Privacy Impact Assessment
for the

Targeted Violence and Terrorism Prevention Grant Program

DHS/ALL/PIA-083

April 8, 2020

Contact Point
David D. Gersten
Director (Acting)
Office for Targeted Violence and Terrorism Prevention
(202) 344-1009

Reviewing Official
Dena Kozanas
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) uses the Targeted Violence and Terrorism Prevention (TVTP) Grant Program to help states and local communities prevent targeted violence and terrorism. To properly execute the grant program, DHS must ensure that grant recipients will use any potential funding consistent with the purpose of the program. In administering this process, the DHS Office for Targeted Violence and Terrorism Prevention (OTVTP) and the Federal Emergency Management Agency (FEMA) will review grant applications considering information and analysis contained in security assessments developed in partnership with DHS's Office of Intelligence and Analysis (I&A) directly in support of OTVTP, FEMA, and this departmental effort. This Privacy Impact Assessment (PIA) examines the privacy implications of the TVTP Grant Program.

Overview

On December 20, 2019, the Department of Homeland Security Appropriations Act, 2020 was enacted as part of Pub. L. 116-93.[1] Included in that legislation was funding for targeted violence and terrorism prevention grants that are an evolution of the Countering Violent Extremism Grant Program (CVEGP).[2] The DHS Office for Targeted Violence and Terrorism Prevention (OTVTP), in partnership with the Federal Emergency Management Agency (FEMA), administers the new Targeted Violence and Terrorism Prevention (TVTP) Grant Program.[3]

The application process for the TVTP Grant Program 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 lifecycle of the grants, including the application process. Applicants provide information to DHS through Grants.gov[5] when applying for a grant under the TVTP Grant Program. To properly execute the grant program, DHS must ensure that grant recipients do not use TVTP grant funding to support terrorism or otherwise conduct or support activities contrary to the purpose of the program or the missions of the Department. Therefore, DHS conducts security reviews of grant applications to determine the likelihood that:

---

[1] *See* https://www.congress.gov/116/plaws/publ93/PLAW-116publ93.pdf.
[2] For more information about CVEGP, *see* https://www.dhs.gov/cvegrants and DHS/ALL/PIA-057 Countering Violent Extremism Grant Program, *available at* https://www.dhs.gov/privacy.
[3] OTVTP is a sub-office of the DHS Office of Strategy, Policy and Plans (PLCY). It was previously known as the Office for Terrorism Prevention Partnerships and, before that, the Office for Community Partnerships (OCP), which administered the CVEGP in partnership with FEMA.
[4] *See* DHS/FEMA/PIA-013 Grant Management Program and DHS/FEMA-004 Non-Disaster Grant Management Information Files, 80 FR 13404 (March 13, 2015), *available at* https://www.dhs.gov/privacy.
[5] Grants.gov, managed by the Department of Health and Human Services (HHS), provides a centralized location for grant seekers to find and apply for federal funding opportunities. FEMA uses Grants.gov as a service provider to intake grant applications and the information provided on those applications into ND Grants.

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

Security Review Process

The TVTP Grant Program will use the security review process to assess grant applications. This process uses a risk-based approach in which DHS assesses the relative risks of various applicant types. The eligible applicant types are state, local, tribal, and territorial governments; institutions of higher education; and non-profit organizations. Governmental entities pose the lowest risk, as they are longtime partners in the homeland security enterprise and are administered by individuals previously screened for positions in the public trust. Institutions of higher education pose the next lowest risk; under this grant program, only institutions of higher education with independent accreditation are eligible. Accredited institutions of higher education have a long track record of performing on DHS grants, must vest their authority in a large number of people, and have a vested interest in maintaining their accreditation. Non-profit organizations pose an unknown, and by extension, higher risk. While some non-profits are long-existing, reputable institutions with sizeable groups of individuals controlling them, others are newly registered with 501(c)(3) status with the Internal Revenue Service (IRS), are closely controlled by a limited number of individuals, and as a group have less experience performing on DHS grants. Applicants with no likelihood of being recommended for funding have no risk of misusing the funds and, as such, the risk-based approach calls for only conducting the security review on the top-tier of scored applications from the non-profit organization pool.

