Privacy Impact Assessment
for the

Next Generation First Responder Apex Program

DHS/S&T/PIA-038

August 19, 2019

Contact Point

John Merrill
First Responders and Detection Division
DHS Science and Technology Directorate
(202) 254-5604

Reviewing Official

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

Abstract

The Department of Homeland Security (DHS) Science and Technology (S&T) Directorate established the Next Generation First Responder (NGFR) Apex Program (Program), a research, development, testing, evaluation, (RDT&E) and standards program, adapting existing technologies, developing new capabilities, and working with the private sector to enhance capabilities for first responders across the nation. More than 60 individual RDT&E projects "align" to the NGFR Apex Program. Program activities include technology integration demonstrations and/or operational experimentations (OpEx) and the development of knowledge products, such as facts sheets and case studies. DHS S&T is conducting the NGFR Apex Program Privacy Impact Assessment (PIA) because the Program involves the use of personally identifiable information (PII) as well as technologies that raise potential privacy concerns.

Introduction

The Homeland Security Act of 2002 authorizes DHS S&T to conduct "basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs."[1] In exercising its responsibility under the Homeland Security Act, DHS S&T is authorized to collect information, as appropriate, to support research, development, and other test and evaluation activities related to improving the security of the homeland.

The Intelligence Reform and Terrorism Prevention Act of 2004 established the Office for Interoperability and Compatibility (OIC) within DHS S&T to enhance public safety interoperable communications at all levels of government.[2] The Homeland Security Appropriations Act, 2007 (Appropriations Act) further refined OIC's responsibilities to focus on research, development, testing, evaluation, and acceleration of the development of standards to improve interoperable communications.[3]

In particular, the Appropriations Act states that OIC shall "encourage the development and implementation of flexible and open architectures incorporating, where possible, technologies that currently are commercially available, with appropriate levels of security, for short-term and long-term solutions to public safety communications interoperability."[4]

DHS S&T fulfills these responsibilities, in part, through NGFR Apex Program. This PIA provides a high-level overview of the NGFR Apex Program, covering NGFR program-level

[1] *See* 6 U.S.C. § 302(4).
[2] *See* 6 U.S.C. § 194.
[3] *See* 6 U.S.C. § 195.
[4] *Ibid*.

activities and identifying the types of technologies aligned under the NGFR Apex Program. This PIA does not provide the specific details for each RDT&E project. Individual RDT&E projects must submit the details of those projects, separately, for individual privacy analysis, documentation, review, and approval.

When the NGFR Apex Program incorporates NGFR project technologies in a program-level activity, such as an NGFR Integration Demonstration, the Program will submit an NGFR program-level Privacy Threshold Analysis (PTA) for the activity. The purpose of the PTA is to provide awareness to the S&T Privacy Office and the DHS HQ Privacy Office, as well as to address any privacy risks and provide mitigation efforts. The DHS Privacy Office will also determine whether the activity will be associated with this PIA or the DHS/S&T/PIA-027 S&T Test Data PIA or if a new PIA is required, depending on the nature and scope of the project technology and if new or significant privacy risks are anticipated. Given the extensive outreach the Program conducts, involving first responders and other participants, some activities may be addressed in other PIAs, for example, PIAs related to taking surveys and conducting interviews and focus groups.[5]

DHS S&T initially launched the NGFR Apex Program in 2014. In 2015, DHS S&T made the Program a five-year strategic initiative to develop and integrate next generation technologies with the goal of expanding first responder mission effectiveness and safety. The NGFR Apex Program runs through January 2020 with a final program report to Congress and the public on the developments, results, and impact of the Program.

The NGFR Apex Program has the following goals:

(1) Develop and transition technologies to meet requirements of the emergency response community, as identified through DHS S&T's periodic capability assessments of responder needs and based on changes in the response environment and technological advances;

(2) Develop and transition a standards-based approach to integrating first responder technologies in partnership with industry and encourage technology developers to design capabilities using these standards;

[5] Depending on the nature and scope of a program activity, one or more other DHS/ALL and/or S&T PIAs may be applicable, including DHS/ALL/PIA-069 DHS Surveys, Interviews, and Focus Groups; DHS/ALL/PIA-006 DHS General Contacts List; DHS/ALL/PIA-031 Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue; and DHS/S&T/PIA-020 Research Projects Involving Volunteers. All DHS and S&T PIAs are available at https://www.dhs.gov/privacy.

(3) Integrate NGFR-developed technologies, commercially available technologies, and existing first responder infrastructure using the NGFR standards-based integration approach to enhance first responder capabilities; and

(4) Develop and transition to the response community key knowledge products to guide public safety agencies on how to integrate and deploy NGFR capabilities in their communities.

Program Focus

The NGFR Apex Program develops, adapts, and integrates cutting edge technologies using open standards to increase competition in the first responder technology marketplace, and give first responders more options to build the systems they need for their missions and budgets. By leveraging advanced communications systems, wearable "Internet of Things" (IoT) devices, and situational awareness platforms, the Program seeks to equip first responders with the next generation of tools and technologies. The Program envisions an environment that uses data and hardware standards to integrate technologies enabling faster, more efficient, and safer responses to threats and disasters. To achieve this vision, DHS S&T tests and evaluates technologies and their integration in operational settings, i.e., NGFR Integration Demonstrations/Operational Experimentations, with first responders across the country.

