Privacy Impact Assessment
for the

Countering Violent Extremism Grant Program

DHS/ALL/PIA-057

December 7, 2016

Contact Point
David Gersten
Deputy Director
Office for Community Partnerships
(202) 344-1009

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) uses 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. To properly execute the grant program and help adhere to congressional intent, DHS must ensure that grant recipients do not use Countering Violent Extremism (CVE) grant funding to support terrorism, engage in other criminal activities, or otherwise conduct or support activities that are contrary to the purpose of the program. The DHS Secretary has the discretion to consider those factors necessary to properly execute the grant program. Acting on behalf of the DHS Secretary in administering the grant process, the DHS Office for Community Partnerships (OCP) and Federal Emergency Management Agency (FEMA) will review grant applications considering information and analysis contained in security assessments coordinated and produced by DHS's Office of Intelligence and Analysis (I&A), with the assistance of U.S. Customs and Border Protection (CBP), directly in support of OCP, FEMA, and this departmental effort. This privacy impact assessment (PIA) examines the privacy implications of these security reviews.

Introduction

In July 2016, the Department of Homeland Security (DHS) announced the Fiscal Year 2016 Countering Violent Extremism Grant Program (CVEGP),[1] which will support programs, projects, and activities designed to prevent recruitment or radicalization to violence in the Homeland by interrupting those efforts, building community-level resilience to them, and identifying the early signs of radicalization to violence and providing appropriate interventions through civic organizations, law enforcement, or other entities. Eligible activities for the Countering Violent Extremism (CVE) initiative include planning, developing, implementing, or expanding educational outreach, community engagement, and social service programs, as well as other activities.[2] The notice of funding opportunity for the CVE program formally announced the program and solicited applications from states, local and tribal governments, non-profit organizations, and institutions of higher education.

The CVEGP grants are the first federal grants dedicated to supporting local CVE programs. Accordingly, they are of heightened concern. During recent congressional testimony by Secretary Jeh C. Johnson, for instance, several members of Congress highlighted the risk that some applicants might themselves support terrorism, engage in other criminal activities, or otherwise

[1] For more information, *see* https://www.dhs.gov/cvegrants.
[2] 161 Cong. Rec. H10162 (2015) (Joint Explanatory Statement).

conduct or support activities contrary to the purpose of the program. Unless the applicants were properly vetted, they continued, it was even possible that DHS grant money could be used to support nefarious activity.[3] In testimony, Secretary Johnson acknowledged members' concerns and previewed a new risk assessment process to review applications for CVE grants.

Since that time, the DHS Office for Community Partnerships (OCP) has worked with other DHS stakeholder offices to refine a new review process. To design this new process, OCP used a risk-based approach. For instance, the risk that a state, local, tribal government, or college or university would misuse a DHS grant to support terrorism is so comparatively small that OCP determined that applications from such institutions may be considered presumptively risk-free and judged under more traditional standards of grant review. On the other hand, even though the risk that any individual non-profit organization-applicant seeks to exploit a DHS grant program is exceedingly small, these are the portion of the applicant pool DHS typically knows the least about. Thus, out of an abundance of caution, prudence requires the swift and narrowly tailored risk assessment process for these organizations designed by the OCP and described herein.

DHS's OCP, in partnership with the Federal Emergency Management Agency (FEMA), will administer the CVEGP. The application process for the CVEGP is managed through FEMA's Non-Disaster Grants System (ND Grants)[4] in accordance with standard procedures. ND Grants is FEMA's web-based grant management system, which maintains grant applicant information that FEMA uses to manage and administer the grant application process. Applicants provide information to DHS through ND Grants when applying for a grant under the CVEGP. To properly execute the grant program and help adhere to congressional intent, DHS must ensure that grant recipients do not use CVE grant funding to support terrorism, engage in other criminal activities, or otherwise conduct or support activities contrary to the purpose of the program. Therefore, DHS will conduct security reviews of grant applications to determine the likelihood that:

a. An applicant may use CVE grant funding to support terrorism or engage in other criminal activities;
b. An applicant may, with or without the funding, conduct or support activities contrary to the purpose of the CVE grant; or
c. An applicant may otherwise be an inappropriate choice to receive a CVE grant based on other domestic, national, or international security considerations.