Only applications that meet the initial eligibility requirements and score well in the merit process will undergo with 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 from the individuals who submit the application and individuals with a controlling responsibility within the organization (i.e., board of directors and key staff). 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. DHS will provide written notice of the security review to prospective applicants through clear statements included in a Notice of Funding Opportunity (NOFO).[6] Language in each NOFO will provide prospective grant applicants notice that their application may be subject to such a review. Additionally, all NOFOs that govern programs with

[6] A NOFO is a publicly available document by which a federal agency makes known its intentions to award discretionary grants or cooperative agreements, usually as a result of competition for funds. NOFOs may be known as funding opportunity announcements, program announcements, notices of funding availability, solicitations, or other names depending on the agency and type of program.

a security review, as described in this document, will have a link to this PIA.

OTVTP and FEMA will engage with the Office of Intelligence and Analysis (I&A), which will provide the information analysis and support necessary to inform the security reviews. This includes identifying relevant intelligence or information necessary for OTVTP to assess the likelihood of an applicant's involvement or association with terrorism or any of the other activities relevant to an applicant's suitability for receiving a grant award, as described above.[7] A security review is initiated when OTVTP accesses the following information for the purposes of conducting the review:

- the name, address, email, and phone number of the organization applying for the grant (applicants); and
- the name and email and/or phone number of the individuals submitting those applications on behalf of an organization (individuals).[8]

This information is derived directly from the grant application. There are no additional requests or collections of information from grant applicants. In order to identify information responsive to Security Factors relevant for determining risk, [9] I&A will access the following: currently available departmental and Intelligence Community holdings; open source and publicly available social media resources; and foreign holdings.[10]

I&A's collection, maintenance, and dissemination of information identifying U.S. citizens or lawful permanent residents in furtherance of its support to the security review process 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),[11] 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 records."[12]

OTVTP and FEMA's partnership with I&A is in accordance with 5 U.S.C. § 552a(b)(1)

[7] *See* 6 U.S.C. § 121(d)(1).
[8] Additional information about individuals may be used to conduct an additional security review; this process is detailed further on in this PIA. However, at this stage in the security review, only the submitting individuals are impacted.
[9] For operational security reasons, DHS will not list the Security Factors in this PIA.
[10] DHS will conduct vetting through relevant departmental systems as needed, but may not need to check each and every database listed. DHS may conduct vetting checks for connection to known or suspected terrorists and checks of open source and publicly available social media content. DHS will vet organizational applicants, including the name of the organization and the name of the individual(s) who filed on behalf of the organization, through the following databases (as appropriate): the Terrorist Screening Database (DHS/ALL-030 Use of the Terrorist Screening Database (TSDB) System of Records, 81 FR 19988 (April 6, 2016)); and Terrorist Identities Datamart Environment (TIDE) System of Records (72 FR 73887 (December 28, 2007)).
[11] *See* DHS/IA-001 Enterprise Records System (ERS), 73 FR 28128 (May 15, 2008).
[12] 73 FR 28130.

and based on I&A's need for those records in the performance of its duties in identifying, analyzing, and providing relevant information to support OTVTP's grant application process.[13]

Security Review Report (SRR)

I&A will transmit any results from its analysis to the OTVTP Director 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 SORN.[14] FEMA's ND Grants System does not retain any SRRs or additional information resulting from the security reviews.

The SRR will reflect I&A's findings regarding (1) any known or suspected involvement or associations of applicants with terrorism. This includes the information, source(s), or summary of the information I&A's review identified and relied upon for any analytic judgements reflected in the SRR. The I&A Privacy/Intelligence Oversight Officer, the DHS Privacy Office, and the Office for Civil Rights and Civil Liberties (CRCL) will review all SRRs disseminated to the OTVTP Director to ensure compliance with intelligence oversight requirements and individual civil liberties and privacy protections. The Office of the General Counsel's (OGC) Intelligence Law Division will review all SRRs to ensure consistency with any applicable legal requirements.

