] NOFO, page 13.
[9] DHS/FEMA/PIA-013 Grant Management Programs, February 2015, *available at*: https://www.dhs.gov/sites/default/files/publications/privacy_pia_FEMA_GrantManagementPrograms_February2015.pdf.
[10] DHS/ALL/PIA-057 Countering Violent Extremism Grant Program, December 2016, *available at:* https://www.dhs.gov/sites/default/files/publications/privacy-pia-all-057-cve-december2016.pdf.

Scope and Methodology

Scope

In January 2017, the DHS Privacy Office initiated a PCR of the CVEGP by issuing an action memorandum to the OCP Director. In order to meet the PCR's objective of determining the program's degree of compliance with the CVEGP PIA and DHS Privacy Policy Guidance Memoranda 2008-01/Privacy Policy Directive 140-06,[11] the DHS Privacy Office included a comprehensive list of questions with the memo as well as a request for supporting documents. Over the next several months, the DHS Privacy Office collected responses and supporting documents from and held informative meetings with OCP, as well as FEMA, CBP, I&A, the Office of General Counsel (OGC), and other DHS subject matter experts.

However, since the launch of this PCR, the Department made several decisions that affected the PCR's final product to include the reorganization of OCP and non-renewal of CVE grant funds. As a result, the DHS Privacy Office now considers the findings herein to be best practices for any future iterations of the CVEGP *or any DHS grant program* that incorporates security reviews as part of its award making process.

The DHS Privacy Office greatly appreciates the cooperation provided by all affected offices and regrets that competing priorities slowed our ability to finalize this review in a more efficient manner.

Methodology

To meet the PCR's objective, the DHS Privacy Office reviewed existing privacy compliance documentation; developed and submitted an extensive questionnaire designed to build a comprehensive understanding of the eligibility and vetting process employed by OCP and FEMA; reviewed OCP, FEMA, I&A, CBP, and OGC responses to said questionnaire, including all supporting documentation; and conducted additional fact finding interviews with subject matter experts.

The DHS Privacy office conducted this PCR in coordination with personnel from OCP; FEMA's Grant Programs Directorate, Office of Chief Counsel, and Privacy Office; and I&A and CBP's Privacy Offices. The findings detailed in this report reflect conclusions reached by the DHS Privacy Office based on an assessment of CVEGP-related compliance documents, exchanges with DHS personnel, and an analysis of documents, responses, discussions, and other information received in response to the initiation of this PCR. The report is organized according to the relevant DHS Fair Information Practice Principles (FIPPs) as articulated in DHS Privacy Policy Directive 140-06.

---

[11] Privacy Policy Guidance Memorandum 2008-01/Privacy Policy Directive 140-06, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security, December 2008, *available at:* https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.

In conducting this PCR, the DHS Privacy Office:

- Reviewed DHS/ALL/PIA-057 and FEMA/PIA-013 Grant Management Programs PIA;[12]
- Reviewed July 2016 CVEGP NOFO, as well as briefing materials and Frequently Asked Questions (FAQs);
- Developed and distributed an initial questionnaire to OCP;
- Resubmitted questionnaire to supporting DHS Components: FEMA, CBP, and I&A;
- Reviewed I&A provided Security Review Reports of reviewed applicants;
- Reviewed initial questionnaire responses and supporting documentation;
- Developed follow-up questionnaires and conducted additional discussions with OCP, FEMA, I&A, and CBP personnel to better understand responses;
- Drafted an initial PCR Report for OCP, FEMA, CBP, and I&A review;
- Responded to any comments received, as appropriate; and
- Drafted and published the final PCR Report.

III. Recommendations and Findings

A. Summary of Recommendations

The DHS Privacy Office acknowledges the important objectives of the CVEGP and the relationship of these objectives to the DHS mission. It is also important to acknowledge that programmatic responsibility was placed with OCP, an office that does not have an assigned Privacy Point of Contact, nor an embedded individual with substantial privacy experience that could have provided timely insight and direction regarding privacy matters, which are obligations for all DHS programs. DHS Privacy Policy[13] applies throughout DHS and requires implementation of DHS privacy policies and procedures established by the Chief Privacy Officer.