[3] 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/.
[4] Privacy compliance documentation for this system includes the following: DHS/FEMA/PIA-013 Grant Management Program and DHS/FEMA-004 Non-Disaster Grant Management Information Files, 80 Fed. Reg. 13404 (Mar. 13, 2015).

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 review and award process shall not be conducted based solely on an individual's or group's race, ethnicity, gender, religion, sexual orientation, gender identity, country of birth, or nationality, or for the sole purpose of monitoring activities protected by the U.S. Constitution.

I&A (Homeland Threats Division), supporting OCP and FEMA, is responsible for providing the information analysis and support necessary to inform the security reviews, including identifying, with appropriate assistance from the U.S. Customs and Border Protection's (CBP) National Targeting Center (NTC),[5] relevant intelligence or information necessary for assessing the likelihood of an applicant's involvement or association with terrorism or any of the other activities appropriate for considering an applicant's suitability for receiving a grant award, as described above.[6] For each application that will undergo a security review, a security review is initiated when OCP provides I&A with:

- 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).[7]

This information is derived directly from the grant application. DHS received information directly from grant applicants through grant applications; there were no additional or separate requests or collections of information from grant applicants by DHS. I&A, with appropriate assistance from CBP NTC, will use that information to identify from within available Departmental, Intelligence Community, and law enforcement holdings, open source and social media resources, financial data, import/export data, immigration data, travel history, and foreign holdings in order to identify information responsive to Security Factors that are relevant for determining risk in this program. For operational security reasons, DHS will not list the Security

[5] I&A will first access, review, analyze, and integrate information from sources uniquely available to I&A to identify any responsive information related to the grant applicant prior to sending to CBP NTC for review. CBP NTC may supplement initial findings of I&A by conducting further checks of travel, immigration, criminal, open source (including social media), or other records under its control for additional responsive information.
[6] See 6 U.S.C. §§ 121(d)(1).
[7] Information from the grant application will be retrieved by the name of the organization and will be provided, along with other contact information about the organization, to I&A.

Factors in this PIA.

I&A will provide information received from OCP and the results of I&A's initial research and analysis on that information on each grant applicant to CBP NTC. As warranted, I&A will request further assistance from CBP NTC to supplement I&A's initial findings with responsive information gleaned from further checks against the travel, border, immigration, law enforcement, open source, or other appropriate records and databases available to or otherwise under the control of CBP NTC.[8]

I&A's collection, maintenance, and dissemination of information identifying U.S. citizens or lawful permanent residents in furtherance of its support to security reviews is covered by and undertaken consistent with the authorized uses of that information as articulated in I&A's Enterprise Records System (ERS) System of Records Notice (SORN),[9] which notes that the information in ERS includes not just intelligence information but also "historical law enforcement, operational, immigration, customs, border and transportation security, and other administrative information."[10]

CBP will share the results of its analysis in accordance with 5 U.S.C. 552a(b)(1) and I&A's need for those records in the performance of its duties in identifying, analyzing, and providing relevant information to support OCP's grant application process.[11] CBP will retain the information received from I&A and the results of I&A's and CBP's vetting for each selected applicant in the