The NGFR Apex Program focuses the technologies' primary operational objectives on:

(1) Providing real-time situational awareness that enables first responders to recognize and avoid hazards before, during, and after incidents;
(2) Enabling first responders to withstand threats they cannot avoid through advanced material science, resulting in fewer fatalities and injuries;
(3) Assuring the right information is received by decision makers in time to make a difference;
(4) Reducing the time it takes first responders to arrive on-scene and complete their mission response; and
(5) Integrating existing and emerging technologies into a modular, standards-based open architecture that meets first responder needs and operates within on-scene environmental constraints.

The NGFR Apex Program roots its objectives in the first responder community's most pressing needs and priorities. Capability gaps are identified by direct engagement with other DHS Components and direct first responder community stakeholder engagement with communities such as the First Responder Resource Group, SAFECOM,[6] and the National Public Safety

[6] More information on SAFECOM is available at: https://www.dhs.gov/safecom.

Telecommunications Council (NPSTC).[7] NGFR projects address several of these capability gaps through coordinated RDT&E efforts.

DHS S&T performs formal periodic requirements assessments for NGFR, including the 14 highest priority capability needs that first responders identified they needed to improve their ability to respond to catastrophic incidents.[8] Capability priorities addressed by NGFR include:

- Communications systems that are hands-free, ergonomically optimized, and can be integrated into personal protective equipment;
- The ability to communicate with first responders in any environmental conditions (including through barriers, inside buildings, and underground);
- The ability to detect, monitor, and analyze passive and active threats and hazards at incident scenes in real time;
- The ability to incorporate information from multiple and nontraditional sources (e.g., crowdsourcing and social media) into incident command and operations; and
- The ability to remotely monitor the tactical actions and progress of all first responders involved in the incident in real time.

The NGFR organizes affiliated research, development, testing, and evaluation projects into three portfolios, as described below.

Technology Portfolios

- **Protected Portfolio – Defending Against Life-Threatening Hazards**

DHS S&T leverages new technologies that can help keep responders safer in the line of duty. NGFR's Protected Portfolio includes: physiological monitoring to understand when responders are in distress; IoT sensors to detect chemical or radiological threats, hydration levels, or dangerous changes in the incident environment; and advanced protective materials that can protect them against frequent hazards. These tools will assist not only the first responders, but also help incident commanders make better decisions to protect their public safety partners.

- **Connected Portfolio – Having A Lifeline When It's Needed Most**

DHS S&T leverages new technologies to ensure reliable and resilient voice, video, and data communications. NGFR's Connected Portfolio targets: interoperable communications

[7] More information on NPSTC is available at: http://www.npstc.org/.
[8] DHS S&T "Project Responder 4: 2014 National Technology Plan for Emergency Response to Catastrophic Incidents," July 2014, is *available at*: https://www.dhs.gov/sites/default/files/publications/Project%20Responder%204_1.pdf.

systems that can reliably exchange messages; deployable networks to give connectivity anywhere, anytime, and in any condition; and universal data and interface standards for public safety to make information sharing easy and secure. The NGFR Apex Program goal is an open plug-and-play system, which means that sensors, situational awareness platforms, network support, and other first responder technologies are designed using open-source standards that allow each piece to plug into another piece, whether it is a physical connection or a data connection. The NGFR Integration Handbook[9] recommends specific data standards that can help industry design technologies to be plug-and-play from the beginning; the handbook has evolved based on industry feedback and the lessons learned from NGFR Integration Demonstrations/OpEx events. Eventually, if industry widely adopts the recommended standards and every company in the first responder market builds their technology to be plug-and-play, then public safety agencies will be able to pick the technologies that fit best with their mission without worrying about whether or not the devices will work together.

Fully Aware Portfolio – Making Informed Decisions That Save Lives

NGFR's Fully Aware Portfolio helps convey the right information to responders at the right time by integrating wearables, sensors, and remote monitoring, and then analyzing the data they provide. Situational awareness tools can provide critical context even before responders arrive on scene, allowing them to jump into the response already knowing what to do. Data analytics, artificial intelligence, and other advanced decision support tools help sift through a significant amount of sensor data to identify what information is important for decision-making. Alerts and notifications help present that information to responders in a usable way that draws attention to priorities.

NGFR Integration Demonstrations/Operational Experimentations

In order to develop the technologies each portfolio focuses on, the NGFR Apex Program conducts Integration Demonstrations or Operational Experiments. These demonstrations and experiments include a range of test and evaluation events, including simple table-top tests, PlugTest, set in a laboratory environment,[10] Technology Experiments in the field, and finally full-scale Operational Experimentations, which assess technology integration in an operational setting with end-users. DHS S&T has held a series of NGFR Integration Demonstrations/Operational

[9] The NGFR Integration Handbook and more information about it is available at: https://www.dhs.gov/science-and-technology/ngfr/handbook.

[10] NGFRs conducted PlugTest, a lab-based experiment, to test the architecture and standards documented in the NGFR Integration Handbook, using a small set of technologies. NGFR structured the event to validate interoperability characteristics in three primary functional categories: sensors (e.g., physiological, chemical, location), communication hubs, and situational awareness tools.