The DHS Privacy Office discusses our findings as lessons learned from reviewing the CVEGP and offers the following recommendations to help guide OCP, and other offices programmatically responsible for grant programs, to better protect privacy, foster adherence to the FIPPs, and promote compliance with published PIAs and DHS policies. While this PCR focused on OCP given their programmatic responsibilities for the CVEGP, FEMA, as the administrator and manager of the DHS grants system and the party with the most influence on how other DHS offices utilize this system, should consider the findings and fully implement the recommendations herein. The DHS Privacy Office notes greater transparency and "privacy by design" could lead to better compliance and a better ability to address any concerns from the public.

While the CVEGP was not funded after 2017, the DHS Privacy Office notes that the lessons learned from this PCR concerning OCP's programmatic management and the partnership with FEMA should be considered in the future by *any* DHS program using the FEMA Grants system:

---

[12] DHS/FEMA/PIA-013 Grant Management Programs, February 2015, *available at*: https://www.dhs.gov/sites/default/files/publications/privacy_pia_FEMA_GrantManagementPrograms_February2015.pdf.
[13] Privacy Policy and Compliance Directive 047-01, July 2011, *available at*: https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-directive-047-01_0.pdf.

1. Clearly state in all public grant documents, including but not limited to the PIA, NOFO, and FAQs, information regarding all eligibility and review criteria, including DHS's option to conduct security reviews and the DHS Secretary's discretion to consider other criteria.
2. Provide explicit notice to eligible applicants that DHS may conduct a security review, including specifically who or what may be reviewed, and give sufficient time to consent to said review or to withdraw from consideration.
3. Clearly specify that the main applicant and any sub-applicant may undergo a security review. Consider stating in the NOFO that it is the applicant's responsibility to inform sub-applicant(s) of the grant review criteria including the possibility of a security review.

B. Findings

Requirement: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).

Review: The DHS Privacy Office reviewed the publicly available information associated with the CVE grant program, including its PIA, NOFO, Fact Sheet, FAQs, webinar presentation and transcript, the FEMA ND Grants System of Records Notice[14] (SORN), and responses to the PCR questionnaire.

Finding: Sufficient and timely notice regarding the potential to undergo a security review as part of the CVE grant review process, and what that would entail, was not provided.

As outlined in Privacy Policy Directive 140-06, "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security,"[15] the Department must provide transparency for how it handles PII through various mechanisms, including PIAs, SORNs, Privacy Notices, general notices, Privacy Compliance Reviews, and through the Freedom of Information Act (FOIA). OCP could have better employed each of these instruments in a timely matter to operate the CVE grant program as transparently as possible.

The July 2016 NOFO stated that DHS would take a risk-based selection approach in granting funds. Section E regarding application evaluation criteria, specifically stated the following may be considered in determining the eligibility of any applicant:

(1) financial stability;
(2) quality of management systems and ability to meet management standards;
(3) history of performance in managing federal award;
(4) reports and findings from audits; and
(5) ability to effectively implement statutory, regulatory, or other requirements.

Once deemed eligible, technically reviewed, and scored, OCP and FEMA compiled a recommendations package for the Secretary. Final funding determinations were made by the DHS Secretary. Only briefly did the NOFO indicate that additional factors may be considered

---

[14] *See*: https://www.govinfo.gov/content/pkg/FR-2015-03-13/html/2015-05799.htm.
[15] *See*: Privacy Policy Guidance Memorandum 2008-01/Privacy Policy Directive 140-06, December 2008, *available at*: https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.

when it stated that the "Secretary retains the discretion to consider other factors and information in addition to those included in the recommendations;" however, this wording does not refer specifically to a security review.[16] While these "other factors and information" are not otherwise defined in public documents, OCP and FEMA considered these to include security-based reviews. As the OGC analysis on the authority to conduct security reviews noted, the Secretary possesses the legal authority to conduct such reviews. Under DHS Privacy Policy,[17] however, the DHS Privacy Office strongly encourages greater transparency when doing so whenever possible.

Other information was made public at the time of the NOFO, including the FY2016 CVE Grants Fact Sheet,[18] which included similar language regarding the Secretary's discretion to "consider other factors and information" when making an award determination. The FY2016 CVE Grants FAQs[19] and webinar,[20] however, did not mention any additional review criteria.

DHS/ALL/PIA-057 is more transparent when it stated that the DHS Secretary has the discretion to consider "those factors necessary" to properly execute the grant program and provided additional clarification that DHS will consider "information and analysis contained in *security assessments* [emphasis added] coordinated and produced by DHS's Office of Intelligence and Analysis (I&A), with the assistance of U.S. Customs and Border Protection (CBP)." The PIA provided greater detail[21] on the security review process:

> Only applications that meet the initial eligibility requirements and score well in the merit process will go through the security review. Security reviews are used to examine the organization requesting the grant; those reviews may also require a review of individual-level data. DHS will provide written notice to these applicants prior to conducting the security review. In this written notice, DHS will provide grant applicants the opportunity to withdraw their applications.