[8] CBP will conduct vetting through relevant Departmental systems as needed, but may not need to check each and every database listed. The NTC may supplement initial vetting conducted by I&A by conducting vetting checks for travel history that suggests support for terrorism or criminal activity; immigration status (e.g., work authorized); National Crime Information Center (NCIC) check of criminal history; and open source and social media content. Following the initial vetting results from I&A, CBP NTC will then vet organizational applicants, including the name of the organization and the name of the individual who filed on behalf of the organization, through at least the following databases (as appropriate): TECS (DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 Fed. Reg. 77778 (Dec. 19, 2008)); Advance Passenger Information System (DHS/CBP-005 Advance Passenger Information System (APIS), 80 Fed. Reg. 13407 (March 13, 2015)); Border Crossing Information (DHS/CBP-007 Border Crossing Information (BCI), 81 Fed. Reg. 404 (Jan. 25, 2016)); Import Information System (DHS/CBP-001 Import Information System (IIS), 81 Fed. Reg. 48826 (July 26, 2016); the Automated Targeting System (DHS/CBP-006 Automated Targeting System (ATS), 77 Fed. Reg. 30297 (May 22, 2012)); the NCIC (JUSTICE/FBI-001, 64 Fed. Reg. 52343 (Sept. 28, 1999) (as amended by, regarding routine uses, 66 Fed. Reg. 8425 (Jan. 31, 2001), 66 Fed. Reg. 33558 (June 22, 2001), 70 Fed. Reg. 7513 (Feb. 14, 2005), and 72 Fed. Reg. 3410 (Jan. 25, 2007)); the Export Information System (EIS) (DHS/CBP-020 Export Information System, 80 Fed. Reg. 53181 (Sept. 2, 2015)); the Terrorist Screening Database (DHS/ALL-030 Use of the Terrorist Screening Database (TSDB) System of Records, 81 Fed. Reg. 19988 (Apr. 6, 2016)); Terrorist Identities Datamart Environment (TIDE) (72 Fed. Reg. 73887-02 (Dec. 28, 2007)); and the Department of Treasury's Financial Crimes Enforcement Network (FinCEN) systems, last published at 79 Fed. Reg. 20969 (Apr. 14, 2014).

[9] DHS/IA-001 - Enterprise Records System (ERS), 73 Fed. Reg. 28128, 28128 (May 15, 2008).

[10] 73 Fed. Reg. at 28130.

[11] See also 6 U.S.C. § 121(d)(17) (I&A's responsibility to "provide intelligence and information analysis and support to other elements of the Department").

ATS-Targeting Framework.[12]

Security Review Report (SRR)

I&A will transmit its findings to the OCP Director and the FEMA Grant Programs Directorate (Assistant Administrator for Grant Programs with the results of the security review in a standardized I&A report format known as the Security Review Report (SRR). Each SRR will include a summary of responsive information that was found for each application, including the organizations and individuals identified therein. I&A will retain any SRRs produced in accordance with its governing records management systems and covered by the applicable I&A system of records notice.[13] FEMA's ND Grants System does not retain any SRRs or additional information resulting from the security reviews.

The SRR reflects I&A's findings regarding any known or suspected involvement or associations of applicants with terrorism or other criminal activities or conduct contrary to the purposes of the grant program, and includes the information or, as appropriate, the source(s) or summary of the information identified and relied upon in the course of I&A's review for any analytic judgements reflected in the SRR. All SRRs intended to be disseminated to the OCP Director and the FEMA Assistant Administrator for Grant Programs will be reviewed in advance by the I&A Privacy/Intelligence Oversight Officer, to ensure compliance with intelligence oversight requirements and individual privacy protections, and the Office of the General Counsel's (OGC) Intelligence Law Division, to ensure consistency with any applicable legal requirements.

If, after reviewing the SRR, the OCP Director and the FEMA Assistant Administrator for Grant Programs, based upon information provided in the SRR, intend to recommend that the DHS Secretary not approve an award, the OCP Director will convene a working group with members from OCP, OGC, the Office for Civil Rights and Civil Liberties (CRCL), the Privacy Office, the DHS Policy Screening Coordination Office (SCO), and I&A to further consider the recommendation. The working group will review the recommendation made by OCP and FEMA, in light of the information and analytic conclusions provided in the SRR and specifically relied upon as a basis for their recommendation, in order to identify any concerns based upon each office's equities, and, as appropriate, address or memorialize those concerns in writing to accompany the final recommendation sent to the DHS Secretary.

