Privacy Impact Assessment

for the

Public Safety and Violence Prevention (PSVP) Research

DHS Reference No. DHS/S&T/PIA-045

September 3, 2024

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) funds a social and behavioral science research portfolio on public safety and violence prevention (PSVP) that supports the DHS Countering Terrorism and Targeted Violence Strategic Framework[1] and the National Strategy for Countering Domestic Terrorism.[2] S&T funds research in other areas within its social science portfolio; however, this Privacy Impact Assessment (PIA) focuses on the research activities performed by extramural performers as part of the portfolio's ongoing data development for public safety and violence prevention research which may impact the privacy of individuals. This research addresses acts of terrorism[3] and targeted violence,[4] terrorist organizations, and domestic violent[5] extremism[6] (DVE). The S&T-funded projects in the public safety and violence prevention research area include data development for DHS and the broader homeland security enterprise. This Privacy Impact Assessment will address the privacy risks associated with this privacy sensitive research, and the steps S&T takes to ensure this S&T-funded research sustains and does not erode privacy protections. S&T-funded research does not collect personally identifiable information (PII) that DHS would be prohibited from collecting, including information based on the content of the individual's speech or how they express themselves non-violently, their associations, how and whether they choose to worship, or how they

[1] The Strategic Framework and the Public Action Plan are *available at* www.dhs.gov/publication/strategic-framework-countering-terrorism-and-targeted-violence.
[2] *Available at* www.whitehouse.gov/briefing-room/statements-releases/2021/06/15/fact-sheet-national-strategy-for-countering-domestic-terrorism.
[3] 6 U.S.C. § 101(18). The Homeland Security Act defines terrorism as any activity that involves an act that is dangerous to human life or potentially destructive of critical infrastructure or key resources; and is a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and appears to be intended to intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by mass destruction, assassination, or kidnapping. This definition does not distinguish between international and domestic terrorism.
[4] DHS Directive 045-02-01, Programs and Partnerships to Prevent Targeted Violence and Terrorism (March 24, 2022). DHS defines targeted violence as an unlawful act of violence that is dangerous to human life or potentially destructive of critical infrastructure or key resources wherein actors or groups intentionally target a discernible population of individuals or venue in a manner that poses a threat to homeland security. The attack is based on: an apparent terrorist motive indicated by: the population, or the venue targeted, or by the particular means of violence employed, or the significance of actual or potential impacts to the Nation's economic security, public health, or public safety, or to the minimal operations of the economy and government; or the severity and magnitude of the violence or harm and impact of either upon the capabilities of state and local governments to effectively respond without federal assistance.
[5] "Violent" extremism does not include advocacy of political or social positions, political activism, use of strong rhetoric, or generalized philosophic embrace of violent tactics does not constitute violent extremism and may be constitutionally protected.
[6] "Domestic Violent Extremism (DVE)": A domestic violent extremist is defined as an individual based and operating primarily within the United States or its territories without direction or inspiration from a foreign terrorist group or other foreign power who seeks to further political or social goals, wholly or in part, through unlawful acts of force or violence dangerous to human life.

choose to non-violently express their concerns or positions to government.

Introduction

The DHS S&T statutory mission includes "conducting basic and applied research, development, demonstration, testing, and evaluation (RDT&E) activities that are relevant to any or all elements of the Department, through both intramural and extramural programs."[7] S&T's statutory mission also includes "establishing priorities for, directing, funding, and conducting national research, development, test and evaluation, and procurement of technology and systems for … detecting, preventing, protecting against, and responding to terrorist attacks."[8] S&T is the independent research and development Directorate of DHS and carries out this mandate by conducting basic research and applied research. S&T is committed to the protection of privacy, civil rights, and civil liberties in all DHS-funded research.

Social and Behavioral Science Portfolio (SBS)

S&T funds social and behavioral science research pursuant to S&T's statutory mission. This portfolio is conducted by S&T subject matter experts (SME) from a range of academic and professional disciplines including but not limited to behavioral science, economics, criminology, criminal justice, applied anthropology, sociology, psychology, and social work. In addition to scientific SMEs, the portfolio utilizes Program Managers who oversee research activities that support national and Department priorities. Social and behavioral science aids DHS in developing a scientific understanding of how individuals, small groups, and organizations affect threat prevention, deterrence, resilience, security, and recovery activities related to the Homeland Security mission. Knowledge of how human beings behave in, and interact with, the various social contexts they inhabit is an essential component of sound decision-making. To that end, S&T and extramural performers apply behavioral, social, and economic science to advance technologies and knowledge that improve performance, policy, strategy, tactics, techniques, procedures, methods, and operational impacts to the DHS mission. Extramural research is DHS-managed or -funded research that is conducted at non-DHS sites by non-DHS researchers. S&T funds extramural performers from organizations including industrial firms, universities and colleges, non-profit institutions, Federally Funded Research and Development Centers (FFRDC), state and local governments, foreign performers, and private individuals to perform extramural research within the SBS portfolio.

As part of its research mission, SBS funds extramural performers to conduct basic[9] and

[7] 6 U.S.C. § 182(4).
[8] 6 U.S.C. § 182(5).
[9] Basic research "is that RDT&E which is normally conducted without specific applications toward processes or products in mind." *See* DHS/S&T-001 Research, Development, Test, and Evaluation System of Records, 86 Fed. Reg. 58084, (October 20, 2021), *available at* https://www.dhs.gov/system-records-notices-sorns.

applied[10] research that supports the DHS mission while advancing science. SBS develops and applies social and behavioral-based methods, models, training, and technologies that will support resilience throughout all the mission areas of DHS. This is a broad mission space that involves understanding the behaviors of social groups, organizations, and individuals directly related to the research project. DHS Headquarters Offices; DHS operational components; the first responder community; state and local governments; interagency partners, such as the Centers for Disease Control and Prevention (CDC), Department of Health and Human Services (HHS), and the Department of Justice (DOJ); as well as the American people are all beneficiaries of SBS's efforts.

SBS-funded research efforts are designed to address DHS's long-term needs by advancing the state of science and technology in areas that support the DHS mission and enable mission performance of homeland security professionals.

While SBS funds research in other DHS mission areas, this Privacy Impact Assessment is focused on projects that are part of SBS's ongoing research efforts on events of terrorism and targeted violence, terrorist organizations, and domestic violent extremism pursuant to SBS's focus area of PSVP. **National and DHS Strategic Frameworks for Countering Terrorism and Targeted Violence**

In September 2020, DHS published the Public Action Plan for implementing the DHS Strategic Framework for Countering Terrorism and Targeted Violence.[11] This Framework delineates overarching goals to address current, emerging, and future threats.[12] According to the Framework, terrorism and targeted violence "[p]revention efforts must be interdisciplinary, and increase enhanced whole-of-society partnerships with mental health professionals, social service providers, and civil society that can provide 'off ramps' away from terrorism and targeted violence, both protecting the American people and reducing the burden on the criminal justice system."[13]

In October 2020, DHS published a corresponding Strategic Implementation Plan.[14] Through the Public Action Plan and Strategic Implementation Plan, DHS identifies priority actions aligned to achieving the goals in the strategy. All of S&T's funded research efforts in public safety and violence prevention are designed to address at least one priority action in the Implementation Plan and the Strategic Framework Plan through a framework of public safety and violence prevention. S&T funds projects for the Department that support research across all goals.

[10] Applied research "is that RDT&E which is conducted to determine the means, by which a recognized and specific operational need may be met." *See id.*
[11] The Strategic Framework and the Public Action Plan are *available at* www.dhs.gov/publication/strategic-framework-countering-terrorism-and-targeted-violence.
[12] *Id.* at ii.
[13] *See* U.S. DEPARTMENT OF HOMELAND SECURITY STRATEGIC FRAMEWORK FOR COUNTERING TERRORISM AND TARGETED VIOLENCE, *available at* https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf.
[14] *Id.*

Specifically, S&T is tasked with leading the objective to enhance methods to collect and analyze data related to patterns of violence[15] by "explor[ing] DHS's possible roles in compiling national-level statistics…[and] to consolidate relevant data and develop national-level statistics on terrorism [and] targeted violence, including hate crimes."[16]

Further, on June 15, 2021, President Biden released the National Strategy for Countering Domestic Terrorism.[17] The Strategy establishes the pillars and goals of a whole-of-government approach to countering domestic terrorism.[18] S&T-funded research and development efforts support the goals of the Strategy through a framework of public safety and violence prevention. Specifically, the collection, analysis, maintenance, reporting, and dissemination of research findings, final data products, and recommendations on violence further goal one of the Strategy: *Understand and Share Domestic Terrorism-Related Information through enhanced research and analysis*.

Public Health Approach to Public Safety and Violence Prevention

The adoption of a public health approach to public safety and violence prevention promotes a multi-disciplinary strategy to respond to a range of social and behavioral risk and protective factors that affect populations from the neighborhood level to nation-wide. This approach encourages collective action to address societal-level problems, like violence, using methods and strategies from diverse foreign and domestic public and private sectors. The four steps to implementing a public health approach to violence prevention are:

1. Defining and monitoring the problem using reliable data;
2. Identifying risk and protective factors;
3. Developing and testing prevention strategies through evaluation research; and
4. Promoting widespread adoption.[19]

DHS has adopted a public health approach to early prevention across a range of public safety issues, including targeted violence and terrorism.

SBS Public Safety and Violence Prevention (PSVP) Research

The first step in using the public health approach to strengthen public safety and prevent violence is to define and understand the problem through the collection and analysis of reliable

[15] *Id*. at 1.
[16] *Id*. at 1-2.
[17] *See* National Strategy for Countering Domestic Terrorism, *available at* www.whitehouse.gov/briefing-room/statements-releases/2021/06/15/fact-sheet-national-strategy-for-countering-domestic-terrorism.
[18] *Id*. at 15-27.
[19] Centers for Disease Control and Prevention (CDC), National Center for Injury Prevention and Control, Division of Violence Prevention, https://www.cdc.gov/violenceprevention/about/publichealthapproach.html.

empirical data with appropriate safeguards. DHS uses this information to appropriately develop capabilities around risk and protective factors and conduct effective evaluation research. Reliable data underpins the public health approach to violence prevention. The second step is to identify potential risk factors for engaging in different types of violence and corresponding protective factors.[20] These factors are identified by empirical data collection methods and conditions, analyzed using rigorous statistical tools, and validated through public and repeatable processes.

To that end, one of the main areas of focus in SBS's funded research efforts is sponsorship of data development research designed to identify objective, quantitative data that provide valuable insights. SBS-funded research focuses on ensuring reliable data is available, evaluating the effectiveness of locally tailored PSVP efforts and interventions, growing the evidence base for intervention tools, fundamental assessments of public safety threats, including violent extremism and related events, to strengthen public safety and prevent violence. This data will inform strategy and operations of DHS components, interagency partners, and homeland security enterprise partners through strategic allocation of resources, effective program design, and prioritization of threats in the United States. SBS-funded data development efforts support DHS and national priorities to strengthen public safety and counter homeland security threats through prevention.

Data Sources and Elements

Within the public safety and violence prevention portfolio, reliable data that informs the public health approach is, in many cases, retrospective, historical data. S&T does not provide sensitive government data on public safety, terrorism, or targeted violence to funded extramural performers. Instead, S&T's extramural performers acquire their own data, such as, previously collected data, open source data,[21] and publicly available information,[22] the sources of which will vary based on the research activity and may include news media, web forums, social media, organization websites, and other secondary data (e.g., data previously collected and made available for analysis by any extramural performer, either free or for purchase; the U.S. Census Bureau; data developed by Pew Research Center). Similarly, specific data elements collected, used, maintained, or disseminated will vary depending on the research project. Each current or new research project will be described in Appendices to this Privacy Impact Assessment, as appropriate.

---

[20] Risk factors refer to attributes that potentially make an individual more likely to engage in violence, and protective factors are those which potentially make an individual less likely to engage in violence.

[21] DHS Lexicon defines open source as "unclassified information that has been published or broadcast in some manner to the general public, could lawfully be seen or heard by a casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public." Open-source information is a form of publicly available information. *See* https://www.dhs.gov/publication/dhs-lexicon.

[22] DHS Lexicon defines publicly available information as "information that has been published or broadcasted in some manner to the general public, is available to the public by subscription or purchase, could lawfully be seen or heard by a casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public." https://www.dhs.gov/publication/dhs-lexicon.

Additionally, S&T's extramural performers may collect data though interviews, surveys, focus groups, site visits, and other collection methods that may be essential to the research question(s) examined by each PSVP project. When conducting these activities, SBS adheres to the practices outlined in DHS's Surveys, Interviews, and Focus Groups Privacy Impact Assessment.[23] Information on the data used by individual projects and how that data is collected is found in the Appendices to this Privacy Impact Assessment.