The main shortcoming here is that the PIA, which defines the security review and provides more information for applicants as they consider whether or not to proceed with a grant application at all, was not made public until months[22] after the NOFO was published. At this time, the application review process was well underway. OCP sent an email on November 15, 2016, to top scoring applicants alerting them of DHS's intent to conduct a security review of the organization, but again did not include the clarifying information that is contained in the PIA. The DHS

---

[16] NOFO, Page 13.
[17] *See*: V. Transparency, Privacy Policy Guidance Memorandum 2008-01/Privacy Policy Directive 140-06, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security, *available at*: https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles.
[18] *See*: https://www.fema.gov/media-library-data/1467815638365-8ffa11047cad2356d43bcebec1fd0c79/070616_CVE_Grants_Rollout_FactSheet_FINAL.pdf.
[19] *See*: https://www.fema.gov/media-library-data/1467815890627-0f823c8ce0947ccccb947679efbaa302/07062016_CVE_Grants_Program_Applicant_FAQ_FINAL.pdf.
[20] *See*: https://www.dhs.gov/publication/cve-grant-webinars.
[21] *See:* Page 3: Security Review Process.
[22] OCP finalized the PIA in November 2016, but it was held in the Office of the Secretary until published on December 7, 2016.

Privacy Office does not consider there to be adequate or detailed notice in the NOFO or the emails to applicants.

Finding: Grant applicants were not provided detailed notice nor timely consent opportunities when undergoing a security review as part of the CVEGP application process.

While discussion of a security assessment during the CVEGP application is provided in the PIA, the timing of the PIA's publication and the timing of the security assessment did not provide timely or detailed notice to the organizations submitting applications to provide meaningful consent. The language of the NOFO was not specific, and the subsequent communication with eligible applicant organizations was not as detailed as the PIA to allow applicants a reasonable amount of time to consider the implications of the security review. OCP emailed eligible applicant organizations that scored well in the merit process on November 15, 2016,[23] to inform them that the organization would undergo a background check to remain in consideration for a CVE grant. In that email, OCP indicated that the NOFO did not provide specific notice that a background check of the organization would be a part of the Department's application review. The email went on to caveat that other factors, such as programmatic and financial, were still under consideration and that a security issue during a background check may not be the reason an organization was not awarded a grant. The email provided the organization with a choice to withdraw from consideration and gave the recipient approximately 24-hours to opt-out of the security review process. OCP states that staff followed up with each emailed applicant that same day to confirm receipt of the email and to address any questions.

While Congress specifically wanted DHS to conduct security reviews for the CVEGP funding, with no public definition of what a security review entails, applicants were also potentially unaware that such reviews may be considered intrusive and privacy-sensitive, which is one reason why the DHS Privacy Office required this PCR as part of the PIA mitigation. Not all DHS grant programs require a security review of applicants. The DHS Privacy Office found one other DHS grant program,[24] which chiefly provides funds to nonprofit organizations, that also includes a security assessment as part of its review process. Similar concerns over the lack of notice or individual participation are evident for that program as well. As such, greater transparency within FEMA's Grant Management Program PIA, Uses of Information, would inform grant applicants that a security review may occur and what that means for the applicant.[25]

Explicit notice of the security review requirement within the NOFO and other grant supporting documents would not be extraordinary, given congressional attention to and DHS testimony[26] on

---

[23] Note CVEGP PIA was published on December 7, 2016.
[24] Fiscal Year (FY) 2017 Nonprofit Security Grant Program NOFO, *available at*: https://www.fema.gov/media-library-data/1496432820413-257c868ed47d92699315aff1aea1d544/FY_2017_NSGP_NOFO_508_Final.pdf.
[25] Grant Management Programs FEMA/PIA-013, February 2015, *available at*: https://www.dhs.gov/sites/default/files/publications/privacy_pia_FEMA_GrantManagementPrograms_February2015.pdf and FEMA 004 Non-Disaster Grant Management Information Files System of Records Notice, *available at*: https://www.gpo.gov/fdsys/pkg/FR-2009-08-07/html/E9-18931.htm.
[26] Written testimony of DHS Office for Community Partnerships Director George Selim for a Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations hearing titled "ISIS Online: Countering Terrorist Radicalization & Recruitment On the Internet & Social Media," July 6, 2016, *available at*: https://www.dhs.gov/news/2016/07/06/written-testimony-ocp-senate-homeland-security-and-governmental-