Experimentations (OpEx)[11] to incrementally test and evaluate interoperable technologies currently in development, and to assess how DHS-funded technologies, commercially-developed technologies, and existing first responder systems integrate to improve response operations.

Since 2016, these demonstrations have evolved from tabletop integrations to field exercises with partner public safety agencies and have matured to include more commercial technologies. During many of these events, first responder partners simulate emergency response activities to a pre-scripted incident while using the DHS or industry partner-provided technologies. While these demonstrations and exercises are similar to exercises that public safety agencies conduct to improve their preparedness, DHS S&T adds both the new technologies and a technology evaluation framework to assess the devices and whether they improve responder operations.

For example, the Program will conduct the Birmingham Shaken Fury Operational Experimentation (OpEx) in August 2019, at Legion Field stadium in Birmingham, Alabama, in partnership with regional public safety agencies and technology providers. DHS S&T partnered with public safety agencies in Birmingham and Jefferson County, Alabama, because they will be hosting the World Games 2021, a major international multi-sport competition. The City and County seek to augment their public safety capabilities and assess how advanced, integrated technologies can help better prepare responders and emergency managers for planned events, like the World Games, and no-notice events, like natural disasters. Technology solutions and capabilities to be assessed during the Birmingham OpEx include: gas sensors (location, gas, physiological), smartphones, data collection point, mobile device management, data translator (e.g., converts data into a common format), on-body signal router, evacuation modeling, situational awareness platforms, deployable communication systems, video streaming, body-worn cameras, resource management tracking, small Unmanned Aircraft Systems (sUAS), and emergency vehicle traffic signal preemption systems.

One key component of the NGFR Apex Program is the focus on interoperability in the technical approach and across the Program's diverse projects. Technologies developed by projects within the NGFR Apex Program must be "modular," meaning that first responders can select different technologies that will easily integrate via open standards and interfaces. Technologies must also be "scalable," meaning that responders can build a large and complex system or a small and streamlined system, depending on their mission needs and budget. The Program considers gathering responder feedback critical to helping improve both individual technologies developed for first responders and the NGFR integration approach.

[11] More information on specific NGFR Integration Demonstrations and the technologies tested is available at: https://www.dhs.gov/science-and-technology/ngfr-integration-demonstrations.

DHS S&T incorporates the results and responder/industry feedback from the NGFR Integration Demonstrations/OpEx events into the NGFR Integration Handbook, which outlines a standards-based environment that enables commercially-developed technologies to integrate with existing first responder infrastructure. Using the lessons learned and responder feedback from these integration demonstrations, DHS S&T has also produced materials to help public safety agencies implement new technologies that address their capability gaps and operational priorities. For example, the NGFR Case Study series helps agencies understand how tools like location services,[12] deployable communications,[13] video services,[14] physiological monitoring,[15] and situational awareness[16] can improve their mission response and provides guidance on how agencies can best implement them.

The NGFR Apex Program's Collection, Use, Dissemination, and Maintenance of PII

DHS S&T and its research and technical partners collect, use, maintain, and disseminate PII and sensitive privacy-related data in three categories of information collection: administrative, communications and outreach, and technology assessment. The NGFR Apex Program does not permanently retain any PII.

(1) Administrative: Administrative data is PII collected, used, and maintained about individuals who participate in NGFR Integration Demonstrations/OpEx events. Administrative data is used to facilitate planning and execution of the event.

- *Application Forms*: When industry partners apply to participate in an NGFR Integration Demonstration/OpEx, they respond to a Request for Information for Participation posted on FedBizOpps.gov by submitting an application for their company via email that includes contact information for the submitter. Information collected includes: organization name, organization type, state of incorporation, country of incorporation, parent corporation (if applicable), DUNS Number/Cage code, principal place of business address, preferred contact (name, title, email, phone number), legal counsel contact (name, title,

[12] NGFR Case Study: Location Services is *available at*: https://www.dhs.gov/publication/st-frg-ngfr-case-study-location-services.
[13] NGFR Case Study: Deployable Communications is *available at*: https://www.dhs.gov/publication/st-frg-ngfr-case-study-deployable-communications.
[14] NGFR Case Study: Video Services is *available at*: https://www.dhs.gov/publication/st-frg-ngfr-case-study-video-services.
[15] NGFR Case Study: Physiological Monitoring is *available at*: https://www.dhs.gov/publication/st-frg-ngfr-case-study-physiological-monitoring.
[16] NGFR Case Study: Situational Awareness is *available at*: https://www.dhs.gov/publication/st-frg-ngfr-case-study-situational-awareness.

email, phone number), and details of the technology solution that it would like to participate in the event.

Submission of an application is fully voluntary. DHS S&T uses the contact information to notify the company of the selection decision and, for those selected, to coordinate any legal requirements. DHS S&T stores application materials containing PII on secure DHS S&T federal and contractor computer workstations, with Personal Identity Verification (PIV)-card and personal identification (PIN) access controls on the secure DHS network. Following the conclusion of the NGFR Apex Program, all application materials relating to NGFR events are destroyed.

- *Registration*: The NGFR Apex Program collects NGFR Integration Demonstration/OpEx participant names, email addresses, and agency/affiliation through an online registration site (Cvent) or via email and Excel spreadsheet. Participant contact information is used to coordinate event logistics, understand facility capacity, to assure that adequate supplies of printed materials are available, take attendance, and cross-check participant lists to ensure that each participant signs the mandatory Rules of Behavior for that NGFR Integration Demonstration/OpEx, which includes a video and media use authorization section, Privacy Act Statement or Privacy Notice, liability waivers, and other rules affecting event participation.