Privacy Protections for SBS-Funded PSVP Data Development Activities

SBS extramural performers' data development activities are centered around issues of public safety and violence prevention, including acts or incidents of targeted violence and terrorism, groups who may perpetrate[24] such acts, as well as narrative themes, motivations, or trends that directly relate to such violent acts. SBS extramural performers' data development activities are intended to generate quality data, based on past events, to create or expand a body of knowledge on a given area, and inform recommendations to DHS policymakers. The projects may not intentionally collect, maintain, use, or disseminate the personally identifiable information of any specific individual based on their First Amendment-protected activities. Rather, extramural performers will collect, maintain, use, or disseminate information about an event, such as an act of terrorism or targeted violence, or an organization involved in such an event. However, it is possible that personally identifiable information may be collected incidental to collections about specific targeted violence, terrorism, or domestic violent extremism events, perpetrating organizations, or applicable violent narrative themes,[25] motivations, and/or trends directly related to the act or incident of targeted violence or terrorism. SBS and its extramural performers take several steps to minimize the likelihood of maintaining personally identifiable information in these collections, which are described later in this Privacy Impact Assessment. SBS and its extramural performers cannot and will not make operational decisions about individuals nor share personally identifiable information with an operational DHS component or other law enforcement or security agency unless exigent circumstances arise (such as an actionable and credible threat to life or property).[26] If any sharing must occur under exigent circumstances, SBS will confer with the S&T Privacy Office, the DHS Privacy Office, and the DHS Office of the General Counsel.

---

[23] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR SURVEYS, INTERVIEWS, AND FOCUS GROUPS, DHS/ALL/PIA-069 (2018), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

[24] For purposes of this research, "perpetrator" is defined as a group or individual who is identified as having committed an act of terrorism and/or targeted violence. To be identified as a perpetrator, the group or individual's responsibility is widely reported by credible sources, acknowledged by an authoritative source, or the group or individual has self-proclaimed responsibility for the act.

[25] DHS S&T defines "narrative," when used in extremism research, as a rationale or explanation used by the perpetrator of an attack to explain or justify their violence, often including some sort of grievance or perceived victimhood for which their target(s) are responsible.

[26] *See* DHS/S&T-001 Research, Development, Test, and Evaluation System of Records, 86 Fed. Reg. 58084, (October 20, 2021), *available at* https://www.dhs.gov/system-records-notices-sorns.

Prior to funding a research project, SBS will consult with the S&T Privacy Office to scope the project and intended data collection to ensure that any potentially collected personally identifiable information is minimized to the greatest extent possible. The S&T Privacy Office and S&T counsel will also develop and apply contract clauses and/or specific terms and conditions for agreements with prospective extramural performers to clearly articulate the privacy policy requirements to which the performers are expected to adhere. In turn, SBS will communicate any further data minimization strategies identified during the privacy compliance process to the extramural performers and ensure these recommendations are documented in associated research and/or data development plans, which will be reviewed with S&T Privacy. This will include instructions to extramural performers to avoid taking actions, including collecting or maintaining personally identifiable information based upon an individual's First Amendment-protected activities, that SBS could not do under its own authorities.

Since publicly available information may involve an individual's exercise of rights protected under the First Amendment of the U.S. Constitution, the legal, policy, and privacy analysis, described above, is performed to ensure that S&T-funded research projects do not run afoul of constitutional protections.[27] The DHS Chief Privacy Officer and Undersecretary for Science and Technology have established that DHS privacy policy protections apply to research funded via grants or cooperative agreements. Additionally, S&T funding will not be used to support the collection, maintenance, use, or dissemination of individuals' personally identifiable information based on the content of their speech or how they express themselves non-violently, their associations, how and whether they choose to worship, or how they choose to non-violently express their concerns or positions to government. Non-violent forms of political activism and the political views held by individuals or groups may not provide the basis for collecting personally identifiable information.[28]

Thus, when funding extramural performers via a Federal Acquisition Regulation (FAR)-based contract or Other Transaction Agreement (OTA) for research related to or involving publicly available information, SBS will consult with S&T counsel and the S&T Privacy Office regarding specific constitutional and Privacy Act considerations to determine, respectively, (1) whether the information is protected (e.g., speech protected by the First Amendment); and (2) whether the collection of information is permissible under the Privacy Act.[29] This consultation will include the joint development and implementation of instructions, safeguards, and practices specific to the proposed project to avoid collecting or maintaining information that may be

[27] *See* DHS Memorandum, Information Regarding First Amendment Protected Activities, *available at* https://www.dhs.gov/sites/default/files/publications/info_regarding_first_amendment_protected_activities_as1_signed_05.17.2019.pdf.
[28] *See* Homeland Security Act of 2002, Pub. L. No. 107-296 § 222.
[29] 5 U.S.C. § 552a(e)(7) requires that agencies "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity."

protected by the First Amendment, regardless of funding vehicle.

When funding research that is related to or involving publicly available information, by means other than a FAR-based or OTA contract, SBS will consult with the S&T Privacy Office regarding whether the research falls within the DHS privacy policy covering the collection, maintenance, use, or dissemination of personally identifiable information based on the content of an individual's speech or how they express themselves non-violently, their associations, how or whether they choose to worship, or how they choose to non-violently express their concerns or positions to government. This consultation will include the joint development and implementation of safeguards and practices specific to the proposed project to avoid collecting or maintaining personally identifiable information inconsistent with this Privacy Impact Assessment and the terms and conditions of the applicable Notice of Funding Opportunity (NOFO) or the award funding the research project.

If appropriate for the specific research project, when searching publicly available sources for information to use in a data development activity for example, S&T's extramural performers are instructed to use keywords related to specific targeted violence, terrorism, or domestic violent extremism events, perpetrating organizations, or applicable violent narrative themes, motivations, and/or trends directly related to the act or incident of targeted violence or terrorism and not profile, target, or discriminate, against any individual based on the content of their speech or how they express themselves non-violently, their associations, how or whether they choose to worship, or how they choose to non-violently express their concerns or positions to government. To further avoid collecting or maintaining information about individuals, extramural performers will be prohibited from searching for information using an individual's name or other personally identifiable information[30] except in limited circumstances as described in appendices. Extramural performers will be instructed to use source material that is about specific targeted violence, terrorism, or domestic violent extremism events, perpetrating organizations, or applicable violent narrative themes, motivations, and/or trends directly related to the act or incident of targeted violence or terrorism and not source materials about individuals. If extramural performers identify a potentially useful source document that is about an individual, the extramural performer may not collect, maintain, use, or disseminate that document if the collection is based upon the content of an individual's speech, how they express themselves non-violently, their associations, how and

[30] DHS defines "personally identifiable information" as any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the United States, or employee or contractor to the Department. Such information includes a name, Social Security number, date and place of birth, mother's maiden name, A-Number, account number, license number, vehicle identifier number, license plate number, device identifier or serial number, internet protocol address, biometric identifier (e.g., facial recognition photograph, fingerprint, iris scan, voice print), educational information, financial information, medical information, criminal or employment information, information created specifically to identify or authenticate an individual (e.g., a random generated number).

whether they choose to worship, or how they choose to non-violently express their concerns or positions to government. Furthermore, any newspaper articles, journal articles, or other publicly available documents identified through the extramural performers' keyword searches for use as source materials will be maintained and organized with respect to the specific targeted violence, terrorism, or domestic violent extremism event, perpetrating organization, or applicable violent narrative theme, motivation, and/or trend directly related to the act or incident of targeted violence or terrorism that is the subject of the research. These materials will not be collected, maintained, used, or disseminated with respect to an individual. To the extent that an SBS extramural performer may incidentally collect, maintain, or use information about an individual during a data development activity, this information about an individual will not be shared with S&T or included in any deliverable described, regardless of funding vehicle.

Regardless of funding vehicle, SBS will work with its extramural performer and the S&T Privacy Office to devise procedures for each project to minimize further the likelihood of inappropriately collecting or maintaining personally identifiable information. SBS's extramural performers, in every S&T-funded PSVP project, will limit the collection, maintenance, use, and dissemination of personally identifiable information to only the information necessary to implement their project and in accordance with the Privacy Act (for contracted research) and DHS privacy policy (for research funded through grants, cooperative agreements, and contracts). The Appendices to this Privacy Impact Assessment will be updated for each new funded research activity to provide transparency to the public, to enable the assessment of potential privacy risks, and to document mitigation strategies for individual projects.

Data Development Research

SBS will seek the support of scientists and SMEs outside of DHS to conduct data development research and address strategic research goals. SBS has access to a network of scientists and SMEs through national laboratories, university Centers of Excellence (COEs), and Federally Funded Research and Development Centers, none of which are addressed in this Privacy Impact Assessment. S&T may issue grants,[31] contracts,[32] cooperative agreements,[33] and interagency agreements, which are the subject of this Privacy Impact Assessment, to a wide range of entities in the scientific community including private industry, universities, or research institutions to access the scientists and SMEs.

SBS Program Managers and SMEs will work with procurement, privacy, legal, and compliance experts to ensure that appropriate procurement vehicles are used to identify potential extramural performers, develop evaluation criteria, review proposals, review research outputs for scientific quality and rigor, and ensure that sufficient privacy, legal, and policy protections are

[31] 2 C.F.R. §200.51.
[32] 48 C.F.R. §2.101 "Contract".
[33] 2 C.F.R. §200.24.

established at the outset through specific privacy terms and conditions when making awards for proposed research projects. SBS will draw on its experience in conducting, leading, and evaluating ethical research designs to ensure all funded research is conducted in an ethical and responsible manner and that the Program Managers can validate and verify that extramural performers are abiding by the parameters of this Privacy Impact Assessment on an ongoing basis. During this process, when necessary, S&T staff also will engage with appropriate staff from partnering DHS components to confirm their participation in S&T's source selection evaluation boards and ensure research proposals meet DHS component needs, prior to an award being issued.

SBS Program Managers and SMEs follow established processes common throughout the government when seeking to fund research projects and use several different funding vehicles to support SBS projects. S&T will announce grants and cooperative agreements through NOFOs and will announce new Federal Acquisition Regulation-based contracting opportunities through Requests for Proposals (RFP). These announcements will contain a description of the research areas of interest, research objectives and needs, eligibility criteria, evaluation criteria, any pertinent information that organizations need to develop a proposal (such as amount of funding available), and any data security requirements. These announcements (and subsequent awards made pursuant to these announcements) will also contain privacy-specific terms and conditions or clauses that clearly articulate privacy policy and privacy compliance requirements that pertain to S&T, its extramural performers, and any further entities engaged by extramural performers to execute a funded research activity.

Regardless of how the project is funded, DHS privacy SMEs will complete a privacy analysis before the project is funded and advise on appropriate privacy safeguards in accordance with the Homeland Security Act of 2002 and DHS privacy policy (specifically Privacy Policy and Compliance Directive 047-01[34] and Policy Directive 140-03[35]). For research funded through Federal Acquisition Regulation-based contracts, the privacy analysis and safeguards will also be subject to the Privacy Act of 1974, as amended.

S&T will institute a matrixed approach (e.g., involving the procurement, privacy, legal, and compliance experts discussed above) to work with program management to review and accept research outputs and monitor extramural performers' projects for compliance with the established requirements. DHS S&T SMEs will review research outputs for scientific quality, rigor, and alignment to stated objectives. DHS Program Managers will ensure that the project remains on time and on budget while managing the day-to-day administration and oversight of the project for the government. S&T Program Managers, SMEs, and S&T and DHS Privacy officials will review the research applications and any additional documentation provided to DHS before the project is

[34] *See* https://www.dhs.gov/publication/privacy-policy-and-compliance-directive-047-01.
[35] *See* https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles.

funded, to assess the extramural performer's proposed implementation of the privacy-specific terms and conditions.

If research is being conducted under a Financial Assistance instrument, the extramural performer should include a description of their data collection methodologies as part of their NOFO application, which will be one of the evaluation criteria for the technical review team. S&T Program Managers, SMEs, and S&T Privacy officials will review the description of the proposed data collection to ensure it aligns with the privacy-specific terms and conditions included in the award agreement.

For FAR-based contracts, the Program Manager will work with the Contracting Officer to include a required data collection plan under the contract. DHS S&T Privacy will review the data collection plan to ensure it aligns with legal and policy privacy requirements. The benefits of developing a data collection plan include:

- Experts from the extramural performer may provide cutting-edge, state of the science recommendations for how to conduct data collection in the most efficient manner; and
- S&T will approve the data collection plan before the project commences. This will include consultation with the S&T Privacy Office and counsel to ensure the collection of any personally identifiable information is minimized to the greatest extent possible and information collection is consistent with the Privacy Act of 1974, OMB guidance, and DHS privacy policy, as appropriate.

For FAR-based contracts that include data collection, the Program Manager will request and provide instructions on how to develop the data collection plan, and the S&T SME, the S&T Privacy Office, and—at the Program Manager's request—S&T counsel will review the draft data collection plan and provide technical feedback before the Contracting Officer's Representative (COR) accepts the final version.

SBS Research Methods

Once a project is under way, there are additional steps SBS will take to ensure the scope of data collected by an extramural performer for a project is limited to only that which is necessary to accomplish the research objective.