---

[12] See Automated Targeting System (DHS/CBP-006 Automated Targeting System (ATS), 77 Fed. Reg. 30297 (May 22, 2012). Per the ATS SORN, CBP may retain source (as opposed to ingested or pointer) information in ATS "for law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source and/or classified information." CVE reviews of this information aligns with the purpose of ATS, which is to 'to perform targeting of individuals who may pose a risk to border security or public safety, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law."

[13] I&A will retain these records in its systems pursuant to its Privacy Act SORN, DHS/IA-001 Enterprise Records System (ERS), 73 Fed. Reg. 28128 (May 15, 2008).

Alternately, if the group believes an applicant warrants additional scrutiny before a recommendation is transmitted to the DHS Secretary, the group may request that I&A conduct additional research or analysis, including, as appropriate, of open source data, to ascertain additional information about the organization, its officers, employees, and any associates (i.e., board of directors and key staff), as necessary, for further assessing the nature of the security risk. Based upon the further input of the working group, the OCP Director and FEMA Assistant Administrator for Grant Programs will provide a recommendation in writing regarding the applicant organization, clearly articulating that, based on the totality of information, the applicant organization has or may a) engage in activity to support terrorism, b) engage in criminal activities, or c) may otherwise be an inappropriate choice based on domestic, national, or international security concerns or, when applicable, explaining how the security concern was resolved. If any reviewing office does not concur with the written recommendation, that office shall provide its dissenting opinion in writing and that opinion will accompany the written recommendation sent to the DHS Secretary.

Any choice not to recommend an award to a grant applicant resulting from the security review will be based on all relevant and responsive information available to DHS, including any reasonably identified neutral or mitigating information. The decision to recommend disqualification of an applicant based on the security review rests jointly and exclusively with the OCP Director and the FEMA Assistant Administrator for Grant Programs and will be completed before their joint recommendation for awards is sent to the DHS Secretary, along with any written dissenting opinion.[14]

If an application is not recommended for disqualification by the OCP Director and the FEMA Assistant Administrator for Grant Programs, the DHS Secretary may still choose to review the SRRs and any associated derogatory information as part of his deliberation for making the awards. The DHS Secretary may also request that I&A conduct additional research or analysis, including, as appropriate, with assistance from DHS partners and of open source data, to ascertain additional information about organizations.

The DHS Secretary is the final approval authority regarding the issuance of CVE Grant awards.

This PIA covers the first iteration of this program. The DHS Privacy Office will initiate a Privacy Compliance Review (PCR) ninety days from the start of the review period to provide recommendations for improving the privacy protections inherent in deploying a security review process. If the CVEGP is renewed, DHS will update this PIA.

[14] The written recommendation will be tied to the organization and not to any single individual or member of the organization, and thus does not implicate any Department system of record notices.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal Government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to Section 208 of the E-Government Act of 2002 and Section 222 of the Homeland Security Act of 2002. Given that OCP, I&A, and CBP's NTC are offices of the Department and the CVEGP is a program rather than a particular information technology system, this PIA is conducted as it relates to the DHS construct of the FIPPs. This PIA examines the privacy impact of I&A's research and analytic support for the CVEGP as it relates to the FIPPs.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

DHS OCP published a Notice of Funding Opportunity (NOFO) on grants.gov for the CVEGP on July 6, 2016, with a deadline for applications of September 6, 2016.[15] This NOFO was similar to those issued for other federal grant opportunities in its requirement for collection, use, dissemination, and maintenance of PII for the purpose of making an award determination based on multiple levels of review, scoring, due diligence, and discretion.

[15] "The Department of Homeland Security Notice of Funding Opportunity Fiscal Year 2016 Countering Violent Extremism (CVE) Grant Program." (July 6, 2016). *Available at:* http://www.grants.gov/web/grants/view-opportunity.html?oppId=285773.