  DHS S&T stores registration materials containing PII on secure DHS S&T federal and contractor computer workstations, which are PIV-card and PIN protected and on the secure DHS network, and on the restricted NGFR Apex Program site on the Homeland Security Information Network (HSIN),[17] and Cvent (online registration site). Access to the PII is limited to DHS employees and DHS contractors with a need-to-know. Following the conclusion of the NGFR Apex Program, all registration materials and records containing participant PII from NGFR events are destroyed.

- *Equipment Issuance Lists*: DHS S&T develops an Equipment Issuance List with the participant information from registration—including names, organization, and email addresses—which is used to assign, issue, and confirm returns of technologies provided by DHS S&T to participating volunteer first responder participants, ensuring that all devices are returned. If equipment being issued to

[17] For more information about HSIN, please see DHS/ALL/PIA-061 HSIN 3.0 Shared Spaces On The Sensitive But Unclassified Network, *available at* https://www.dhs.gov/privacy.

a participant is not DHS-furnished, the equipment provider *is not* provided access to this participant PII.

DHS S&T stores registration materials containing PII on secure DHS S&T federal and contractor computer workstations, which are PIV-card and PIN protected, on the secure DHS network, and on the restricted NGFR Apex Program site on the Homeland Security Information Network (HSIN). Access to the PII will be limited to DHS employees and DHS contractors with a need-to-know. Following the conclusion of the NGFR Apex Program, all equipment issuance lists and records containing participant PII from NGFR events will be destroyed.

(2) Communications and Outreach: Communications and outreach data is collected at NGFR Integration Demonstrations, OpEx events, and stakeholder outreach events such as conferences, and includes business cards with PII contact information, media and press contact information, and photography, videography, and audio recording releases for promotional purposes.

- *Business Cards with PII*: Industry and public safety personnel voluntarily give DHS S&T federal and contractor staff business cards during stakeholder outreach events such as conferences, seminars, and association meetings. PII, in the form of business contact information, may be extracted from these sources and included in an NGFR contact list file. DHS S&T federal and contractor staff use this information to identify and engage new industry and public safety partners to advance the NGFR Apex Program.
- *Media and Press Contact Information*: DHS S&T works with public safety partners to identify local media outlets in the areas where NGFR Integration Demonstrations/OpEx events occur. Media and press contact information includes name, organization, email, and phone number. DHS S&T uses this information to disseminate press releases and media advisories and to invite journalists to attend and to engage general audiences on NGFR events, technology, R&D, demonstrations, and experiments. Following the conclusion of the NGFR Apex Program, media contacts will be destroyed or transferred to the S&T Communication and Outreach Division. The NGFR Apex Program collects media and press contact information only in connection with externally-facing NGFR Integration Demonstrations/OpEx events.
- *Photography, Videography, and Audio*: DHS S&T and partners participating in NGFR Integration Demonstrations, OpEx events, and stakeholder outreach

events (conferences, seminars, and association meetings) collect photographs, video footage, and audio recordings regarding the event.

DHS S&T and NGFR Apex Program staff capture photographs, video footage, and audio recordings for purposes of enhancing outreach materials about S&T and the NGFR Apex Program. For NGFR Integration Demonstrations and OpEx events, all participants sign a Rules of Behavior form that includes a Media Use Authorization release that grants DHS S&T unlimited use rights to the participant's likeness from photos or videos during the event.

DHS S&T staff and technologies capture photos and video footage during all NGFR Integration Demonstrations to improve outreach about the impacts of the event and the NGFR Apex Program. Any participant may capture photos and video footage during an NGFR Integration Demonstration, and may use government-furnished equipment, partner-furnished equipment, first responder agency-furnished equipment, and/or invited local and national media-furnished equipment. Participants may voluntarily share their photos and video footage with DHS S&T for use in DHS products, with credit to the contributor. Any photos or video footage collected by DHS S&T or shared for DHS S&T use may be included in DHS products, which may be made publicly available on platforms including the DHS website, public safety agency partners' websites, and social media platforms.

Once captured by DHS S&T, all photo, video, and audio materials become the property of DHS S&T Communication and Outreach Division to promote DHS S&T. DHS S&T may use images and video from NGFR Integration Demonstrations/OpEx events and stakeholder outreach events for communication products that are unrelated to the NGFR Apex Program, such as DHS S&T annual reports, other first responder-focused outreach products, collage images of S&T activities, or general S&T social media outreach.

All participants and observers who choose to engage with invited media at NGFR Integration Demonstrations/OpEx events do so according to the rules implemented by their participating agency, organization, or company's public affairs office. DHS S&T is not responsible for the photographs, video, and audio of participants and observers that are collected by invited media.

(3) Technology Assessment: Technology assessment data is collected by devices, systems, applications, software, or hardware technology solutions that are participating in an NGFR Integration Demonstration/OpEx, as well as the evaluation data collected by the DHS S&T test and evaluation staff. Technology solutions may be provided by DHS

S&T, S&T technical performer partners on research and development contracts and subcontracts, or certain industry and academia partners.