Literature Reviews

Violence prevention, especially from terrorism and targeted violence, is a field that is rapidly changing. Accordingly, it is routine that SBS requires extramural performers to complete literature reviews or state of the science summaries as one of the first thematic outputs on many projects. Literature reviews are a systematic examination of the existing corpus of previously published academic research that is germane to a given subject. These reviews arm the Principal Investigator with both the most relevant and most recent research that can help guide the Principal

Investigator to areas that may be under-researched and are thus worthy of further study. Literature reviews also help to inform the next step in the research process or the development of an operational definition. Extramural performers conducting literature reviews may collect, maintain, use, and disseminate the personally identifiable information of the authors or researchers responsible for the previously published academic research, as it is necessary to provide appropriate citations.

Operational Definitions

Operational definitions are constructed by the extramural performer, in consultation with SBS, to describe things not necessarily observable directly, but that still need to be observed, quantified, and analyzed—one example might be popularity. Popularity, as an abstract concept, is not directly observable. Certain proxies, however, are observable. Literature reviews enable the Principal Investigator to determine which proxy variables were successfully employed in previous research that would suggest a likelihood of future success.

Inherent to developing operational definitions are inclusion and exclusion criteria. Inclusion criteria describe what characteristics a piece of data must possess to be included; exclusion criteria describe characteristics that a piece of data must not possess. For example, a database analyzing terrorist groups might have the following inclusion criteria: 1) must be an organized group with a hierarchy, 2) must be in operation in 2022, and 3) must be active in the United States. Exclusion criteria would be the opposites of the inclusion criteria but could also include other factors.

Coding Schemes

After an extramural performer articulates the operational definition for a given variable, such as hierarchy, the variable is then organized in a cascading list called a coding scheme. A fully developed coding scheme, which might be Code 1 - Leaderless, Code 2 - Multiple Leaders, Code 3 - Single Leader, allows extramural performers to then "code" the entire dataset using this coding scheme. Once everything has been coded, analysis might include a comparison of frequency of different codes run through various statistical tests. Operational definitions, and the coding schemes, can change as new themes and observations emerge. Similarly, themes can change as extramural performers develop newer understandings of a concept that may require different ways of observing the data. Coding schemes and definitions are generally well tested before data collection fully begins, but are adaptable as the need arises, and the DHS Program Manager and SME review and advise on definitions and coding schemes before they are finalized.

Thematic Analysis

Thematic analysis is a method used to make sense of qualitative data (e.g., interview transcripts, text analysis, message boards). One common approach to dealing with qualitative data is grounded theory approach, where extramural performers attempt to identify patterns or

reoccurring observations in qualitative data, then group them with other similar observations, and compare and contrast the groups. In the instance of a public message board, researchers could, for example, read every post over a seven-day period, then group similar posts together based on shared elements. Once they are grouped together, extramural performers apply labels to describe what makes the individual posts similar. As noted previously, speech-based research is restricted to non-First Amendment protected activity (e.g., violence).

Mitigating and Acknowledging Bias

Science attempts to remove as much bias as possible through creating objective and repeatable measurements so that a replicated study would find the same or very similar results. However, not all bias is avoidable, so scientific reports generally have a section where the authors state whatever biases the study has. For example, it could be a sampling bias where only men over the age of 45 were asked to complete a survey, so the bias in this example is that the results are limited to that demographic, and specifically excludes women and all people under 45. Another common form of bias is measurement bias, where the tools used to collect data were not precise enough to give a perfect reading, so the results may be skewed one way or another.

One way to mitigate bias in thematic analysis is the development of the coding scheme. The scheme is then tested and refined so it is both accurate and precise. Once the coding scheme and protocol have been tested, the Principal Investigator trains the rest of the research team on how to use it. This ensures interrater reliability, or the confidence that if two or more people are trained to the same degree on the same tools and protocols, then they should reach the same or very similar conclusions when reviewing the same data. So, the measurements and the coding scheme may be biased, but the application of the coding is at least uniformly biased in the same way to assure that if another research team utilizes the same methods, with the same tools, on the same data, they will achieve the same results.

It is important to note that these coding schemes do not carry any moral judgments. The coding schemes and inclusion or exclusion criteria are based on definitions used throughout DHS, and the classifications are focused solely on objective and measurable behaviors. For these reasons, DHS S&T always strives to use transparent, empirical, and repeatable methods to conduct scientific analyses, and to apply these methods as consistently as possible.

Accessing and Collecting Information

Extramural performers may access information concerning individuals to achieve their research objectives; however, for SBS FAR-based-contracted PSVP projects to collect any information about how an individual exercises their rights under the First Amendment, the collection must fall within one of the following three exceptions: the collection must be authorized by statute, made with consent of the individual, or be pertinent to and within the scope of an

authorized law enforcement activity.[36] SBS PSVP research funded under grants or cooperative agreements is deemed privacy sensitive by the Chief Privacy Officer and Undersecretary for Science and Technology; therefore, researchers funded by grants and cooperative agreements (absent consent from the individual) may access, but not collect, information based upon the content of an individual's speech, how they express themselves non-violently, their associations, how and whether they choose to worship, and how they choose to non-violently express their concerns or positions to government.

Accessing information occurs when SBS extramural performers view or examine information for research purposes but do not store or otherwise maintain under their control such information. Access is distinct from collection. Collection occurs when information accessed by SBS extramural performers is brought into a DHS or extramural performer system or is otherwise stored or maintained. For example, if an extramural performer merely views information concerning an individual's non-violent activity online, that information would be "accessed." However, if the extramural performer retains the personally identifiable information of the individual and stores the information electronically or in a physical file system (e.g., copies and pastes or transcribes the information into a separate document), the information would be "collected," which is not permissible for FAR-based-contracted research partners under the Privacy Act absent one of the three exceptions mentioned above. Under DHS privacy policy, collection would not be permissible for research partners funded under cooperative agreements or grants. The information is still considered collected even if the information is subsequently redacted. To satisfy the legal and/or policy requirements described above, personally identifiable information based upon the content of an individual's speech, how they express themselves non-violently, their associations, how and whether they choose to worship, and how they choose to non-violently express their concerns or positions to government will be anonymized after accessing and before collecting. Moreover, anonymized information will not be combined with additional information to identify an individual.

SBS extramural performers may access and collect information that *does not* implicate individuals' First Amendment-protected activity consistent with S&T authorities and the privacy-specific terms and conditions stipulated in the applicable NOFO, FAR-based contracts, grants, and cooperative agreements. Such information must be collected overtly[37] and from publicly available sources. SBS extramural performers may appropriately use this information for research purposes, if the information *excludes* how individuals exercise their First Amendment rights. In exercising this authority to access and collect information, SBS extramural performers will minimize the amount of personally identifiable information collected. SBS extramural performers will take

[36] 5 U.S.C. § 552a(e)(7). To be within the scope of an authorized law enforcement activity, any contracted PSVP research project must partner with a DHS component with law enforcement authorities.
[37] "Overt collection" is the collection of information openly acknowledged by or readily attributable to the government, or where no steps are taken to conceal the sponsor of the research activity.

further actions to mitigate privacy risks, such as by redacting or expunging personally identifiable information after it is collected.

SBS extramural performers will use reliable data to identify risk and protective factors for terrorism, targeted violence, and extremism violence that may include publicly available information. Although empirical data collection is the primary collection method, SBS may also acquire publicly available information that relates to and is consistent with an authorized purpose.

Mitigation Measures to be Applied to Publicly Available Information and Social Media Information

- Review of Governance Documentation (e.g., data management plans or data collection plans as referenced above): There is a risk that the work will be inconsistent with fair information practice principles, such as data minimization, use limitation, and data quality and integrity. This risk is partially mitigated as S&T will review each project's governance documentation, regardless of funding vehicle, before the research begins. This will include consultation with S&T counsel and approval by the S&T Privacy Office to ensure the collection of any personally identifiable information is minimized to the greatest extent possible and no information describing how an individual exercises rights guaranteed by the First Amendment is collected, maintained, used, or disseminated.

  Likewise, for research being conducted under a Financial Assistance instrument, the extramural performer will include a description of their data collection methodologies as part of their NOFO application, which will be one of the evaluation criteria for the technical review team. S&T Program Managers, SMEs, and S&T Privacy officials will review the description of the proposed data collection to ensure it aligns with the privacy-specific terms and conditions to be included in the award agreement. For FAR-based contracts, the Program Managers will work with the Contracting Officer to include a data collection plan as a deliverable under the contract. S&T Privacy will review the data collection plan to ensure it aligns with the appropriate legal and policy requirements. Eligibility requirements enabling data collection and management that align with the privacy-specific terms and conditions will be built into the notice of funding and technical evaluation criteria for grants and cooperative agreements.

- Terms of Service: There is a risk that accessing publicly available information and social media may be inconsistent with the use limitation principle. This risk is partially mitigated as SBS extramural performers will only access publicly available information, including information available on social media platforms, consistent with the established terms of service of those respective sites or platforms. Any collection and subsequent use of information from such sites or platforms will either adhere to any limitations imposed on account holders through the site or platform's terms of service or through processes that

would permit the collection and use to be admissible in a court of law. SBS's extramural performers will access and retain a copy of the relevant Terms of Service of each website accessed, and review monthly the Terms of Service for each website accessed within the last 30 days. If the Terms of Service have been updated, a copy of the updated Terms of Service must be retained.

- Network Analysis: SBS does not perform or fund network analysis and does not intend to perform or fund network analysis. Network analysis, also often referred to as "link analysis," refers to an analytic technique to graphically analyze and illustrate the linkage between organizations and individuals within a network. If SBS changes its position on network analysis, this Privacy Impact Assessment will be updated accordingly.
- Limitation on Emotion Detection and Analysis: SBS does not perform or fund emotion detection and analysis and does not intend to perform or fund emotion detection and analysis. If SBS changes its position on emotion detection and analysis, this Privacy Impact Assessment will be updated accordingly.
- Keyword Queries: There is a risk that using keywords to search an individual's publicly available information or social media information may violate the purpose specification principle. This risk is partially mitigated because any keywords used to query publicly available information will be designed in such a way as to not profile, target, or discriminate, based upon the most recent Department of Justice guidance[38] and DHS training as described below, against any individual based on the content of their speech and how they express themselves non-violently, their associations, how and whether they choose to worship, and how they choose to non-violently express their concerns or positions to government. For example, keywords used will focus thematically on events, narratives, or actions, rather than individuals or their personally identifiable information. To ensure that keyword searches are conducted in an authorized manner and free from bias, keywords used to query publicly available information or social media information will be documented and may be periodically reviewed, by the S&T Privacy Office, the DHS Privacy Office, and the DHS Office for Civil Rights and Civil Liberties, consistent with their authorities.
- Risk Profiles: SBS does not use or fund research that includes creating or using risk profiles of individuals or groups and does not intend to use or fund research involving risk profiles on individuals or groups. If SBS changes its position on risk profiles, this Privacy Impact

[38] Department of Justice "Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, Gender Identity, and Disability," *available at* https://www.dhs.gov/publication/guidance-federal-law-enforcement-agencies-regarding-use-race-ethnicity-gender-national

Assessment will be updated accordingly.

- Training: The S&T Privacy Office will develop and offer training on the implementation of publicly available information and social media privacy mitigation measures to SBS extramural performers.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[39] 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.[40]

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.[41] 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 the E-Government Act of 2002, Section 208[42] and the Homeland Security Act of 2002, Section 222.[43] Because SBS is a program rather than a particular information technology system, this Privacy Impact Assessment is conducted as it relates to the DHS construct of the Fair Information Practice Principles. This Privacy Impact Assessment examines the privacy impact of SBS-funded research projects related to public safety and violence prevention as they relate to the DHS Fair Information Practice Principles.

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.

S&T's data development efforts related to PSVP[44] are aligned with the priority actions

[39] 5 U.S.C. § 552a.
[40] 6 U.S.C. § 142(a)(2).
[41] 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/privacy-policy-guidance.
[42] 44 U.S.C. § 3501 note.
[43] 6 U.S.C. § 142.
[44] *See* https://www.dhs.gov/CP3.

identified in the DHS Strategic Framework for Countering Terrorism and Targeted Violence and the ensuing Strategic Implementation Plan. Specifically, S&T is tasked with leading DHS efforts to fulfill the objective to enhance methods to collect and analyze data related to patterns of violence by "explor[ing] DHS's possible roles in compiling national-level statistics … [and] to consolidate relevant data and develop national-level statistics on terrorism, targeted violence, including hate crimes."[45]

S&T provides additional notice to the public about its funded PSVP projects in its related Requests for Proposals, Notices of Funding Opportunity, and Long-Range Broad Agency Announcements (LRBAA).[46] These announcements contain a description of the research objectives and needs, eligibility criteria, evaluation criteria, and any pertinent information that organizations need to develop a proposal (such as amount of funding available).

Lastly, this Privacy Impact Assessment provides notice to the public regarding SBS-funded research on PSVP, as well as the information SBS research partners collect, use, store, and maintain when conducting SBS-funded research. This Privacy Impact Assessment includes appendices to provide additional transparency on specific research projects.

Privacy Risk: There is a risk that the government will not provide transparency to the public that universities, nonprofits, and other partners conduct privacy sensitive research and other PSVP research funded by S&T.