the Department's actions to manage the $10 million in available funds provided by Congress in the 2016 Consolidated Appropriations Act. Eight days after the NOFO's release,[27] former DHS Secretary Johnson acknowledged lawmakers' concerns over the possibility of potential terrorists obtaining DHS CVE grant funding in verbal testimony, and previewed a new risk assessment process to review applications for CVE grants. The Secretary's statements clarify his discretion to consider the results of a security assessment in making his final determination. To improve transparency, however, explicit notice of the security review could have been made in the NOFO and other grant supporting documents. The DHS Privacy Office is not suggesting that actual security factors considered during the review be identified, but simply the fact that applying organizations may undergo a security review and clarification on what or who[28] may be reviewed.

As previously stated, the November 15, 2016, email was sent to those non-governmental and non-academic organizations whose applications were recommend to the Secretary for selection. The email did not explicitly clarify who or what would be reviewed. The email language used, "background check of your organization," is vague and could mean that only the organization itself would be reviewed (i.e., ABC Company), but not necessarily the individual listed on the application as the point of contact, nor any sub-applicants used to fulfill the organization's proposal. The PIA, however, notes that "the name, address, email, and phone number of the organization applying for the grant (applicants); the name and email and/or phone number of the individuals submitting those applications on behalf of an organization (individuals); and the name of the sub-applicant organizational entities (subs)" would all be a part of the security review. Nowhere in the email did DHS provide an indication to the recipient that the applicants, individuals, and/or subs would be the subject(s) of the background check, nor that it was the applicants' responsibility to notify and affirm consent from any of its sub-applicants.

IV. Conclusion

While this PCR was focused on the CVEGP, the DHS Privacy Office notes that the lessons learned from this PCR concerning OCP's programmatic management and the partnership with FEMA should be considered in the future by all DHS programs using the ND Grants system. To improve transparency, the Office of Terrorism Prevention Partnerships should consider best practices for any future CVEGP and FEMA should work with grant office leads to implement the recommendations herein across the board for any DHS grant program.

---

affairs-permanent. Written testimony of DHS Secretary Jeh C. Johnson for a Senate Committee on Homeland Security and Governmental Affairs hearing titled "Fifteen Years after 9/11: Threats to the Homeland," September 26, 2016, *available at*: https://www.dhs.gov/news/2016/09/27/written-testimony-dhs-secretary-johnson-senate-committee-homeland-security-and.

[27] Verbal Testimony of Secretary Jeh C. Johnson before the House Committee on Homeland Security on "Worldwide Threats to the Homeland: ISIS and the New Wave of Terror," July 14, 2016. Video *available at*: https://homeland.house.gov/hearing/worldwide-threats-homeland-isis-new-wave-terror-2/.

[28] *See* DHS/ALL/PIA-057, page 3, regarding security review to examine the "organization" and possibly "individual-level data," using the name, address, email and phone number of the organization; the name, email and phone number of the individual submitting the application; and the name of the subs to conduct the review. Page 6 further notes that after the initial review, additional review of the organization, its officers, employees, and any associates, may occur.

The DHS Privacy Office appreciates cooperation from OCP, FEMA, CBP, and I&A in responding to this PCR. The recommendations of this PCR are intended to provide the Department, and particularly FEMA Grants Management, with a means to further enhance the privacy-protective processes for DHS grant awards that include a security review. The DHS Privacy Office remains available to support FEMA, the Office of Terrorism Prevention Partnerships, and any other DHS office to ensure greater transparency and implementation of privacy best practices. As such, the DHS Privacy Office requests that FEMA and the Office of Terrorism Prevention Partnerships:

- Monitor the implementation of the recommendations of this PCR, and

- Provide PRIV a written report on the implementation status of all recommendations within one year of this PCR's publication date. For any recommendation not implemented in that timeframe, or that a Component chooses not to implement, please explain why the recommendation was not implemented.

cc: William Holzerland, Privacy Officer, FEMA
John H. Hill, Assistant Secretary, Office of Partnership and Engagement
David Gersten, Acting Director, Office of Terrorism Prevention Partnerships