Technology solutions deployed for an NGFR Integration Demonstration/OpEx may collect PII. Such technologies include those collecting locations of devices or individuals, vital signs of individuals, and video with audio of individuals. DHS S&T will not use any of the data collected by or transmitted through any of the technology solutions to determine the identities of individuals. This data is not retained by DHS S&T following the completion of an NGFR Integration Demonstration/OpEx and is deleted from DHS S&T-provided devices no later than 180 days after completion of the event.

Because the NGFR Apex Program aims to integrate technologies using open data standards, the majority of NGFR Integration Demonstration/OpEx technology solutions seek to show how the technology selected from a specific event can integrate to share data between multiple technology solutions. This means the devices and technologies involved in an event may share PII among multiple solutions to increase the situational awareness of first responder volunteer actors during simulated operational use at the NGFR Integration Demonstration/OpEx. This data is not retained by DHS S&T following the completion of an NGFR Integration Demonstration/OpEx and is deleted from DHS S&T-provided devices. DHS S&T requests that industry and public safety partners who provide the remaining devices also delete all data from an NGFR Integration Demonstration/OpEx no later than 180 days after the completion of the event.[18]

DHS S&T evaluates how the first responders use the technology solutions and the data they collect, transfer, use, and display to make operational decisions during the simulated scenario. DHS S&T will collect information from first responder volunteer actors on anonymized data collection sheets to document how first responders are using the technologies and their specific feedback on the technologies, including form, fit, and function. Evaluation methods may include direct observation, individual interviews, and focus groups. The first responder feedback gathered through each of these evaluation methods is anonymized. This anonymized feedback is shared with the

[18] DHS S&T documents these request requirements through Memoranda of Agreement with public safety partners and Cooperative Research and Development Agreements with industry partners.

technology providers to improve their technology solutions, as well as incorporated into DHS S&T products such as after-action reports or case studies.

The DHS S&T Human Subjects Research (HSR) Protections Branch Compliance Office works with the NGFR Apex Program to determine whether volunteer participant involvement in an NGFR Integration Demonstration/OpEx constitutes HSR. If it is, the NGFR Apex Program works with the HSR Protections Branch to assure that the appropriate HSR protections are incorporated into the NGFR Integration Demonstration/OpEx, including an Informed Consent to be signed by each volunteer participant.[19]

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal Government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The Homeland Security Act of 2002 Sections 222 (a) (1) and (a) (2) states that the Chief Privacy Officer shall assure that personal information contained in DHS Privacy Act systems of records, as well as non-privacy information systems is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

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

DHS conducts PIAs on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208, and the Homeland Security Act of 2002, Section 222. Given that the NGFR Apex Program is not a particular information technology system, this PIA is conducted as it relates to the DHS construct of the Fair Information Practice Principles. This PIA examines the privacy impact of the NGFR Apex Program operations as it relates to the Fair Information Practice Principles.

[19] *See* DHS Directive 026-04 Protection of Human Subjects , *available at* https://www.dhs.gov/sites/default/files/publications/mgmt-directive-026-04-protection-of-human-subjects.pdf.

1. Principle of Transparency

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

This PIA provides notice about the NGFR Apex Program, its activities, and privacy risks and mitigations. General information about the Program is available on the DHS website.[20] Additionally, the activities undertaken by the Program are generally planned well in advance and executed with the help of a number of different agencies and participants. With NGFR Integration Demonstration/OpEx specifically, DHS S&T must work with regional agencies and local government to conduct these activities because they are generally conducted in public areas and require local authority assistance and participation.

All individuals who participate in NGFR Apex Program activities sign Rules of Behavior that outline the collection and use of the data.

Privacy Risk: There is a privacy risk that participants at an NGFR Integration Demonstration/OpEx may not be aware that DHS S&T is collecting PII before and during the event.

Mitigation: DHS S&T mitigates this risk in in several ways. DHS S&T provides notice of data collection through this PIA and the Rules of Behavior for an NGFR Integration Demonstration/OpEx. The applicable Rules of Behavior include a Privacy Act Statement or Privacy Notice. Individuals who do not accept and sign an event's Rules of Behavior are not permitted to attend or otherwise participate in that event. The Rules of Behavior are electronically distributed to registered participants at least one week in advance of the NGFR Integration Demonstration/OpEx and then signed in hard-copy at the event check-in. DHS S&T and/or participating public safety partners also post notice signage at the event check-in to remind participants of event data collection, such as videography and photography.

Privacy Risk: There is a privacy risk that individuals near an NGFR Integration Demonstrations/OpEx venue may be unaware that their information, such as images and video or device information, could be captured as part of the testing activities.

Mitigation: DHS S&T's public safety partners post barriers and/or signage to control access to any NGFR Integration Demonstration test sites. Those members of the public who enter an area where NGFR Integration Demonstration activities are occurring have given consent to possibly having their images inadvertently captured by not obeying the signs and altering their path. Even in such cases, DHS S&T will not use such images to identify persons. DHS S&T's

[20] *See* https://www.dhs.gov/science-and-technology/ngfr.

public safety partners may also choose to notify the public using other methods, such as alerting the media, communicating with neighborhood associations, posting signage around the test site neighborhood, or posting on local government social media accounts.