Mitigation: The risk is mitigated. With limited exceptions, S&T makes its research outputs available to the public through a variety of outlets including press releases, Congressional Notices, the S&T/DHS publications website, academic journals, and professional/academic conferences. Further, most grants, cooperative agreements, and FAR-based contracts include language in the signed agreements that the extramural performer must disclose that the work was funded (either all or in part) by DHS including (where applicable) the specific grant or contract award number. To remain transparent and to acknowledge any (perceived or real) biases, most academic, scientific, and professional publications and conferences have ethics rules mandating that researchers disclose their funding sources in all publications and presentations.

Privacy Risk: There is a risk that individuals whose data will be collected by S&T's extramural performers do not have a clear understanding about S&T's use of the data collected.

Mitigation: This risk is partially mitigated. This Privacy Impact Assessment, its appendices, any subsequent updates to this Privacy Impact Assessment, the DHS 2019 Countering Terrorism and Targeted Violence Strategy, S&T Long-Range Broad Agency Announcements, Notices of Funding Opportunities, and Requests for Proposals, as well as the final research

[45] *See* www.dhs.gov/publication/strategic-framework-countering-terrorism-and-targeted-violence.
[46] *See* https://www.dhs.gov/science-and-technology/st-lrbaa and https://sam.gov/content/home.

products, which are made publicly available, provide the public with information about extramural performer-led collections funded by S&T.

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.

SBS's funded data development projects are intended to generate quality data, based on past events, to build the body of knowledge on a given area and inform recommendations to DHS policymakers. Specifically, these projects are focused on PSVP, including acts or incidents of targeted violence or terrorism, and the motivations that spur such violent acts. SBS extramural performers do not seek to collect, maintain, use, or disseminate personally identifiable information about any specific individual. Further, SBS and its extramural performers cannot and will not make operational decisions about individuals. SBSs extramural performers will not share personally identifiable information with an operational DHS component or other law enforcement or security agency unless exigent circumstances arise.

Except for information obtained from consenting individuals through surveys, interviews, and focus groups, all information that SBS extramural performers collect for PSVP data development activities is publicly available on publicly accessible websites using methods available to the public. Information collected by extramural performers is focused on past specific targeted violence, terrorism, or domestic violent extremism events, perpetrating organizations, or applicable violent narrative themes, motivations, and/or trends directly related to the act or incident of targeted violence or terrorism. If any incidental collection of personally identifiable information occurs, extramural performers will take steps to scrub the personally identifiable information before sharing the results of their research. Although such performers take steps to scrub personally identifiable information before sharing the results of their research with DHS, individuals may submit a Freedom of Information Act (FOIA) or Privacy Act request to access or correct information maintained by DHS that relates to SBS's funded data development projects. Individuals may submit requests to the Privacy Office: Chief Privacy Officer/Chief Freedom of Information Act Officer, U.S. Department of Homeland Security, 2707 Martin Luther King Jr. Avenue, S.E., Washington, D.C. 20528-0628, or electronically at https://www.dhs.gov/foia-contact-information.

Privacy Risk: There is a risk that individuals will be unaware that their publicly available information may be accessed by SBS-funded extramural performers.

Mitigation: The risk is partially mitigated. These collections are focused on PSVP, including historical specific targeted violence, terrorism, or domestic violent extremism events, perpetrating organizations, or applicable violent narrative themes, motivations, and/or trends

directly related to the act or incident of targeted violence or terrorism, not on the individuals themselves. While SBS extramural performers do not provide individuals notice prior to accessing or collecting publicly available information, except for the notice provided through this Privacy Impact Assessment, SBS extramural performers only collect open source and publicly available information and may not attempt to bypass privacy settings, such as by "friending" or "liking" user accounts. SBS provides notice of this collection of information from publicly available sources through this Privacy Impact Assessment, Requests for Proposal, Notices of Funding Opportunity, and Long-Range Broad Agency Announcements.

Privacy Risk: There is a risk that an individual will not know how to correct inaccurate information about themselves that is used in SBS-funded data development activities.

Mitigation: The risk is partially mitigated. For data development activities involving the creation of new datasets, the extramural performers who collect and maintain information for use in the datasets they make available to the public will include procedures to correct inaccurate information. For instance, an extramural performer will post contact information to a project helpdesk where individuals can supply information to correct any inaccuracies.

Privacy Risk: There is a risk that individuals may be unaware that someone has publicly posted information about them that may be available to S&T for research purposes.

Mitigation: This risk is partially mitigated. This Privacy Impact Assessment, and any appendices to this Privacy Impact Assessment, provide notice that S&T-funded extramural performers are accessing and possibly collecting publicly available online content for RDT&E. As part of this initiative, SBS extramural performers only access and collect information that is publicly available, and limit collection of information to past specific targeted violence, terrorism, or domestic violent extremism events, perpetrating organizations, or applicable violent narrative themes, motivations, and/or trends directly related to the act or incident of targeted violence or terrorism.

Privacy Risk: There is a risk that an individual may be categorized as being part of an ideological group.

Mitigation: The risk is mitigated. The projects may not intentionally collect, maintain, use, or disseminate the personally identifiable information of any specific individual. Additionally, SBS research is focused on historical specific targeted violence, terrorism, or domestic violent extremism events, perpetrating organizations, or applicable violent narrative themes, motivations, and/or trends directly related to the act or incident of targeted violence or terrorism rather than specific individuals. This Privacy Impact Assessment details the rigorous steps that S&T and their extramural performers employ to collect empirical, objective, and accurate data as consistently as possible. These methods are routinely published in reports and publications and discussed at conferences where other subject matter experts can comment and critique, as necessary. Findings

are either supported through replication, accepted based on the soundness and rigor of the methods that were used to collect data and perform analyses, or are refuted and revised through peer-review.

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.

S&T's statutory mission is "conducting basic and applied RDT&E activities that are relevant to any or all elements of the Department, through both intramural and extramural programs."[47] SBS-funded research projects in the PSVP space are completed in furtherance of the 2019 DHS Strategic Framework for Countering Terrorism and Targeted Violence, the 2020 Strategic Implementation Plan for the Framework, and the 2021 National Strategy for Countering Domestic Terrorism.

S&T PSVP subject matter experts coordinate with privacy, legal, and compliance experts to ensure that appropriate procurement vehicles are used to identify potential extramural performers, develop evaluation criteria, review proposals, and review deliverables for scientific quality and rigor. When appropriate, S&T staff also engage with staff from partnering DHS components to ensure their participation prior to an award being issued. When issuing a Notice of Funding Opportunity, Long-Range Broad Agency Announcement, or Request for Proposal, S&T will also publish the objective and clear criteria used to evaluate the research proposals received.

Privacy Risk: There is a risk SBS's extramural performers may retain data longer than necessary.

Mitigation: This risk is partially mitigated. One of the objectives of peer-reviewed research is to make all findings and supporting datasets publicly available to spur further research on the subject. SBS-funded research pursued via a grant or cooperative agreement is intended to serve a public purpose — the benefits extend to the American people writ large, not just S&T or DHS. Due to the nature of grants and cooperative agreements, S&T's extramural performers retain ownership of the underlying data they collect and produce. As a result, this data is not subject to federal records retention requirements. Nevertheless, SBS extramural performers and S&T program staff will coordinate with S&T counsel and the S&T Privacy Office to ensure that research topic areas and data collection plans are appropriately scoped to minimize the information collected to that which is necessary to conduct the research.

For FAR-based contracts, disposition of data is driven by the terms of the contract. When the data for a contracted research project is included as a deliverable to S&T, that data is then subject to federal records retention requirements.

[47] 6 U.S.C. § 182(4).

Further, federal regulations require research records to be retained for at least three years after the completion of the research (45 C.F.R. Part 46), and some institutional review boards (IRB) may independently recommend or mandate as many as five or more years as governed by some Health Insurance Portability and Accountability Act (HIPAA) regulations. These retention policies are in place to 1) protect the extramural performers from any accusations of scientific misconduct, and 2) to facilitate contacting research participants should their health or safety be in jeopardy. The necessity to contact research participants is primarily for health-related and clinical research studies in which SBS does not engage. Nevertheless, the IRBs that review SBS-funded research typically do impose these protections for all human-subjects research.

Privacy Risk: There is a risk that information collected during SBS-funded PSVP research projects may be used for non-research purposes.

Mitigation: The risk is partially mitigated. As outlined in this Privacy Impact Assessment, DHS S&T makes its funded research available to the public which includes members of government agencies who may benefit operationally from this information. Additionally, DHS components may access the publicly available results of SBS-funded research. Sometimes DHS operational components are either direct or indirect customers of S&T-funded research, but extramural performers may not share the raw data (e.g., individual survey responses, focus group notes) with these components or S&T. Data shared with DHS operational components would be limited to aggregate data, trends, and summary results, observations, and recommendations. If any sharing must occur because of exigent circumstances (e.g., the extramural performers discover or witness an imminent, specific credible threat of violence) extramural performers will follow the procedures established at their respective institutions and/or DHS guidance according to Duty to Report protocols.

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).

S&T extramural performers scope RDT&E to a specific domain and/or use before initiation of the project. As a result, the collection of any data, including personally identifiable information, that falls outside the scope of an RDT&E activity is minimized. During RDT&E, extramural performers employ several methods, such as keywords and geofences,[48] to further minimize the information collected to what is relevant and required for the RDT&E activity. For example, geolocation data is not collected. Extramural performers may discover and implement additional ways to minimize data as part of the research activity.

[48] Geofencing is a technology that defines a virtual boundary around a real-world geographical area.

After an award has been issued, S&T staff within the PSVP portfolios that require data development work with the extramural performers on the development of a data collection plan. The development of the data collection plan will provide two benefits:

- Extramural performer SMEs will be able to provide cutting-edge, state of the science recommendations for how to conduct data collection in the most efficient manner; and
- When applicable, SBS will review the draft data collection plan before work commences and provide guidance to ensure the appropriate information is collected to complete activities within the scope of work. As part of the privacy compliance process, the data collection plan will be submitted to the S&T Privacy Office to review and ensure the appropriate safeguards are in place to minimize any privacy impact on individuals before data collection commences.

In addition to scoping collection of information to only what is relevant to the project, SBS extramural performers will also endeavor whenever possible to strip, remove, or redact personally identifiable information from the information they collect. For instance, any data collected from social media platforms will be anonymized and usernames will not be used or tracked. Extramural performers may use technical means to strip personally identifiable information, such as usernames, from information accessed online before the information is stored on the systems of SBS's extramural performers for RDT&E purposes. SBS's extramural performers may also manually redact or obfuscate personally identifiable information before storing the information.

It is important to note that these data development efforts examining acts of terrorism and targeted violence and violent extremism only use historical data for retrospective analysis. Since data is pulled from open-source, publicly available sources, there is a significant lag between when an event occurs and when it appears in a dataset. During this time, the event must be reported in the media, identified in a keyword search, coded based on predetermined criteria, quality control checked, and entered into a database. This lag usually varies between several weeks and six months.

SBS and extramural performer personnel will receive project-specific guidance, including but not limited to, from S&T counsel and the S&T Privacy Office when scoping each research effort. Constitutional and/or Privacy Act analysis will also foster data minimization efforts. For instance, the S&T Privacy Office and counsel will determine whether the information proposed to be collected is protected by the First Amendment to the U.S. Constitution, which is impermissible under the Privacy Act of 1974.[49]

Privacy Risk: There is a risk that S&T FAR-based contract extramural performers will collect, maintain, use, or disseminate information that describes how an individual exercises

[49] 5 U.S.C. § 552a(e)(7).

rights guaranteed by the First Amendment, or that extramural performers funded through grants or cooperative agreements will support the collection, maintenance, use, or dissemination of individuals' personally identifiable information based on the content of their speech or how they express themselves non-violently, their associations, how or whether they choose to worship, or how they choose to non-violently express their concerns or positions to government.

Mitigation: This risk is partially mitigated as S&T counsel and the S&T Privacy Office will provide SBS and its extramural performers guidance when scoping their research efforts. The S&T Privacy Office and S&T counsel will develop and offer training on the implementation of publicly available information and social media mitigations to SBS extramural performers. In addition, each FAR-based contracted project involving the collection of publicly available information from social media platforms will complete the proper privacy compliance documentation, such as a "Social Media Operational Use Template" (SMOUT), a Privacy Threshold Analysis (PTA), and a new or updated appendix to this Privacy Impact Assessment prior to social media information collection. For projects involving the collection of publicly available information from social media platforms that are funded via a financial assistance agreement, a new or updated appendix to this Privacy Impact Assessment will be completed prior to social media information collection. Each appendix describes any unique privacy risks involved with a specific research effort that are not captured in the main body of the Privacy Impact Assessment. This privacy compliance documentation process will include determinations from the DHS and S&T privacy offices and counsel as to whether information to be collected may be protected by the First Amendment or through the application of DHS policy. Lastly, SBS extramural performers collect all data only for research purposes and not to make any operational decisions regarding any individual.

Privacy Risk: There is a risk S&T's extramural performers will collect more information than necessary to perform their PSVP RDT&E activities.