The NOFO stated that the "application evaluation criteria may include the following risk-based [sic] considerations of the applicant: (1) financial stability; (2) quality of management systems and ability to meet management standards; (3) history of performance in managing federal awards; (4) reports and findings from audits; and (5) ability to effectively implement statutory, regulatory, or other requirements."[16] The security review, one of these "other requirements" outlined in the risk-based considerations, is designed to assess whether grant recipients will use the funding to support terrorism, engage in other criminal activities, or otherwise conduct or support activities that are contrary to the purpose of the program. Indications that a grant applicant may use grant funding for a purpose that is antithetical to the purpose for which the grant is given has bearing on the applicant's ability to meet the Outcomes and Data evaluation criteria in Appendix D of the NOFO; as such an applicant is unlikely to achieve the outcomes outlined in the grant application.

The NOFO also noted that "The Secretary retains the discretion to consider other factors and information in addition to those included in the recommendations."[17] On July 14, 2016, Secretary Jeh C. Johnson testified before Congress that DHS would conduct security reviews.[18] On September 22, 2016, OCP Director George Selim testified about the rigorous review process, noting that "there is a high degree of scrutiny and review for every grant applicant" and "each and every grant application that we receive has four degrees of review that it goes through."[19] Besides the official posting of the NOFO on grants.gov, OCP and FEMA – partners in administration of the CVEGP – endeavored to further publicize the NOFO through several online webchats, direct dissemination to interested parties, and posting of links on public webpages.

Privacy Risk: There is a risk that points of contact, or other associated individuals for an organization, do not have notice that DHS is conducting a security review on them.

Mitigation: This risk is partially mitigated. In addition to this PIA, DHS provided notice in the NOFO that DHS would take a risk-based approach to selecting successful applications. DHS is also providing written notice to applicants prior to conducting the security review. In this written notice, DHS will provide grant applicants the opportunity to withdraw their applications. If DHS

[16] "The Department of Homeland Security Notice of Funding Opportunity Fiscal Year 2016 Countering Violent Extremism (CVE) Grant Program." (July 6, 2016). *Available at:* http://www.grants.gov/web/grants/view-opportunity.html?oppId=285773.
[17] "The Department of Homeland Security Notice of Funding Opportunity Fiscal Year 2016 Countering Violent Extremism (CVE) Grant Program." (July 6, 2016). *Available at:* http://www.grants.gov/web/grants/view-opportunity.html?oppId=285773.
[18] 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/.
[19] Verbal Testimony of George Selim before the House Committee on Homeland Security on "Identifying the Enemy: Radical Islamist Terror." (September 22, 2016). Video *available at:* https://homeland.house.gov/hearing/identifying-enemy-radical-islamist-terror/.

determines that it will review an organization's key personnel or members of the board of directors, DHS will not provide additional notice to those individuals beyond this PIA. The PCR, required to be initiated ninety days from the start of the review period, will focus on the effectiveness of the notice process.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

In the NOFO for the CVEGP, DHS specifically asks for the name of the organization applying for the grant along with contact information for the individual(s) filing the application. Individuals who are filing the application have consented to DHS's collection of their PII by voluntarily providing the PII as part of the grant application. Access and corrections of PII submitted can be formally offered through the FEMA system and, thereafter, corrected by contacting OCP directly at the email noted on OCP's public-facing webpage.

Privacy Risk: If derogatory information is found on the organization, DHS may conduct additional searches using publicly available information to identify other known associates, including key employees and board members, of the organization not otherwise identified in the grant application or materials accompanying submissions. Since these individuals did not have notice that DHS would be looking at this information, the impacted individuals do not have the opportunity to provide the information or consent to its uses.

Mitigation: This risk is not mitigated. DHS will only conduct a review of these previously unidentified individuals if that review is deemed necessary by a panel that includes OCP, OGC, CRCL, the Privacy Office, SCO, and I&A. In addition, by only using publicly available information to identify key employees or board members, DHS is likely to collect information on an organization's senior leadership; individuals who are charged with representing the organization publicly as part of their official duties (e.g., a contact listed for press inquiries); or individuals who have otherwise voluntarily published or released publicly information about their association with the organization. Senior leaders may have approved the grant application, and individuals who have otherwise published or permitted the publication of their personal information publicly have tacitly accepted the possibility that their publicly available information may be used for a variety of purposes.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