During an NGFR event, all electronic devices to be used as part of the event are registered through a mobile device management process. Data collected or transmitted by an electronic device (such as a personal cell phone) not registered through the event's mobile device management process is not collected or viewed by the event participants. The electronic signal data is thus limited to that collected by the registered devices.

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.

The NGFR Apex Program's collection of PII from individuals relies on the fact that an individual providing PII in connection with an Integration Demonstrations/OpEx is entirely voluntary. To participate in an Apex Program event as either an attendee, partner, OpEx actor, or other role and to enter the venue where the event is held, the individual must sign the Rules of Behavior for that specific event. An Integration Demonstration/OpEx Rules of Behavior provides the participant information on all PII that may be collected from the individual as an event participant, the uses that DHS S&T may make of that PII, and obtains consent to the collection of that PII. Participants sign the Rules of Behavior and if an individual objects to his or her PII being collected or to any of the disclosed possible uses of that PII, he or she is not permitted to participate in the event.

Privacy Risk: There is a privacy risk that a participant at an NGFR Integration Demonstration/OpEx may not provide knowing consent to participate in an NGFR event.

Mitigation: The Program mitigates this risk by requiring registration for NGFR Integration Demonstrations events from all participants or attendees, including government employees, contractors, other S&T partners, state and local public safety partners, observers, VIPs, and media, are required, in order to participate in an event, to sign the event's Rules of Behavior. Individual participants have the opportunity, through the event's Rules of Behavior and the registration process to consent to program uses, decline to provide information, or opt out of the event. This applies to both past and future events, and these requirements are further described in PTAs associated with individual NGFR Integration Demonstrations and OpEx events.

An individual who does not agree to the terms and conditions and does not sign the Rules of Behavior is not permitted to attend or otherwise participate in the event. Consent must be given for the entire event and all uses of information and other terms and conditions; individuals cannot provide partial consent. Notices will be posted at the NGFR Integration Demonstration/OpEx

venue at check-in reminding participants that their likeness may be captured in photos and video footage from DHS, participant and media cameras, body-worn cameras, and UAS cameras (if the event includes UAS use).

Members of the public who are not registered participants are not permitted entrance to the NGFR Integration Demonstration/OpEx venue. For NGFR Integration Demonstrations in public settings, such as the NGFR – Birmingham Shaken Fury OpEx, which takes place in a city-owned stadium and adjoining parking lot, DHS S&T's local public safety partners erect obvious access control measures and post signage to demarcate the NGFR Integration Demonstration/OpEx area and provide notice of photography and videography.

Privacy Risk: There is a risk that DHS S&T may inadvertently collect information from members of the public (generally through photos and/or video) who have not consented to this collection and have no opportunity to opt out of the collection.

Mitigation: This risk is mitigated through several practices, particularly with reference to individuals who are outside the event boundaries and who are not participants in the event. DHS S&T's local public safety partners will post barricades and/or signage to control access to any NGFR Integration Demonstration/OpEx venues. The signage will advise members of the public who enter an area where NGFR Integration Demonstration/OpEx activities are occurring are deemed to have given consent to possibly having their images inadvertently captured by not obeying the signs and altering their path. Even in such cases, DHS S&T will not use such images to identify persons. Prior to the publication and/or release of NGFR Apex Program products, DHS S&T will review the products to ensure that they do not include any PII of individuals who are not event participants. For example, if a video of the event includes images of members of the public outside of the venue, the video will be edited to obscure the image of the individual to prevent identification.

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.

The Homeland Security Act of 2002 [Public Law 1007-296, §302(4)] authorizes DHS S&T to conduct "basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs." In exercising its responsibility, S&T is authorized to collect information, as appropriate, to support research, development, and other test and evaluation activities related to improving the security of the homeland.

The Intelligence Reform and Terrorism Prevention Act of 2004[21] established the Office for Interoperability and Compatibility within S&T to enhance public safety interoperable communications at all levels of government.[22] The Homeland Security Appropriations Act, 2007[23] further refined the Office for Interoperability and Compatibility's responsibilities to focus on research, development, testing, evaluation, and acceleration of the development of standards to improve interoperable communications.[24]

In particular, the Office for Interoperability and Compatibility shall "encourage the development and implementation of flexible and open architectures incorporating, where possible, technologies that currently are commercially available, with appropriate levels of security, for short-term and long-term solutions to public safety communications interoperability."[25]

Privacy Risk: There is a privacy risk that DHS S&T may collect or use PII outside of its intended and legislatively-authorized purpose.

Mitigation: This risk is mitigated. DHS S&T will collect and use information for the NGFR Apex Program only in accordance with the authorities described above and in the Introduction section of this PIA and limited to the purpose of developing and integrating next generation technologies with the goal of expanding first responder mission effectiveness and safety.

The Program submits PTAs to the DHS Privacy Office for adjudication specifying the use of PII by specific RDT&E projects and for specific NGFR events using those technologies.