Mitigation: The risk is partially mitigated. Prior to the initiation of a research project, SBS consults with the S&T Privacy Office, S&T counsel, and other DHS SMEs to provide contextualization and explanation of how the pending research responds to research requirements outlined in DHS strategic documents. Prior to data collection, extramural performers develop data collection plans, including operational definitions of research variables of interest, to narrow the data collected to only that which is necessary to address the research topic. This information is included in the documents provided by SBS for review by the S&T Privacy Office and (if necessary) the DHS Office of the General Counsel (OGC). Extramural performers are evaluated based on prior experience and expertise in both the subject matter and the proposed research methodology. This experience provides the extramural performers with an understanding of what information is relevant and what is extraneous so that extraneous information is not collected.

Privacy Risk: There is a risk that information collected may not be sufficiently

anonymized due to its specificity.

Mitigation: The risk is partially mitigated. SBS extramural performers work with the S&T Privacy Office, counsel, the DHS Compliance Assurance Program Office (CAPO), and institutional review boards to review and approve data collection and data storage procedures for each project. This process includes the establishment of safeguards that ensure all data collected is sufficiently anonymized. Additionally, researchers are not permitted to link or attempt to link research data to an individual.

5. Principle of Use Limitation

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

One objective of SBS-funded research efforts is to generate new data and new statistics on terrorism and targeted violence that can be used to enable informed decision-making. One of S&T's responsibilities in fulfilling its obligations under the 2019 Strategic Framework for Countering Terrorism and Targeted Violence is the widespread dissemination, as appropriate and consistent with authorities, of analysis, findings, recommendations, and, in some cases, datasets, to increase awareness across the homeland security enterprise. An important aspect of research is the ability to validate the results through replication studies. Therefore, source documentation used to create datasets must be accessible.

SBS's PSVP data development efforts focus, in most cases, on analyzing historical events. S&T PSVP data development efforts involving the collection of social media information focus exclusively on analyzing historical events. These research efforts are not concerned with specific individuals and any personally identifiable information associated with the event itself is not relevant to the analysis. For example, a news article about a terrorist event may include a witness statement but the extramural performers will not collect the statement made by the witness nor any personally identifiable information about the witness.

Privacy Risk: There is a risk that information collected by researchers may be used for purposes inconsistent with the original purpose of the collection.

Mitigation: The risk is mitigated. DHS S&T and its extramural performers work with DHS OGC, DHS and S&T Privacy, and the DHS Compliance Assurance Program Office to review and approve data collection and data storage procedures through processes such as Privacy Threshold Analyses and Privacy Impact Assessments, to ensure information collected and maintained is limited to what is necessary to achieve the research project's objective(s) and consistent with the applicable terms and conditions. For example, SBS extramural performers' deliverables are often limited to final summary reports, which do not contain personally identifiable information, rather than the raw data collected by the extramural performer.

SBS's extramural performers may, outside of DHS processes, submit packages that include procedures for collecting and protecting data, to IRBs for further review and approval. Extramural performers are required to adhere to any further requirements provided by IRBs in addition to those identified by S&T.

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.

There are three core values to SBS's research: quality, independence, and mission relevance. A focus on scientific rigor and quality, both within specific disciplines and interdisciplinary approaches, is a primary priority for selection and engagement in all work. To remain relevant and maintain a reputation of quality, integrity, independence, and objectivity, S&T pursues an unbiased and scientifically led research agenda, reflecting the wider needs of DHS and the public.

Online information presents unique data quality and integrity risks because S&T cannot determine in every instance whether information posted online is accurate, timely, and complete. One of SBS's goals regarding data development is the compilation of accurate and complete information to build the body of knowledge regarding terrorism and targeted violence and to better inform DHS policy. SBS data development efforts will help to ensure the body of knowledge and understanding of terrorism and targeted violence maintains pace with the ever-evolving threat landscape.

Privacy Risk: There is a risk that information used in SBS data development research efforts is not accurate, timely, and complete.

Mitigation: This risk is partially mitigated. One of the primary objectives of SBS's data development efforts is to identify accurate, comprehensive, and up-to-date information to improve the body of knowledge of terrorism and targeted violence research. Trained research teams collect information from reliable sources and follow peer review processes to corroborate information and to assess what information to include or exclude for all research efforts. Lastly, this information is not used to make operational decisions.

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.

S&T solicitations, requests for proposals, and notices of funding opportunities clearly state all applicable security requirements to which the extramural performer must adhere, and they must include data security plans and procedures in their proposals. In most circumstances, SBS does not provide any personally identifiable information or other sensitive information to its extramural

performer to execute a research activity. The only exception would be the contact information (e.g., name, business phone number) of a SME that SBS suggests should be asked to participate in an interview or focus group.

The entirety of research performed in the context of this Privacy Impact Assessment is performed by either universities or professional research institutions that have additional levels of internal security protocols specific to their institution. Some of the protocols may include standard operating procedures (SOP) that limit access to information to only active research staff, and internal data security trainings that certify research staff on best practices to limit, eliminate, mitigate, and report data security breaches in human subject related research (often called CITI Human Subjects Research training, it is typically required certification by all staff who have access to personally identifiable information). SBS's assessment of research proposals includes a review of the extramural performer's security infrastructure, and security requirements are often contractual elements of the award. An extramural performer's non-compliance with those requirements, or a breach of the extramural performer's security, can lead to termination of the contract.

If the project is no longer in compliance with the privacy-specific terms and conditions to which they are obligated due to a breach or unauthorized activity, the researcher provides notice to any non-DHS affected participant's Point of Contact within one hour of first learning of the breach or unauthorized activity. The researcher also reports the incident to their DHS Point of Contact within 24 hours of first learning of the breach or unauthorized activity and the DHS Point of Contact will then follow the DHS Privacy Incident Handling Guidance[50] for further action within DHS. Researcher breach response plans will be coordinated with the S&T Privacy Office.

In addition, all S&T-funded research must comply with Protection of Human Subjects,[51] commonly known as "The Common Rule" (6 C.F.R. Part 46), and Confidentiality of Identifiable Research and Statistical Information[52] (28 C.F.R. Part 22). The necessary associated documents and findings from a certified Institutional Review Board for Human Subjects Protections must be filed and submitted to the Contracting Officer's Representative as well as the DHS Compliance Assurance Program Office. These actions must be completed before any DHS funding can be used for the collection of data, recruitment of subjects, or any other activity that is subject to "The Common Rule."

Privacy Risk: There is a risk of loss or unauthorized disclosure of personally identifiable information due to a security incident.

Mitigation: The risk is partially mitigated. Extramural performer staff are trained and

[50] *See* DHS Instruction Guide 047-01-008, *available at* https://www.dhs.gov/publication/privacy-incident-handling-guidance-0.
[51] *See* https://www.ecfr.gov/on/2018-07-19/title-6/chapter-I/part-46.
[52] *See* https://www.govinfo.gov/app/details/CFR-2011-title28-vol1/CFR-2011-title28-vol1-part22.

certified on best practices for collecting and storing information, and data security measures are contractual requirements. SBS extramural performers have independent protocols and rules for secure storage of personally identifiable information and reporting of any unauthorized loss or disclosure of personally identifiable information to the IRB of record which will instruct the performer on how to proceed. In addition, SBS does not provide personally identifiable information or other sensitive information to extramural performers.

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.

All extramural performer personnel are required to be trained and certified on best practices for handling information, such as through CITI Human Subjects Research training. Extramural performers are required to have access controls in place to ensure only authorized members of the extramural performer staff have access to project data. Data security and protection of information, such as personally identifiable information, is typically overseen by the IRB of Record, which will periodically audit the studies they approve at their discretion. Data breaches and non-compliance are reported to the IRB of Record and S&T. An extramural performer's failure to report can lead to legal consequences, including termination of the contract, fines, or even criminal liability. In addition, the S&T Privacy Office will provide training to S&T employees on a regular and recurring basis on best practices for handling information, including regarding information that may be protected by the First Amendment.

Conclusion

SBS funds a variety of efforts with extramural performers, such as universities and non-profits, to identify objective, quantitative data that provide valuable insights consistent with DHS's mission priorities. SBS's funded research focuses on ensuring reliable data is available, evaluating the effectiveness of locally tailored terrorism prevention efforts and interventions, growing the evidence base for intervention tools, and conducting fundamental assessments of violent extremism events. SBS and its extramural performers continue to actively engage the DHS Office of the General Counsel and the S&T Privacy Office to ensure these S&T-funded research projects are completed in a manner that protects personally identifiable information, respects the constitutional rights of individuals, and implements the safeguards discussed in this Privacy Impact Assessment.

Contact Official

Maria Petrakis
Privacy Officer
Science and Technology Directorate
stprivacy@hq.dhs.gov

Responsible Official

Kathleen Deloughery
Lead, Enduring Sciences Branch
Science and Technology Directorate

Approval Signature

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

_____

Deborah Fleischaker
Chief Privacy Officer (A)
Department of Homeland Security
privacy@hq.dhs.gov

Appendix A

Privacy sensitive research funded through **Federal Acquisition Regulation-based or Other Transaction Agreement contracts** subject to the Privacy Act, applicable federal guidance, and DHS Privacy Policy

The following projects are under award or in the process of being awarded via a Federal Acquisition Regulation (FAR)-based contract or Other Transaction Agreement (OTA) for research related to or involving publicly available information. For each project, S&T consulted with S&T counsel and the S&T Privacy Office regarding specific constitutional and Privacy Act considerations to determine, respectively, (1) whether the information is protected (e.g., speech protected by the First Amendment); and (2) whether the collection of information is permissible under the Privacy Act. This consultation included the joint development and implementation of instructions, safeguards, and practices specific to the proposed project to avoid collecting or maintaining information that may be protected by the First Amendment, regardless of funding vehicle. Documents described below may also involve personally identifiable information (PII) and other activities that otherwise impact the privacy of individuals as determined by the DHS Chief Privacy Officer.

TITLE	DESCRIPTION
Center for Prevention Programs and Partnerships Public Safety Violence Prevention Program Evaluation	This project is funded via a FAR-based contract. S&T has entered into a contract with the University of Nebraska at Omaha National Counterterrorism Innovation, Technology, and Education Center (UNO NCITE) to conduct outcome and impact evaluations for the Center for Prevention Programs and Partnerships grant program for the fiscal years it has been active (FY16, FY20, FY21, FY22, FY23, and FY24) and develop infrastructure for future grantees, in addition to conducting evaluation research for selected TVTP programs that have been implemented domestically. The FY23 and FY24 grants are addressed in this Privacy Impact Assessment UNO NCITE will develop a TVTP grant program-level evaluation framework tied to a comprehensive strategy. Specifically, the purpose of this task will be to (a) develop an evaluation framework, (b) conduct an initial program-level evaluation based on available evidence, and (c) develop a maturity model for continuous program evaluation and enhanced effectiveness. UNO NCITE will work closely with DHS throughout the period of performance to systematically collect and analyze existing (i.e., previously collected) evidence to answer key questions about Center for

	Prevention Programs and Partnerships grant program effectiveness and efficiency. **Data Collection:** UNO NCITE will collect qualitative (e.g., interview) data from a list of stakeholders, who have provided their informed consent, to fill in gaps in DHS's knowledge of TVTP Grant Program implementation, program goals, program objectives, and how best to evaluate the program. None of this information will be commingled with other datasets. UNO NCITE will combine the results of the materials review, literature review, and data collection activities to generate a report including both formative and outcome evaluation information. The formative and outcome evaluation information will determine the effectiveness of TVTP grant programming objectives and implementation, and what, if any, policy changes should occur. UNO NCITE will follow both DHS and University of Nebraska at Omaha privacy and research policies, best practices, and the Privacy Act when collecting, using, or sharing personal information. All researchers involved in the proposed study will safeguard any data collected, although ultimate responsibility will fall to the NCITE Principal Investigator. The Principal Investigator and other researchers involved will clearly define and commit to data quality and safety protocols per the Institutional Review Board and data management plan. All members of the research team are required to complete Collaborative Institutional Training Initiative training in the responsible conduct of research as well as security awareness and data protection training annually. DHS S&T will receive for each of the evaluation efforts final reports detailing the findings of the evaluation, the effectiveness of the grantees, tools to conduct future evaluation activities, international awareness of terrorism prevention and recommendations, to be shared with practitioners, policy makers, and other researchers. This report will not contain any PII; rather, information will only be reported in aggregate form to protect individual privacy.
Public Safety Violence Prevention (Office of Terrorism and Targeted	This project is funded via a FAR-based contract and is a sub-contracted effort under the Center for Prevention Programs and Partnerships Public Safety Violence Prevention Program Evaluation

Violence Grant Program) Grantee Evaluation	project described above. S&T, and its contractor RTI International, seek to evaluate and assess the effectiveness of selected awardees of the FY20 – FY24 Targeted Violence and Terrorism Prevention (TVTP) Grant program. S&T will use a multidisciplinary approach where applied tools and techniques in evaluation research are utilized, while following standards identified in the U.S. Executive Office of the President, Office of Management and Budget's (OMB) Foundations for Evidence-Based Policymaking Act of 2018 (OMB M-20-12). **Data Collection:** RTI International researchers will: • Distribute web-based surveys, • Conduct phone interviews, site visits, data capacity assessments, and document/literature reviews to assess program implementation, review logic models, understand theories of change, from individuals that have provided informed consent and • Document program goals. The project will start with collecting programmatic information about the DHS grant funded programs. This involves emailing, talking, and observing individuals to learn about how they implemented their program, the types of activities they are engaged in, and any adjustments they have made to the programs. The initial phase of the study is focused on learning about the programs to document their program goals and to determine if additional data collection would facilitate assessing program outcomes. RTI will collect and use names, email address, and telephone numbers from individuals who have directly implemented grant programs only to facilitate grantee participation in the evaluation effort. None of this information will be commingled with other datasets. DHS S&T will receive a final report detailing the findings of the evaluation and suggestions and benefits about the effectiveness of the grantees, tools to conduct future evaluation activities, awareness of terrorism prevention from an international perspective, to be shared with practitioners, policy makers, and other researchers. This report will not contain any PII.