If, after reviewing the SRR, the OTVTP Director believes the information provided raises security concerns that may disqualify the organization from receiving an award, the OTVTP Director will convene an SRR working group comprised of FEMA, OGC, the DHS Privacy Office, CRCL, and the Office of Strategy, Policy, and Plans (PLCY), including the PLCY Screening and Vetting Office. The working group will review the information and analytic conclusions in the SRR and will provide advice to the OTVP Director based upon each office's equities, authorities, and responsibilities.

If, as a result of the working group's review, the OVTVP Director believes an applicant warrants additional scrutiny before a final recommendation on awards is transmitted, the OTVTP Director 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. This secondary review will consist of the same type of checks conducted during the initial security review, following the identification of individuals as described above.

As part of the recommendation for grant awards, the OTVTP Director will provide a

[13] *See* also 6 U.S.C. § 121(d)(15) (I&A's responsibility to "provide intelligence and information analysis and support to other elements of the Department").
[14] I&A will retain these records in its systems pursuant to its SORN, DHS/IA-001 Enterprise Records System (ERS), 73 FR 28128 (May 15, 2008).

recommendation in writing regarding an applicant organization for which an SRR was conducted. The recommendation will either explain how the security concern was resolved or articulate that, based on the totality of information, the applicant organization has or may a) engage in activity to support targeted violence or terrorism, b) conduct or support activities contrary to the purpose of the TVTP grant, or c) may otherwise be an inappropriate choice based on domestic, national, or international security concerns, and therefore was determined to be disqualified from receiving an award. If any member of the SRR working group does not concur with the written recommendation, that office shall provide its dissenting opinion in writing. That opinion will accompany the written recommendation sent to the DHS Secretary or his/her designee responsible for approving the awards.

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 exclusively with the OTVTP Director. Even if the OTVTP Director does not recommend disqualifying an application, the DHS Secretary or his/her designee may still choose to review the SRRs and any associated derogatory information as part of his/her deliberation for making the awards. The official may also request that I&A conduct additional research or analysis, including, as appropriate, of open source data, to ascertain additional information about organizations.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[15] 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. 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.[16]

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.[17] The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

[15] 5 U.S.C. § 552a.
[16] 6 U.S.C. § 142(a)(2).
[17] *See* 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* www.dhs.gov/privacy.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208[18] and the Homeland Security Act of 2002 Section 222.[19] Given that the TVTP Grant Program 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 the TVTP Grant Program 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.

The PIA will be referenced and linked in the NOFO for the FY20 TVTP Grant Program, with additional transparency language describing the review.

Privacy Risk: There is still a risk that points of contact, or other associated individuals for an organization (i.e., controlling individuals of the organization, such as board of directors and key staff), do not have notice that DHS is conducting a security review on them.

Mitigation: This risk is not fully mitigated. DHS provides notice in the NOFO that DHS will take a risk-based approach to selecting successful applications. The NOFO includes details of the security review. However, if DHS 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. That responsibility ultimately falls on the individuals from those organizations who are part of the application process and have direct knowledge of the security review provided through the notice in the NOFO and associated documentation.

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 DHS grant application processes, 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. Additionally, if DHS determines that it will review an organization's key personnel or members of the board of directors, DHS does not collect information directly from these individuals. DHS uses publicly available information not

[18] 44 U.S.C. § 3501 note.
[19] 6 U.S.C. § 142.

otherwise identified in the grant application or materials accompanying submissions to identify these other known associates.

Notice of the security review process is provided in the NOFO; specifically, it states: "By submitting an application under this funding opportunity, applicants consent to undergoing this security review." Therefore, organizations and individuals generally opt-in to this grant program. Organizations can withdraw their applications from consideration at any time prior to initiation of the security review.

Access and corrections of PII submitted can be formally offered through the FEMA ND Grants system and, thereafter, corrected by contacting OTVTP directly at the email noted in the NOFO announcing each grant program.