4. Principle of Data Minimization

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

The NGFR Apex Program applies the principle of data minimization by limiting the PII collected from Integration Demonstrations/OpExs to that necessary to (1) effect registration of each event participant and attendee and (2) provide the minimum necessary information to communicate with registrants about the event. This same information is used to track to whom devices and equipment provided for use as part of the event to assure return of these items at the event's conclusion. Event devices and equipment, including various types of sensors, used by

[21] Public Law 108-458.
[22] 6 U.S.C. § 194.
[23] Public Law 109-295.
[24] 6 U.S.C. § 195.
[25] 6 U.S.C. § 194(a.1.E).

participants playing an assigned role in an event may also collect PII, such as location information and, in some cases, the role player's selected physiological information. Videos and images may also be taken of participants during an event. This PII is collected only within the event venue's boundaries and every effort is made not to inadvertently collect images, videos, or other personal information from individuals outside the event boundaries. Location and physiological information collected from Integration Demonstration/OpEx participants is not retained after the event concludes.

Privacy Risk: There is a privacy risk that DHS S&T may collect non-relevant PII beyond what is needed to accomplish the specified purpose of the NGFR Apex Program.

Mitigation: This risk is mitigated. All Administrative, Communications and Outreach, or Technology Assessment Information PII collected and used by DHS S&T is essential to successfully plan, execute, and report on NGFR Integration Demonstrations and/or conduct NGFR Apex Program communications and outreach. DHS S&T will collect and use Administrative, Communications and Outreach, or Technology Assessment Information PII for the NGFR Apex Program only as described in this PIA and in the specific PTA and Rules of Behavior associated with the NGFR Integration Demonstration/OpEx.

Privacy Risk: There is a privacy risk that DHS S&T may retain PII collected by it or on its behalf in connection with an NGFR Integration Demonstration/OpEx for longer than is needed to accomplish the specified purpose of the NGFR Apex Program.

Mitigation: This risk is mitigated. DHS S&T will dispose of PII collected by it or on its behalf in connection with Program Administrative, Communications and Outreach, or Technology Assessment activities when it is no longer needed for program activities or at the conclusion of the NGFR Apex Program, as described in the PTA associated with the NGFR Integration Demonstration/OpEx for which it was collected. DHS S&T will dispose of this PII in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

DHS S&T will retain contact information from applications, registrations, and business cards until the conclusion of the NGFR Apex Program, and then destroy the paper and electronic records.

DHS S&T will retain photography, videography, and audio recordings collected for communications and outreach indefinitely, as under the Rules of Behavior documentation, these become the property of DHS S&T for use in outreach and knowledge products.

DHS S&T will retain test data collected from technology solutions at NGFR Integration Demonstrations/OpEx events for no longer than 180 days after the even, with the exception of

video and images collected by technology solutions, including body worn cameras and UAS, which will be destroyed at the conclusion of the event.[26]

PII retention and destruction plans are described in the specific project PTAs associated with the NGFR Apex Program and adjudicated by the DHS Privacy Office. DHS S&T will dispose of this PII in accordance with DHS records disposition schedules as approved by NARA.

5. Principle of Use Limitation

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

The NGFR Apex Program is structured to limit the PII it collects from (1) industry partners applying to participate in an Integration Demonstration/OpEx, (2) individuals registering to participate or attending an event, and (3) event participants to whom devices and equipment are issued for use during the Integration Demonstration/OpEx, and the uses of that PII.

Use of PII collected by DHS S&T in connection with event registration is limited to DHS federal employees and contractor staff with a need to know. All such PII will be destroyed at the conclusion of the NGFR Apex Program. Similar use/access and data destruction requirements exist with regard to PII collected on equipment issuance lists used to assign, issue, and confirm returns of technologies provided by DHS S&T to participant volunteers. This PII is not shared with DHS industry partners involved with an Integration Demonstration/OpEx.

Depending on the nature of the technologies to be used at a particular Integration Demonstration/OpEx, a device or technology may collect physiological and other personal information from the volunteer participant to whom the device/technology is issued. That information may be shared among the other devices/technology involved in the event. However, this personal information is not linked to the volunteers' name or contact information. This data is not retained by DHS S&T following the completion of an NGFR Integration Demonstration/OpEx and is deleted from DHS S&T provided devices.

Privacy Risk: There is a privacy risk that DHS S&T may use PII for purpose(s) beyond those specified in this PIA or other related notices.

Mitigation: This risk is mitigated. DHS S&T will only use PII collected or received by it in connection with the NGFR Apex Program Integration Demonstration/OpEx for purposes outlined in this PIA, PTAs associated with the NGFR Apex Program, or in any notices developed to facilitate the NGFR Apex Program and its activities. DHS S&T will further specify and clarify

[26] Note: While body worn camera and UAS video footage and image files are destroyed at the end of the event, this does not include videos and images taken for communications and outreach purposes by DHS or other participating organizations, which are retained as described above.

the uses and purposes of such PII within the framework of this PIA in PTAs associated with the NGFR Apex Program, in NGFR Integration Demonstration/OpEx Rules of Behavior, and in any other posted, published, or written notice associated with the NGFR Apex Program and its events. All NGFR Apex Program uses and PII further outlined in this documentation will align to the principles of this PIA, and all PII will be used for Administrative, Communications and Outreach, or Technology Assessment purposes only. DHS S&T technical and research partners must use and store any NGFR-related PII they maintain on their own secure computer systems according to DHS S&T security requirements for PII.

Furthermore, DHS S&T does not share the PII collected by the Program unnecessarily. Access to the PII is be limited to DHS employees and DHS contractors with a need-to-know.

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.