Educational Facility Threat-Hazard-Risk Analysis and Higher Education Safety & Security Needs Assessment	This project is funded via a FAR-based contract. The goal of the Online Threat-Hazard-Risk Assessment Tool will be to enable users (e.g., School Superintendents and Principals; School and District Administrators; Teachers and School Staff; School Resource Officers and School-Based Law Enforcement; Policy Makers; Emergency Managers; and other affiliated members assisting in K-12 preparedness processes) to easily look across different sources of data to understand the threats, hazards, and risks that are relevant to their school or school district. The types of data the tool may leverage would include, but is not limited to, violent threats to schools (e.g., active shooter, cyber threats), natural hazards (e.g., earthquake, flooding), and technological hazards (e.g., hazardous materials transport near school facilities). **Data Collection:** The Homeland Security Analysis Operational Center (HSOAC) will collect contact information such as name and work email address from various stakeholders for conducting semi-structured interviews and focus groups. In some cases, email addresses of the subject matter experts, organizations, and titles will be identified through referrals from government POCs. In other cases, possible interviewees or participants may be identified based on the organizations they represent, and HSOAC or government POCs will identify email addresses and names through review of publicly available information or outreach to organizations using publicly provided organizational email addresses. For the online assessment tool, the goal of the interviews and focus groups will be to solicit feedback on the tool as it is being developed, whereas in the case of the higher education report the interviews and focus groups will seek feedback from subject matter experts and staff members (e.g., administrators, law enforcement, faculty) at higher education institutions to capture current safety and security concerns. HSOAC will not associate individuals' names directly with their interview notes and will not attribute statements directly to individuals in any work products. All information will be stored in the HSOAC IT enclave and retained over the period of performance of the HSOAC FFRDC contract including follow-on contracts. None of this information will be commingled with other datasets. All public databases and academic datasets that are used in connection with the activities of this project will consist of data that is aggregated in

	nature and will not consist of any personally identifiable information. The online assessment tool will be transferred to the Cybersecurity and Infrastructure Security Agency (CISA) for its use on the CISA.gov website. The Higher Education report, which will consist of reviewing published literature as well as conducting interviews and focus groups, will be synthesized into a single report that will be made publicly available on the CISA.gov and RAND.org websites.
Evaluate Current Threat Assessments and Threat Management – Test Efficacy	This project is funded via a FAR-based contract. DHS S&T has contracted this activity to University of Nebraska at Omaha National Counterterrorism Innovation, Technology, and Education Center (NCITE/UNO), who will conduct an outcome and impact evaluation of current threat assessment tools and threat management techniques to validate whether these efforts were successful in diversion and recidivism. Findings from these outcome and impact evaluations will allow S&T to provide protocols for the development and utilization of new risk assessment techniques and recidivism reduction programming where current methods are found to be lacking. **Data Collection:** NCITE/UNO researchers will: • Review threat assessment literature that is publicly available. • Provide and leverage acumen from colleagues in the United Kingdom (UK) of previous evaluation work conducted by NCITE/UNO. • Gain a better understanding of contrasting approaches of foreign allies (UK) and domestic security agencies, such as those undertaken by USSS. • Gather lessons learned from local and state law enforcement personnel. • Review insider threats threat assessments. • Examine current threat assessment approaches for potential gaps dealing with novel threats. Through case analysis, survey-embedded experiments, and interviews (both virtual and in person), the research team will identify commonly used tools, reactions, and attitudes towards those tools, and how the tools themselves are used and applied. Sample questions will request information on participants' current threat assessment process, and how they cooperate with other agencies. All

	potential research subjects must be 19 years of age or older and utilize threat assessment tools as part of their job responsibilities. This may include members of the Secret Service, other United States government personnel, and threat assessment personnel at the local and federal level. They will be assigned an anonymous identifier to protect identifiable and private information. None of this information will be commingled with other datasets. Institutional Review Board Principal Investigator DHS S&T will receive a final report, detailing the findings of the evaluation of the threat and risk assessments which will be provided directly to participating stakeholders from the study. Due to the nature and any national/state security concerns, recommendations will not be made publicly available. These reports will not contain any PII, and information will only be reported in aggregate form to protect individual privacy.
Evaluate Violence Prevention Programming and Identify Best Practices Undertaken by Allies Abroad	This project is funded via a FAR-based contract. S&T has contracted this evaluation to University of Nebraska at Omaha National Counterterrorism Innovation, Technology, and Education Center (NCITE/UNO) through an existing S&T Basic Ordering Agreement (BOA). This activity has been sub-contracted to RTI International, who will conduct a review of existing programs operating abroad to intervene in extremism, assist with reintegration, and prevent recidivism post-incarceration. These evaluations will allow S&T to provide recommendations about prevention programming and determine best practices undertaken by countries who share the same values in combating extremism in an effort to understand the similarities and differences in the known process of radicalization and mobilization for terrorism as compared to targeted violence. S&T will work with the research team to develop and design evaluation approaches, protocols and measurement instruments that will be used to review current prevention programs, both domestic and international. **Data Collection:** The research team will complete a three-step data collection design. The first step is to conduct a literature review of publicly available sources to identify target violence and terrorism prevention (TVTP) initiatives in countries experiencing similar

	threats and, in coordination with DHS S&T and the DHS Center for Prevention Programs and Partnerships (CP3), identify experts to be included in our study. The literature review will be expanded throughout the course of the project. Next, researchers will conduct a Delphi study to identify TVTP initiatives that are considered best practices by key experts in the international TVTP community. The last step is to identify best practices determined by the experts participating in the Delphi study and examine how they are being used in practice by conducting virtual or in-person interviews with experts. None of this information will be commingled with other datasets. All researchers involved in the proposed study will safeguard any data collected, although ultimate responsibility will fall to the research team Principal Investigator. The Principal Investigator and other researchers involved will clearly define and commit to data quality and safety protocols per the research team Review Board (Institutional Review Board) and data management plan. DHS S&T will receive a final report detailing the findings of the evaluation and suggestions to improve prevention programming and measurement. The objective is to provide tools to conduct future evaluation activities, awareness of terrorism prevention from an international perspective so they can be shared with practitioners, policy makers, and other researchers. This report will not contain any PII; rather, information will only be reported in aggregate form to protect individual privacy.
Evaluation of Soft Target Security and Prevention	This project is funded via a FAR-based contract. DHS S&T has contracted the evaluation to University of Nebraska at Omaha National Counterterrorism Innovation, Technology, and Education Center (NCITE), who, through a subcontract with the Research Triangle Institute (RTI) International, will conduct a review of the state of these awareness trainings. These evaluations will allow S&T to provide recommendations on how to determine the limitations and most effective outcomes in different threat scenarios as they relate to human behavior. S&T will work with RTI to design and develop evaluation approaches, protocols, and measurement instruments that will be used to in the review of the current body of Cybersecurity and

	Infrastructure Security (CISA) threat-related training and guidance. In addition to the evaluation of the effectiveness of CISA OBP trainings, S&T will work with RTI to develop and test agent-based simulation modeling exercises utilizing data collected from literature reviews and stakeholder data collection. Agent-based models provide a flexible framework to estimate outcomes through a series of tests that adjust various parameters (e.g., researchers can change the threat scenarios or the human reaction to a threat) to understand how those changes influence the likelihood of various outcomes. The proposed simulation models combine subject matter expertise, stakeholder input, and technology to deliver actionable insights to inform CISA trainings. **Data Collection:** RTI will work with Cybersecurity and Infrastructure Security (CISA), Infrastructure Security Division (ISD), Office for Bombing Prevention (OBP) to identify samples of trained individuals to participate in the research involved in this project. Business contact PII will be collected for these activities, and to facilitate communications between RTI and the participants. Participants included in the roster of names and contact will be given a unique ID and is kept in a separate computer from the interview notes. RTI will conduct qualitative research including semi-structured interviews with Office for Bombing Prevention training staff, as well as a to-be developed survey with a sample of individuals who have participated in Office for Bombing Prevention training activities. RTI will work with Office for Bombing Prevention to determine the most effective data collection plan for these interviews and surveys, which will likely include a combination of in-person and virtual interviews, from individuals that have provided their informed consent, as well as the use of to-be developed automated surveying instruments. None of this information will be commingled with other datasets. RTI will also conduct a systematic literature review of previous evaluation projects from the general community, such as analyses of motivations and techniques, lessons learned from prior bombings, effective building evacuations models, data driven analysis of the assembled crowd at prior bombings, etc. RTI will collect data about practitioners, environments, and scenarios related

	to Improvised Explosive Device (IEDs); and build Agent-based models to simulate IED placement and use the simulation to test various intervention models under (simulated) real world conditions. All researchers involved in this effort will safeguard any data collected, although ultimate responsibility will fall on the Principal Investigator. The Principal Investigator and other researchers involved will clearly define and commit to data quality and safety protocols per the RTI Institutional Review Board. All members of the RTI research team are required to complete the Collaborative Institutional Training Initiative training in the responsible conduct of research as well as annual security awareness and data protection training. DHS S&T will receive several reports that will be provided to CISA Office for Bombing Prevention. Anticipated end users for the knowledge products resulting from this study could include counter-IED training and education providers, as well as policy- or standard-setting authorities associated with them. Major component beneficiaries would be CISA Office for Bombing Prevention and S&T. Additionally, other DHS components related to the "Soft Target and Crowded Places" and First Responder-mission spaces may benefit from this work. These reports will not contain any PII, and information will only be reported in aggregate form to protect individual privacy.
Managing the Exit of Incarcerated Violent Extremists in the Community Handbook	This project is funded via a FAR-based contract. DHS S&T contracted with the University of Nebraska at Omaha (UNO) to develop a handbook for domestic prevention programs that will assist with managing the exit of federally incarcerated violent extremists back into the community. **Data Collection:** To develop the handbook for managing the exit of federally incarcerated extremists to the community, UNO National Counterterrorism Innovation, Technology, and Education Center (NCITE) will conduct an open-source environment scan, interviews, focus groups and expert working groups with U.S. and non-U.S. persons. None of this information will be commingled with other datasets. All work will be performed on the UNO NCITE system. The UNO

	NCITE system does not connect to DHS IT infrastructure for this effort. This is their internal IT system in which the research team operates within. NCITE will analyze quantitative information derived from open-source materials (e.g., court records, news media, correctional records; however, no social media sources will be used) on extremist arrest, court processing, sentencing, time in correctional facilities, and post release. Court documents will be collected through court record repositories such as JudyRecords (Free Public Records Search – Judy Records) or RECAP (Advanced RECAP Archive Search for PACER – CourtListener.com). Correctional records will be the offender profiles on the website of the correctional institutions that they are incarcerated. Any PII collected will only be done for the sole purpose of identifying stakeholders, conducting interviews, creating focus groups, and creating expert working groups. UNO NCITE will follow both DHS and University of Nebraska Omaha privacy and research policies, best practices, and the Privacy Act when collecting, using, or sharing personal information. All researchers involved in the proposed study will safeguard any data collected, although ultimate responsibility will fall to the NCITE Principal Investigator. The Principal Investigator and other researchers involved will clearly define and commit to data quality and safety protocols per the Institutional Review Board and data management plan. All members of the research team are required to complete Collaborative Institutional Training Initiative training in the responsible conduct of research as well as security awareness and data protection training annually. The primary deliverable will be a handbook that is provided to DHS upon completion of the projects. The handbook will be disseminated and presented to relevant stakeholders. NCITE will develop at least one peer-reviewed academic article and presentation at academic conferences aimed at relevant audiences in terrorism and security studies and criminology and criminal justice.
NTER Research Initiatives	This project is funded via a FAR-based contract. The DHS Intelligence and Analysis (I&A), National Threat Evaluation and Reporting (NTER) Office's mission is to strengthen information sharing and enhance our Homeland Security partners' ability to