Privacy Risk: If derogatory information is found on an 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 may not be aware of security review process and that DHS may be looking at this information, the impacted individuals do not have the opportunity to provide the information or consent to its use.

Mitigation: This risk is partially mitigated. Notices in NOFOs that will use this security review process will indicate that there will be a security review and link to this PIA, encouraging applicants to review the entire process. DHS will only conduct a review of these previously unidentified individuals if that review is deemed necessary by a panel that includes OTVTP, OGC, the DHS Privacy Office, CRCL, and PLCY. These additional security reviews will consist of the same type of checks conducted during the initial security review. By only using publicly available information to identify key employees or board members, DHS is likely to only 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 on behalf of the organization.

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] NOFOs, along with this PIA, will inform applicants that the information collected as part of the grant application process will be used to conduct security reviews. The security reviews are consistent with the evaluation criteria outlined in the NOFOs. The security review assistance provided by I&A is designed to assess the likelihood of an applicant's involvement or association with terrorism, targeted violence, or any of the other activities relevant to 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 its support to security reviews is authorized by and undertaken consistent with the authorized uses of that information as articulated in that 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 TVTP Grant Program only obtains information that is relevant to adjudicating a grant application. The applications include program descriptions, background, and endorsements related to how the applicant proposes to use DHS funds to prevent targeted violence and terrorism. Also included in the application is organizational information for DHS to review against several government-wide databases to determine whether the organization is financially responsible.

To promote data minimization in the security review process, security reviews will only be conducted for the applications by non-profit organizations that meet the program eligibility requirements and score well in the merit review process. This limits the data collected to a small portion of the full applicant pool. 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; and the name and email and/or phone number of the individuals. I&A may check those limited data elements against currently available departmental, and Intelligence Community holdings; open source and social media resources; and foreign holdings in order to identify information responsive to security factors and to craft a TVTP Grant Program SRR for each applicant for whom responsive information is found.

After reviewing the SRR, the OTVTP Director may convene a working group to further consider the findings. The working group may determine an applicant warrants additional scrutiny before a final recommendation and may request that I&A conduct additional research or analysis.

[20] *See* DHS/FEMA-004 Non-Disaster Grant Management Information Files, 80 FR 13404 (March 13, 2015).

This analysis requires the collection of additional information, to include open source data to ascertain additional information about the organization's key personnel for further assessing the nature of the security risk. This secondary review will consist of the same type of checks conducted during the initial security review.

The SRR itself will be retained by I&A as Finished Intelligence Case Files, labeled as Permanent Records, retained pursuant to the authorized Disposition N1-563-07-016, item 4. Records should be offered to the National Archives and Records Administration for permanent retention 20 years after cutoff.[21] Pursuant to the Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines, 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.[22]

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.

OTVTP and FEMA collect this information and share it with I&A 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. OTVTP and FEMA share the information with I&A to facilitate the security review. I&A shares the results of its analysis with other DHS offices (e.g., oversight offices) so they can supplement the security review, if necessary.

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

Mitigation: 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. The I&A systems have similar controls in place. Additionally, all DHS personnel receive mandatory, annual training on the appropriate handling of PII.

[21] https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/n1-563-07-016_sf115.pdf.
[22] *See* https://www.dhs.gov/sites/default/files/publications/office-of-intelligence-and-analysis-intelligence-oversight-program-and-guidelines.pdf.

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 DHS personnel 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 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 and Intelligence Community holdings; open source and social media resources; 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. 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 TVTP Grant Program 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 or the SRR I&A produces, hold the appropriate security clearances and 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 TVTP Grant Program is the primary federal grant program dedicated to supporting local targeted violence and terrorism prevention programming. The DHS Privacy Office will continue to collaborate with OTVTP, FEMA, and I&A to ensure that appropriate notices appear in TVTP Grant Program NOFOs.

Responsible Officials

David D. Gersten
Director (Acting)
Office for Targeted Violence and Terrorism Prevention
Department of Homeland Security

Approval Signature

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

_____

Dena Kozanas
Chief Privacy Officer
Department of Homeland Security