DHS collects information as part of the grant application process. The SORN covering ND Grants notes that "the purpose of this system is to assist in determining eligibility of awards for non-disaster related grants."[20] The NOFO informed applicants that the DHS Secretary has authority to consider information beyond the factors explicitly detailed in Appendix D of the NOFO, and the DHS Secretary has publicly announced that DHS will conduct security reviews.[21] The information collected as part of the grant application process will be used to conduct such security reviews. The security reviews are consistent with the evaluation criteria outlined in the NOFO. The security review conducted by I&A is designed to assess the likelihood of an applicant's involvement or association with terrorism or any of the other activities appropriate for considering an applicant's suitability for receiving a grant award. As stated in I&A's ERS SORN, the purpose of I&A's analysis is to provide "intelligence and analysis support to all DHS activities, components, and organizational elements." I&A's collection, maintenance, and dissemination of information identifying U.S. citizens or lawful permanent residents in furtherance of it support to security reviews is authorized by and undertaken consistent with the authorized uses of that information as articulated in I&A's ERS SORN.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

The CVEGP only obtains information that is relevant to adjudicating a grant application. The applications include up to fifteen pages of program descriptions, background, and endorsements related to how the applicant proposes to use DHS funds to counter violent extremism. Also included are specific costs and, when necessary, financial data for OCP and FEMA to determine whether the proposal is financially sound.

To promote data minimization in the security review process, security reviews will only be conducted for the applications that meet the program eligibility requirements and score well in the

[20] DHS/FEMA-004 Non-Disaster Grant Management Information Files, 80 Fed. Reg. 13404 (Mar. 13, 2015). *Available at:* https://www.gpo.gov/fdsys/pkg/FR-2015-03-13/html/2015-05799.htm.
[21] 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/.

merit review process. This limits the data collected to approximately 25 applicants instead of the full applicant pool of more than 200. Further, the information provided to I&A for proposed awardees undergoing security reviews will be narrowly tailored to what is needed to determine security risks. As noted in the introduction of this PIA, that information is limited to: name, address, email, and phone number of the organization; the name and email and/or phone number of the individuals; and the name of the subs. I&A may check those limited data elements against otherwise appropriate Departmental, Intelligence Community, and law enforcement holdings, open source and social media resources, financial data, import/export data, immigration data, travel history, and foreign holdings in order to identify information responsive to security factors and to craft a CVEGP SRR for each applicant for whom responsive information is found.

The SRR itself will be retained by I&A as Finished Intelligence Case Files, labeled as Permanent Records, retained pursuant to the authorized Disposition N1-563-07-16-4. Records should be offered to the National Archives and Records Administration for permanent retention 20 years after cutoff. Pursuant to I&A's current "Interim Intelligence Oversight Procedures," I&A has 180 days from the date of collection of U.S. Person data to determine whether the U.S. Person data meets a two-part test: 1) falls within one of I&A's authorized intelligence activities, and 2) collected information is reasonably believed to fall within one of I&A's authorized collection categories. If the collected data does not meet the two-part test, the records are to be disposed of pursuant to the authorized Disposition N1-563-09-7-1c, which is Temporary and requires the agency to destroy or delete the information immediately but no later than 180 days from date collected.

CBP will retain the information it receives from I&A along with the results of any additional checks CBP conducts for each selected applicant and returned in summary-form to I&A within the ATS-Targeting Framework,[22] consistent with the existing retention period in ATS. All ATS records are retained for fifteen years, whether or not the records demonstrate any derogatory or national security information. The justification for a fifteen-year retention period for the official records is based on CBP's law enforcement and security functions at the border. This retention period is based on CBP's historical encounters with suspected terrorists and other criminals, as well as the broader expertise of the law enforcement and intelligence communities. It is well known, for example, that potential terrorists may make multiple visits to the United States in advance of performing an attack. It is over the course of time and multiple visits that a potential risk becomes clear. Travel records, including historical records, are essential in assisting CBP Officers with their risk-based assessment of travel indicators and identifying potential links between known and previously unidentified terrorist facilitators. Analyzing these records for these