	identify and prevent targeted violence and mass attacks, regardless of ideology. The NTER Office does this by equipping Federal, State, Local, Tribal, Territorial (FSLTT), and Private Sector partners with tools and resources to identify, report, and mitigate threats of terrorism and targeted violence, to keep the Homeland safe. NTER provides a Master Trainer Program (MTP) that certifies FSLTT partners in the instruction of Behavioral Threat Assessment and Management (BTAM) techniques and best practices. This train-the-trainer program prepares Certified Master Trainers (CMTs) from a broad range of sectors, including law enforcement, intelligence, school safety, insider threat and workplace violence prevention, to empower their local communities and organizations to mitigate threats and prevent acts of targeted violence. Because this training is new, there is a need to (a) evaluate the effectiveness of MTP in meeting its objectives, and (b) provide research and recommendations to enhance program outcomes. In addition to this requirement, there is a need to identify best practices in BTAM techniques and best practices across sectors, such as educational institutions, social services, the community, and various components of the criminal justice system. DHS S&T contracted with the University of Nebraska at Omaha National Counterterrorism Innovation, Technology, and Education Center (UNO NCITE) to evaluate the effectiveness of the NTER MTP in meeting its objectives. **Data Collection:** To evaluate the effectiveness of the NTER MTP in meeting its objectives, the University of Nebraska at Omaha National Counterterrorism Innovation, Technology, and Education Center (UNO NCITE) researchers will conduct material reviews, stakeholder interviews, focus groups and workshops where participants have provided their informed consent. To identify best practices in behavioral threat assessment management, the research team will conduct material reviews, which include searching for and analyzing publicly available best practice guides. The NCITE researchers will confirm with the NTER office that only de-identified data will be sent to NCITE. The S&T program office will also communicate de-identification requirements to NTER prior

	to data sharing and will review sample data export examples to serve as an additional check to ensure fields involving PII are not included. NCITE also has procedures in place to de-identify data if received with incidental PII. None of this information will be commingled with other datasets. UNO NCITE will also review internal documents related to goals and objectives of the MTP, which may include strategic planning documents and/or materials (e.g., meeting notes/minutes, slides, handouts) from key internal deliberations. Any other documents identified by DHS/NTER that might inform the evaluation or strategic direction of the Master Trainer Program will also be reviewed. UNO NCITE will follow both DHS and its university's privacy and research policies, best practices, and the Privacy Act when collecting, using, or sharing personal information. All researchers involved in the proposed study will monitor and supervise the safety of any data collected, although ultimate responsibility will fall to the NCITE Principal Investigator. The Principal Investigator and other researchers involved will clearly define and commit to data quality and safety protocols per the Institutional Review Board (Institutional Review Board). All members of the research team are required to complete CITI training in the responsible conduct of research as well as security awareness and data protection training annually. Documents will be obtained from DHS through a secured exchange portal, owned, operated, and maintained by the University of Nebraska System Information Technology Security Office. Because documents may include PII, such as participant name and email address, the research team will redact and deidentify all documents prior to transferring them onto a password protected hard drive belonging to the PI. The research team will then analyze data on encrypted, password protected UNO managed computers.
Soft Target Alert Notification Feasibility Study	This project is funded via a FAR-based contract. S&T, in collaboration with the Performer (Team A4SAFE), will conduct a feasibility study on creating a Soft Target Alert Notification System, which can enable the dissemination of coordinated mobile device warnings to large audiences regarding real-time events that may

	necessitate protective and/or mitigation measures, individual and/or organizational evacuations, and other preventative actions. The feasibility study will identify existing alert notification systems that may be available for Federal use and determine how these existing alert notification systems may be harmonized to address the needs of Federal, State, Local and/or Tribal stakeholders. S&T and the Performer will research and evaluate the current state of soft target alert notification systems implemented by both governmental and non-governmental entities, along with other systems that might not be part of an official or formal emergency management chain. The feasibility study will involve evaluating the current state of soft target alert notification systems along with conducting a risk-based assessment to identify gaps in existing alert notification technology that is available in the marketplace. Through the Performer, S&T will examine publicly accessible policies, regulations, and technologies that may be leveraged to improve current alert communications and create a prototype to demonstrate the feasibility of those improvements, thus providing recommendations based on optimization through Emergency Responders alert communication process improvement, enhanced regulations, and emerging technologies which will provide a proactive capability that currently minimally exists. **Data Collection:** As part of this research, S&T will gather publicly available information, to include the following: • Preparedness guides • Security protocol • Best practices and implementation guides • Data exchange specifications • Software websites, software documentation, and executable software demos for trial purposes • Academic literature reviews Personally identifiable information (PII) may be incidentally collected in connection with this feasibility study, such as author names from the various literature journals or documents that are gathered from publicly available information. None of this information will be commingled with other datasets. All information

	collected will be stored securely on a Microsoft SharePoint site, with access limited to those with a need to know. While the objective of the study is to evaluate the current state of Soft Target Alert notification technology in the market, neither S&T nor the Performer will be accessing or collecting any data that is stored in pre-existing alert warning systems. The Performer will provide DHS with a series of reports that summarize the Performer's findings and outline substantive actionable recommendations and next steps for improving soft target alert notification systems.
Soft Target and Crowded Places Landscape Assessment and Research Roadmap	This project is funded via a FAR-based contract. S&T and its contractor, the Homeland Security Operational Analysis Center (HSOAC), seek to assess a planned project that will deliver guidance on the types of "soft targets or crowded places" measures and spending that are best aligned with reducing the number of and casualties from soft targets or crowded places incidents and will provide recommendations to help optimize funding for DHS soft target or crowded place incident prevention, response, and recovery, in part to inform security for upcoming major sporting events (e.g., World Cup, Olympics). S&T is undertaking this activity to reduce the risk to soft targets or crowded places and better understand the threats, vulnerabilities, statuses of existing programs, and the optimal allocation of soft targets or crowded places security resources. This study is designed to answer the primary research question: How can prevention, protection, and response/recovery investments reduce the risk of casualties from attacks on soft targets and crowded places? **Data Collection:** To address the primary research question, the performer will review the state of the literature, the nature of threat, the current DHS policy and programmatic landscape and existing data (e.g., Homeland Infrastructure Foundation-Level Data 3 (HIFLD3), FBI Active Shooter Case Data, Mass Attack Defense Toolkit Case Data, National Threat Assessment Center Summary Data). The information collected are past datasets, SME interviews, academic and gray literature (information produced outside of

	traditional publishing and distribution channels) review, and recent awards and grants. For the past datasets, the summary descriptions of past mass attacks sometimes contain the names of mass attack perpetrators; one can also use the summary information provided to quickly perform searches of open media articles that reveal the perpetrators of specific attacks. No other PII is captured in the referenced datasets; neither HSOAC nor S&T intend to use or analyze the PII of attackers or other persons involved in past attacks in any way. No information describing how any individual exercises rights guaranteed by the First Amendment will be collected, maintained, used, or disseminated by HSOAC or S&T at any point in this research. To facilitate conducting soft targets and crowded places security SME interviews, HSOAC will collect point-of-contact information. This information will include name, organizational affiliation, phone number, and email. All information will be stored in the HSOAC IT enclave. None of this information will be commingled with other datasets. This information will not be shared outside the research team, DHS S&T, and CISA. Academic and gray literature review information will include article name, authors name, publishing or circulation date, and organizational name. Recent awards and grants information will include grant name, grantee name, grant date, grant organization, and grant award. The final report will be a RAND report and will contain all the data sources, methods, analyses, findings, and recommendations for the tasks above, where appropriate. HSOAC will also prepare a graphics-based presentation designed for a general non-technical audience that summarizes results of the study. A version of the report that excludes any DHS sensitive data (and sensitive PII) will be published on the HSOAC website to facilitate DHS S&T's ability to communicate about the findings of this work across DHS and the homeland security enterprise (HSE). If the reports contain classified, DHS sensitive data, HSOAC will create a second report without such data. The second report will focus mostly on methods and non-sensitive findings. There will be only one report if there are no sensitive findings. The only PII in these report(s) will be authors' names in citations.

Systematic Reviews (Campbell Collaboration)	This project is funded via a FAR-based contract. S&T, and its contractor partner research team at Campbell Collaboration Crime and Justice Group (CCCJ), an independent, non-profit organization, seek to conduct systematic reviews of high-quality research on effective methods in preventing terrorism and radicalization. The objective of this research is based on DHS's efforts to prevent terrorism and help address the gaps in knowledge by providing a global evidence-base for practice and policy by producing rigorous and up-to-date reviews of evidence on terrorism and radicalization prevention interventions, and to make them easily accessible (publicly available) to decision-makers, and other researchers. **Data Collection:** All the data collected, coded, and used for analysis in these studies comes from previously published materials, such as journal articles, books, and technical reports. This project does not collect, maintain, use, or disseminate any personally identifiable information. Upon the conclusion of the effort all systematic reviews will be published electronically in a freely accessible web-based archive, Campbell Systematic Reviews, to provide rapid, up-to-date, and rigorous information to those who need to know which crime prevention strategies do and do not work.
Text-Enabled Gatekeeper Intervention Help Line Referral System	This project is funded via a FAR-based contract. S&T, and its contracted university researchers at Georgia State University (GSU), will seek to design and conduct a process evaluation of the crisis assessment and referral protocols for call centers that deal with reported hate crimes. S&T will test the effectiveness and pertinence of current crisis-center referral protocols and assess their suitability for text-enabled handling of potential cases of violent extremism. The effort supports goals for both the DHS Strategic Plan for Fiscal Years 2020-2024, as well as the Department's 2019 Strategic Framework for Countering Terrorism and Targeted Violence by evaluating current crisis-center referral protocols and develop standard protocols and toolkits for threat assessment referrals and management of persons at risk of mobilizing to violence. Findings from the process evaluation will be used to conduct a

	single-site evaluation to develop, field test and evaluate a text-enabled intervention helpline and referral system. (Interventions, in this case may refer to intimate bystanders' concerns about persons becoming involved in violent extremism, or concerns about how to help someone exit violent extremism.) Such a text-enabled service can empower intimate bystanders with a convenient, readily accessible, confidential first step of reaching out for help about concerns that peers or loved ones might be on a path toward engaging in, or otherwise supporting, targeted violence. **Data Collection:** GSU researchers will conduct a scoping review of relevant literature on off-the-shelf case management solutions with particular focus on solutions that are fit for purpose and scalable. This will be informed by the research team's previously developed, evidence-based helpline referral protocols and procedures with 211LA (a helpline program based in Los Angeles). GSU researchers will also conduct focus groups, in collaboration with the evaluation site, to capture policies and procedures that are in line with the sites' operational capacity and procedures. The focus groups will be moderated by the researchers and will take place on Zoom without retaining any of the PII from members of the focus groups. GSU will also develop evaluation site helpline terms of service for operational use with their users. This will be done in accordance with existing intervention helpline policies in the US and based on a review of the relevant literature. GSU will also conduct a survey such as a Likert scale survey, taking less than 60 seconds to complete, measuring satisfaction with the capability, staff responses, and whether the inquirer was helped. GSU will also support the local evaluation site to market the helpline to intended users. This will be performed through both print and online media (including mainstream social media, e.g., Facebook), and a) developed in accord with contemporary theories of social psychology, and b) implemented in a way that affords statistical comparisons of the relative effectiveness of the marketing modalities. GSU will assess the effectiveness of the marketing, protocols, and implementation of the Intervention Helpline & Referral System. This will be performed through mixed (quantitative and qualitative) methods. Specifically, the marketing materials will be compared for statistically significant differences, with respect to the volume of incoming referrals, per marketing

	modality (print vs. online/social media outlets). Only the GSU research team will have access to focus group audio recordings transcripts and the de-identified case reports that the evaluation site will share. The GSU research team will destroy the audio recordings within a week of the focus group session, after the researchers have transcribed the text. If a participant mentions any names or other personally identifiable information, GSU researchers will pseudonymize the transcript to ensure that no information can be tied to an individual. None of this information will be commingled with other datasets. DHS S&T will receive a report on the implementation of the Intervention Helpline & Referral System, to include marketing materials and protocols. This report will not contain any PII.
OTA Canada	This Other Transaction Agreement (OTA) funds the U.S. portion of a coordinated joint research and development (R&D) program as set forth in the Project Arrangement entered into by the U.S. Department of Homeland Security, Science and Technology Directorate (DHS S&T), and the Government of Canada (GC). **Data Collection:** Under the Project Arrangement S&T. will provide funding to the GC to exchange best practices and lessons learned in public safety and violence prevention programming, with a primary purpose to synthesize and mobilize research already completed and grow the existing body of global evidence for public safety and violence prevention policy, strategy, and activity and promote and build stronger shared knowledge. In consultation with the GC, this effort will exchange data and findings through knowledge synthesis, focus groups, symposiums, workshops, and conferences, between researchers, subject matter experts and frontline prevention organizations and practitioners engaged in public safety and violence prevention. These technical exchanges will bring together research and evidence towards developing national standards or evidence-based guidelines, such as to validate tools, methods, and approaches. Personnel exchanges of subject matter experts and practitioners will be included as a means to transfer data and findings in the fields of public safety and violence

	prevention. Findings from these technical data, information, and personnel exchanges that provide best practices and lessons learned in public safety and violence prevention programming will be made publicly available. The U.S. and the GC will jointly codevelop at least two groups of experts collated from those identified by each Party, aimed at bringing together policy, operations, and research partners to advance U.S. and GC knowledge of how existing assessment tools can effectively measure risks, needs and vulnerabilities. An objective will be to publish reports that aim to document methods, tools, and techniques used by academia, practitioners, and frontline public safety and violence prevention programs and provide best practices and lessons learned in meaningfully measuring and evaluating public safety and violence prevention program design, implementation, and outcomes. The Parties will make these reports publicly available as agreed upon by the Parties. The Parties do not intend to share personally identifiable information (PII) for the purposes of this Project Arrangement.
OTA New Zealand / OpenMined	This Other Transaction Agreement (OTA) funds the U.S. portion of a joint and coordinated research and development (R&D) program as set forth in the Project Arrangement entered into by the U.S. Department of Homeland Security, Science and Technology Directorate (DHS S&T), and the Government of New Zealand (NZ). **Data Collection:** Under the Project Arrangement the U.S. will provide funding to exchange data and findings between researchers, subject matter experts and practitioners to grow the existing body of global evidence for public safety and violence prevention policy, strategy, and activity. These exchanges will enhance the existing body of global evidence and support independent study of how algorithms impact users and society more broadly, along with the role they play in spreading radical content online. In consultation with NZ, this effort will support research to develop an encryption software system that allows researchers to access data from tech companies without accessing PII or any protected content. This research is in support of The Christchurch Call Initiative on Algorithmic Outcomes (CCIAO). A joint initiative between the New

	Zealand and US Governments as well as major US tech companies, including Twitter/X, and Microsoft. The project's main goal is to support the creation of new technology to understand the impacts of algorithms on people's online experiences. The CCIAO also involves an open-source non-profit organization called OpenMined, a U.S. based entity, which is developing and testing new privacy-enhancing software infrastructure to help to better understand the impacts that algorithms and other processes may have on terrorist and violent extremist content online. The U.S. and NZ/OpenMined will jointly codevelop at least two academic papers and/or focus groups aimed at bringing together policy, operations, and research partners to advance our knowledge of the impact of algorithms in spreading radical content online.