Contact information is provided by individuals who are registering to participate or attend an Integration Demonstration/OpEx event or by their company (in the case of industry partners) or state, local, or tribal first responder organization, public safety organization, or government entity for which they work. This information may be easily corrected at the request of the individual. With respect to personal information that may be collected by devices/technologies deployed at an NGFR Apex Program event, the purpose of collecting this data is not to make decisions about the individual. Rather, the purpose is to test the ability of the event's deployed devices/technology to integrate and share the data to better support first responders.

Privacy Risk: There is a privacy risk that PII may not be accurate, relevant, timely, and complete, within the context of each use of the PII.

Mitigation: This risk is partially mitigated within the context of the PII's use for applications, registration, etc. DHS S&T relies on public safety departments, industry, and other stakeholder partners to provide relevant, timely, and complete accurate PII, either through individually-provided, self-entered data or through technology-solution collected data. Any individual who believes that NGFR-related PII is not accurate, relevant, timely, or complete and would like to access, correct, or redress DHS's use of his or her PII may contact the NGFR Apex Program at NGFR@hq.dhs.gov.

Furthermore, inaccurate PII will generally not affect the results of a Program activity nor have any negative impact on that individual. The goal of the Program is not to collect PII; PII is used as a necessary tool to facilitate the Program's mission of expanding first responder effectiveness and safety through the development of new technologies and practices.

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.

PII collected and retained by DHS S&T in connection with the NGFR Apex Program (including video and images) is stored on secured DHS SharePoint sites, DHS HSIN, and, in the case of event registration information, Cvent. Access to this PII is limited to DHS federal employees and contractor personnel who access the data through DHS configured workstations and laptops requiring PIV card and PIN access through the secure DHS network. Personal information, if any, collected from volunteer participants through devices/technology issued for use during an Integration Demonstration/OpEx event is destroyed within 180 days after the conclusion of the event.

Privacy Risk: There is a privacy risk of unauthorized loss or disclosure of PII due to a security incident with DHS S&T-maintained PII.

Mitigation: DHS S&T mitigates the likelihood of an unauthorized loss or disclosure of PII due to a security incident by having all DHS S&T-maintained PII secured either on DHS S&T federal or contractor computer workstations that follow all DHS security requirements and polices or in a locked container or room, limiting access to PII to those with a need-to-know, and having all DHS S&T federal and contractor staff complete the annual mandatory DHS privacy training and information security training. DHS S&T partners on a contract or subcontract do not have access to DHS S&T computer workstations and must store any NGFR-related PII they maintain on their own secure computer systems according to DHS S&T security requirements for PII.

Privacy Risk: There is a privacy risk of unauthorized loss or disclosure of PII due to a security incident with partner-maintained PII.

Mitigation: DHS S&T mitigates the likelihood of an unauthorized loss or disclosure of PII due to a security incident by requesting that industry, research, technical, and public safety partners comply with minimum security requirements for data storage and requesting destruction of all test data no later than 180 days following an NGFR Integration Demonstration/OpEx and requiring video data deletion immediately at the conclusion of the event. While DHS S&T is unable to legally require that these partners comply with this request, DHS S&T requests that if industry and/or public safety partners know or suspect a breach of data security, including that of PII or sensitive privacy-related test data, they immediately notify DHS of the incident and planned containment.

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.

DHS S&T federal employees and contractor staff responsible for the NGFR Apex Program undergo Privacy and IT Security training. Supervisors will ensure that policies and procedures are fully enforced through auditing and reviews of programs and practices. Access controls are in place to ensure only authorized users access DHS S&T systems and images.

Privacy Risk: There is a privacy risk that DHS S&T staff will not comply with the FIPPs and will inadequately protect PII collected and used under the NGFR Apex Program.

Mitigation: DHS has an organizational commitment to accountability for legal and privacy policy requirements as well as internal DHS policies and procedures with regard to PII collected by it or in its behalf. DHS S&T staff are all required to undergo annual privacy training, and S&T contracted partners, public safety organization partners, and other partners are notified by the DHS S&T of their requirements for protecting any PII related to the NGFR Apex Program and their work with it. Prior to the publication and/or release of NGFR Apex Program products, DHS S&T will review the products to ensure that they do not include any PII, except for PII (such as video and images) that participants at an Integration Demonstration/OpEx event have consent to use and disclosure through the applicable Rules of Behavior. At the closure of the NGFR Apex Program, DHS S&T will verify destruction of all PII collected by it or on its behalf that is still maintained according to the destruction guidance mentioned in this PIA.

Conclusion

DHS S&T's NGFR Apex Program is working to make first responders better protected, connected, and fully aware, protecting responders, industry partners, S&T technical performers and the public, while ensuring that program activities meet privacy requirements. The NGFR Apex Program will collect, use, maintain, disseminate, and destroy PII and sensitive privacy-related data for administrative, communications and outreach, and technology assessment purposes in accordance with this PIA and PTAs associated with the specific NGFR Apex Program activities. Specific risks will be addressed and mitigated for each activity according to the FIPPs principles, but this PIA provides transparency of the overall NGFR Apex Program and its mission.

Responsible Officials

John Merrill
Director, First Responders and Detection Division
Director, Next Generation First Responder Apex Program
Science and Technology Directorate
Department of Homeland Security

Approval Signature

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

_____

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