[22] DHS/CBP/PIA-006 Automated Targeting System and subsequent updates, *available at* https://www.dhs.gov/publication/automated-targeting-system-ats-update.

purposes allows CBP to continue to effectively identify suspect travel patterns and irregularities. In the event that I&A or CBP discover derogatory information about CVEGP applicants, CBP will maintain this information in the ATS-Targeting Framework for the life of the law enforcement matter to support that activity and other enforcement activities that may become related.[23]

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

OCP and FEMA collect this information and share it within DHS as part of the grant eligibility review process. Information is shared on a need to know basis pursuant to 5 U.S.C. 552a(b)(1) with individuals who need the information in the performance of their official duties. OCP and FEMA share the information with I&A to facilitate the security review. I&A shares the information to be vetted and the results of its analysis with CBP so that CBP can supplement the security review.

Privacy Risk: There is a risk that FEMA, OCP, I&A, or CBP personnel will use the information for purposes other than determining grant eligibility.

Mitigation: This risk is partially mitigated. As outlined below, the FEMA ND Grants System has controls to ensure that only those who have been given permission to manage the data have access to the data. All grant reviewers receive mandatory, annual training on the appropriate handling of PII.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

The preliminary information that is available to CVEGP on individuals and organizations is from the grant application. Because this grant application is submitted voluntarily by the applicant, there is a high likelihood that this applicant-contributed information is correct.

If a security review suggests a potential security issue, DHS may use publicly available information to ascertain the controlling individuals of the organization (i.e., board of directors and

[23] *See* DHS/CBP-006 Automated Targeting System, 77 Fed. Reg. 30297 (May 22, 2012). "Information maintained only in ATS that is linked to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases (i.e., specific and credible threats; flights, individuals, and routes of concern; or other defined sets of circumstances) will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related."

key staff) for further security checks. DHS will ensure the quality and integrity of this information by obtaining identifying data about the controlling individuals of the organization from sources clearly controlled by the organizations. An organization has a vested interest in ensuring the information it promulgates publicly about itself is accurate.

As part of the security checks, DHS will use a variety of information sources that are not supplied or controlled by the grant applicant. These information sources include: Departmental, Intelligence Community, and law enforcement holdings; open source and social media resources; financial data; import/export data; immigration data; travel history; and foreign holdings.

Privacy Risk: There is a risk that the information DHS uses to perform the security checks is not accurate.

Mitigation: This risk is partially mitigated. DHS has operational imperatives to ensure that Departmental data sources are as accurate, timely, relevant, and complete as possible. Many Department data sources include self-reported information (e.g., travel history, immigration data). DHS considers data provided by trusted external partners provided to the Department for analytical and operational purposes to be authoritative. If there are any questions regarding the accuracy of externally-provided data, recipients will work with the originating agency to confirm the information. Finally, when performing security reviews and analysis, DHS analysts will follow good tradecraft practices, which include documenting the source of data and assessing its timeliness and reliability.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

The CVEGP award files are maintained on an accredited grant management system with access limited to DHS personnel involved in grant adjudication matters who have a legitimate need to know. The SRR and subsequent data obtained by I&A is housed in accredited systems and locations limited to DHS personnel.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

The FEMA ND Grants System is an auditable system and the business owner reviews access logs to ensure that only those who have been given permission to manage the data have access. In addition, all personnel who will have access to either the raw information NTC provides

to I&A or the SRR I&A produces, who are cleared at the Top Secret level, are required to complete annual information security, intelligence oversight, and privacy training to remind them of their responsibilities to secure and protect the data.

Conclusion

The DHS CVEGP is the first federal grants program dedicated to supporting local CVE programs. Within ninety days after completing the security reviews, the DHS Privacy Office will initiate a PCR of this program and make recommendations to improve the privacy protections in the security review process. If the CVEGP is funded again, DHS will update this PIA.

Responsible Officials

David D. Gersten
Deputy Director
Office for Community Partnerships
Department of Homeland Security

Approval Signature Page

Original, signed copy on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security