Appendix B

This appendix summarizes the work funded through financial assistance agreements (grants or cooperative agreements). At DHS S&T, financial assistance is the transfer of funds to a non-federal recipient to conduct research and development for a public purpose. Under financial assistance agreements, DHS releases a Notice of Funding Opportunity (NOFO) that highlights key objectives and research priorities for the Department. Applicants can then submit proposals that they believe best meet those priorities. The specific research questions and methodology are developed by the applicant, not dictated by the Department. Financial assistance agreements are subject to the Homeland Security Act of 2002, as amended, federal guidance, and DHS privacy policy.

Terrorism and Targeted Violence Research and Evaluation Notice of Funding Opportunity

Through the 2023 Terrorism and Targeted Violence Research and Evaluation Notice of Funding Opportunity, S&T sought to support foundational research that contributes to advancing the state of the science through novel, nuanced, innovative, and rigorous scientific inquiry using diverse and non-traditional strategies. With a focus on advancing the understanding of behaviors and motivations to engage in terrorist or targeted violence activities, to inform greater understanding and provide situational awareness regarding violent terrorist movements, and to inform the creation of prevention, diversion, and rehabilitation strategies for those involved, the NOFO aimed to:

1. Conduct basic and applied research to improve our understanding of how and why individuals radicalize to violence, mobilize to violence, and disengage from violence using diverse and non-traditional research strategies from a multi-disciplinary perspective.
2. Understand the efficacy of non-government, online interventions to prevent, deter, or otherwise mitigate negative outcomes and harms related to violent online behaviors as they are related to Homeland Security missions.
3. Ensure key stakeholders such as federal, state, local, tribal, and territorial partners, community-based organizations, violence prevention practitioners, and members of the public have the knowledge and tools required to support the implementation of effective violence prevention and intervention programming.

Specific research priorities included:

(i) Research to Understand Trends, Nature, Causes, and Correlates in Terrorism and Targeted Violence in the United States.
(ii) Research on the Implementation of Evidence-Based and Best Practices in Terrorism Prevention and Intervention Research
(iii) Research Applying Computational Social Science to Homeland Security Needs

(iv) Analysis of Online Intervention Programs

Research funded under this Notice of Funding Opportunity has the potential to contribute to the development of evidence-based policy, programs and technologies in support of the DHS Countering Terrorism and Targeted Violence Strategic Framework (CTTV), specifically Goal 3, and the White House National Strategy for Countering Domestic Terrorism, specifically Goals 1 and 2.

To ensure that awards made under this financial assistance agreement comport with the Homeland Security Act of 2002 and DHS privacy policy, DHS S&T worked closely in conjunction with the S&T Privacy Office and the DHS Privacy Office while crafting the Notice of Funding Opportunity. This combined effort resulted in additional language being included in the Notice of Funding Opportunity to establish guardrails so that funding applicants know what research S&T does and does not wish to fund. S&T, the S&T Privacy Office and the DHS Privacy Office jointly developed a list of 16 items we believed were important to state in the Notice of Funding Opportunity. The Notice of Funding Opportunity Program Overview included statements on overarching S&T desires for department funded work. In the Notice of Funding Opportunity Other Submission Requirements S&T added a set of criteria detailing conduct for the research.

The Program Overview description in the Notice of Funding Opportunity on page 6 clearly lays out DHS S&T's commitment to the protection of privacy, civil rights, and civil liberties—delineating that research funded under this NOFO will not be used to support the collection, maintenance, use, or dissemination of individuals' personally identifiable information based on the content of their speech and how they express themselves non-violently, their associations, how and whether they choose to worship, and how they choose to non-violently express their concerns or positions to government. Non-violent forms of political activism and the political views held by individuals or groups may not provide the basis for collecting personally identifiable information. The Notice of Funding Opportunity also asserts that before any data collected as part of this research is archived or publicly released the recipient should conduct a review to ensure that there is no personally identifiable information, and that no secondary personally identifiable information may be used to unmask research any participant's identity.

Additional submission requirements were also added on pages 21-22 of the Notice of Funding Opportunity. While a full list can be found in the Notice of Funding Opportunity, a few highlights of criteria include that recipients may not employ deceptive or covert practices to collect data. No unapproved false identities can be used to collect data. Recipients may not provide identifiable research data to law enforcement, intelligence, or investigative agencies. Recipients will respect the privacy settings set by individuals on websites, only collecting publicly available social media information (e.g., open-source information). Recipients must ensure that, when sourced from social media, data collection must abide by the established Terms of Service of the internet service provider(s) or other publicly available information platforms—including social media

companies—from which the information is collected. Keywords used by recipients to query publicly available information must be designed in such a way as to not profile, target, or discriminate, against any individual based on the content of their speech and how they express themselves non-violently, their associations, how and whether they choose to worship, and how they choose to non-violently express their concerns or positions to government.

Applicants were requested to submit a privacy certificate with their proposals to this Notice of Funding Opportunity. A template was provided. The privacy certificate was intended to provide assurances that the applicant understood and agreed to accept the responsibility to safeguard any personally identifiable information collected through the research and to abide by specific procedures to ensure that the information would be adequately protected. The specific methods, techniques, and procedures to safeguard this information were proposed by the applicant, not dictated by the Department.

As part of the process for reviewing proposals, the S&T Privacy Office and the DHS Privacy Office reviewed the privacy risks and mitigation measures relevant to the applications selected by S&T for funding, and to ensure that recipients understood and could demonstrate their ability to abide by the privacy requirements established in the Notice of Funding Opportunity.

Mitigation measures vary for each individual recipient, based upon the research activity they have proposed. The following are a sample of mitigation measures applied to recipients, when applicable, to ensure that personally identifiable information is adequately protected.

- S&T Program Officials reviewed the criteria with the performer at the kick-off meeting. The recipients will be reminded that these criteria must be met continually throughout the life of the award.
- S&T Program Officials confirmed none of the proposals included the use of any government data or government information systems.
- Based upon the research proposed, some recipients stated that they would: (1) publicly announce their project, its goals, and methods on a webpage; (2) maintain a dedicated web presence that would include detailed data collection methodology information; (3) provide contact information for individuals to raise any concerns that their personally identifiable information might be inaccurate, incomplete, or a risk to their privacy or civil liberties.
- S&T Program, S&T Privacy, and DHS Privacy Officials confirmed that the proposals include methods to avoid over-collecting PII. Depending on the project methodology, performers indicated they would: (1) deidentify, pseudonymize or anonymize data; (2) remove data that could reidentify an individual and once anonymized not combine with other datasets to reidentify a person; (3) collect very limited "business card" personally identifiable information, and exclude social media handles and IP addresses; and/or (4) not

use personally identifiable information in spreadsheets, notes, transcriptions, reports, interview and focus group documentation, or audio recordings.

- S&T will ensure that collection, maintenance, and disposition of PII aligns with the stated criteria in the Notice of Funding Opportunity, the policy of the proposing organizations, and any requirements set forth by Institutional Review Boards (IRB). IRB documentation and decisions are reviewed by DHS Compliance Offices for concurrence.
- The recipients will follow all applicable local, state, and national laws regarding PII. Examples include the California Consumer Privacy ACT (CCPA) and the General Data Protection Regulation (GDPR).
- Based on the research activity proposed, the recipients have provided information to DHS regarding how they will implement access controls to ensure only those with a determined need access PII. Some examples of steps that would be taken, to control access include: (1) reviewing password-protected accounts at least three times per year; (2) purging inactive accounts; and (3) requiring students, staff, and project affiliates to sign comprehensive data use agreements.
- Based on the research proposed, the recipients have provided information to DHS regarding how they will secure physical data and the hardware on which it resides. Some examples of security measures that would be taken, include: (1) logging all evidence in secure folders; (2) encrypting data and using encrypted partitions for sensitive data; (3) using industry standard open-source Linux hosting and web servers; (4) storing data in the cloud and routinely creating back-ups, and not storing data longer than is necessary.
- Based on the research proposed, recipients also indicated several steps they would take to ensure data quality and integrity, such as: (1) appointing a data protection officer—if appropriate; (2) conducting periodic assessments through Data Protection Impact Assessments; (3) conducting regular reviews of data gathered and deleting data irrelevant to the project; and (4) repeatedly reviewing collected data to ensure it is relevant and complete.
- Based on the research proposed, the recipients will provide knowledge products and other publications to the S&T Program Officials for review to confirm the privacy criteria have been satisfied prior to public dissemination. In addition, several performers indicated they would: (1) generate anonymized manuscripts; 2) refrain from disseminating personally identifiable information to third parties. and anonymizing, masking, aggregating, or generalizing data prior to dissemination.
- Each recipient was provided the opportunity to attend a privacy training course with DHS S&T Privacy Officials on compliance with the Terms and Conditions.

The following recipients were selected for funding in 2023:

Australia National University: Grievance-fueled targeted violence in the United States

This project's goal is to improve understanding of the prevalence and nature of threats by offenders who commit an act of grievance-fueled targeted violence outside of organized terrorism.

Institute for Strategic Dialogue: Pioneering New Computational Social Science Approaches to Informing Evidence-based Policy, Practitioner and Public Responses to Domestic Violent Extremism Online

This project's goal is to provide understanding of rapidly shifting domestic violent extremist threat landscapes in the United States, to develop an aggregate view of a new threats using large language models to compare online behaviors of violent extremists.

Moonshot USA, Inc.: Developing empirical evidence on the common motivations and characteristics behind acts of targeted violence and terrorism.

This project's goal is to examine and understand variables that explain trends of targeted violence and terrorism in the United States, vulnerabilities of individuals that have committed acts of targeted violence or terrorism in the United States, and to describe events to match these trends or vulnerabilities with interventions.

President and Fellows of Harvard College: Implementation Science for Targeted Violence Prevention

This project's goal is to enhance the translation of knowledge in the field of risk assessment to improve practice in ways risk is assessed in the prevention of targeted violence and terrorism.

Regents of the University of California, Los Angeles: Addressing the Know-Do Gap in Community Reporting for Terrorism and Targeted Violence Prevention

This project's goal is to investigate and compare intimate bystander reporting of concern in seven countries to understand the effectiveness of citizen engagement in prevention.

RTI International: Evaluation of Moonshot's Redirect Method

This project's goal is to independently evaluate the intended and unintended impacts of commonly used "online redirect" methods as part of a suite of private sector responses to online extremism and radicalization.

SUNY, University at Albany: Violent Extremist Organizations in the United States— Data Collection and Analysis (VEO-US)

This project's goal is to collect and analyze quantitative, longitudinal data on organizational variables to explain non-state organizations engagement in violence.

University of Maryland: Terrorism and Targeted Violence in the United States (T2V):

Database, Analysis, and Dissemination

This project's goal is to provide objective, independent, quantitative data on targeted violence and terrorist events in the United States.

University of South Carolina: Trajectories of Targeted Violence: Mobilization Trends and Interdiction Opportunities

This project's goal is to collect and analyze data on 42 violence mobilization indicators and explain trajectories to violence based on known violent attacks.

National Counterterrorism Innovation, Technology and Education (NCITE) Center: Development and Validation of Assessment Tools for TVTP Outcome and Impact Assessment

This project's goal is to introduce novel assessments for outcome evaluation of targeted violence and terrorism prevention (TVTP) programming.