Privacy Impact Assessment

for the

Office of Industry Partnerships Portal (OIP Portal)

DHS Reference No. DHS/S&T/PIA-041

August 20, 2021

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Office of Industry Partnerships (OIP) manages a public-facing, standalone web portal (OIP Portal). The OIP Portal allows members of industry to submit proposals for Broad Agency Announcements (BAA) for DHS Research and Development (R&D)-related subjects, the Small Business Innovation Research (SBIR) program, and the Silicon Valley Innovation Program (SVIP). S&T is conducting this Privacy Impact Assessment (PIA) to address the OIP Portal's collection, use, maintenance, and dissemination of personally identifiable information (PII).

Overview

Office of Industry Partnerships (OIP)

OIP's mission is to engage industry and facilitate partnerships with private sector innovators to advance commercial technology solutions that address homeland security challenges. OIP's industry engagement, outreach, and awareness efforts focus on communicating S&T's partnership opportunities and homeland security R&D needs to industry. The S&T Industry Liaison within OIP engages with industry to maintain awareness of new and emerging commercial products, technologies, capabilities, and relevant companies[1] in a technology space. OIP also administers the Broad Agency Announcements,[2] Silicon Valley Innovation Program[3], and the Small Business Innovation Research,[4] programs to carry out these responsibilities.

S&T's BAAs allow S&T to use open-ended solicitations to quickly and efficiently execute R&D to deliver practical solutions to critical first responder problems. The Small Business Innovation Research program encourages U.S. small businesses with fewer than 500 employees to provide quality research and to develop new processes, products, and technologies in support of U.S. government missions. Silicon Valley Innovation Program expands S&T's reach to find new technologies that strengthen national security with the goal of reshaping how government, entrepreneurs, and industry work together to find cutting-edge solutions with government applications and to co-invest in and accelerate the timeframe to transition technology to the market.

S&T's innovation funding programs often have open solicitations that incentivize industry to help solve critical homeland security challenges. The contracting mechanisms and funding opportunities managed by S&T support S&T's partnership goals with the private sector to further

[1] The use of "company or companies" throughout this PIA includes all juridical persons regardless of the form the person takes.
[2] *See* https://www.dhs.govcience-and-technologyt-lrbaa.
[3] *See* https://www.dhs.govcience-and-technologyvip.
[4] *See* https://www.dhs.govcience-and-technologybir. S&T adheres to the U.S. Small Businesses Administration Office of Investment and Invocation policy to ensure SBIR programs proceed appropriately and follow all appropriate, rules, regulations, and applicable polices. *See* https://www.sba.gov/about-sbaba-locations/headquarters-offices/office-investment-innovation.

homeland security R&D needs. The OIP Portal is a proposal submission intake system allowing members of industry to respond to posted solicitations and compete for a contract award.

OIP Portal

The OIP Portal is a secure, web-based proposal and data management system that supports the S&T OIP BAA, SBIR, and SVIP proposal and award processes. The portal houses solicitations; proposals submitted by members of industry; awards; and contract deliverables, including business sensitive or For Official Use Only (FOUO) data and company intellectual property information.

The OIP Portal includes (1) a public-facing interface with training, document submission, and tracking capabilities for members of industry who seek to engage with S&T, and (2) an internal-use interface with documentation, tracking, query, and reporting requirements to include contract/data deliverables (e.g., test plans, monthly reports, test results) for contract deliverables. Support for these requirements necessitates tools and functionality for the entire life cycle of these OIP-administered programs for OIP program staff.

The OIP Portal supports functionality specific to the Broad Agency Announcement requirements, including housing of all topic and solicitation information and displaying public portions of this information to allow offerors to submit specific topics. The OIP Portal also supports functionality specific to the Small Business Innovation Research program's requirements, including maintaining a repository of all proposals and awards and contract/data deliverables per contract requirements as part of overall data management. Additionally, the OIP Portal supports functionality specific to Silicon Valley Innovation Program's requirements, including providing links on the OIP Portal's main public page to all SVIP-relevant functions, such as active topic calls, registration module, submission site, user login, and awards.

Members of industry can register and use the portal to submit proposals in response to solicitations posted by OIP, and once a contract is awarded, the contract awardees can upload contract/data deliverables (e.g., test plans, monthly reports, test results). The portal receives information and submissions from members of industry, then proposals are passed to the DHS Office of Procurement Operations (OPO) at the request of the contracting officer. Official notification of contract awards is not provided via the portal, but information about the award may be maintained within the portal. The contract award processes are handled through OPO. The portal serves as a resource to support the intake process, provide a data repository, and function as a one-way communication platform by the submitter.

The OIP Portal is hosted on the secure S&T Amazon Web Services (AWS) environment and is available to external and internal users through web-based interfaces on the DHS network. As the service provider, AWS does not have any rights to the data stored in the OIP Portal and the data is not visible to individuals within Amazon Web Services, as the data is encrypted. This is the default setting in AWS and cannot be turned off. S&T uses the AWS cloud-based computing

environment (to include infrastructure, platform, security boundaries, applications, and services) to control the user community access. Only individuals with a need-to-know will be permitted access to the OIP Portal.

User Community

External users consist of industry partners, or offerors from industry, seeking to do business with S&T. External users create an account in the OIP Portal, including the company president's business contact information, the contact information for an official point of contact (POC) within the company, and the business contact information for the principal investigator who will lead the research effort if the company is awarded a contract. The principal investigator is the individual designated by the company to provide scientific and technical direction to the project. The OIP Portal allows for multiple external users from the same company to register to use the portal. The company verifies external users as members of the company.

External users can use the portal to view open solicitations posted by OIP and submit proposals. External users' access in the portal is limited to viewing their own account and submissions, as well as information that is specifically publicly available. External users can view their own submitted proposals at any time after submission.

Internal users consist of S&T staff and contractors and may include federal employees and military personnel from other federal agencies. Assignments of specific roles in the portal allow administrators to assign internal users to specific solicitations, proposals, and contract packages. Internal users, other than administrators, only have access to the specific proposals and contract packages to which they have been assigned on a need-to-know basis, regardless of role assignments. Contract support staff roles within the portal will be limited in scope and assigned by federal S&T OIP employees.

Only S&T OIP and contractor staff can serve as administrators. Administrators enroll new internal users and assign specific user roles and specific solicitations. Administrators are able to upload and edit content on the public-facing side of the portal and upload content related to the solicitations and the proposal review process within the portal. Administrators can also create, view, download, and print customized reports. S&T OIP and contractor staff with administrative privileges can match all other user modes to mimic what a user sees for the purpose of troubleshooting, but they are not able to enter another user's account.

Certain S&T personnel are assigned Solicitation Manager roles. The Solicitation Manager role is limited to the BAA process. Solicitation Managers can access solicitation applications and manage and assign other users to specific solicitation submissions. Administrators grant Solicitation Managers access to their assigned solicitations after verifying that these are the persons selected to manage proposal submissions. Solicitation Managers have access to view the materials submitted by applicants in response to the publicized solicitations and provide detailed consensus

evaluations for proposals through the application. Solicitation Managers only have access to the information submitted for the solicitations to which they are assigned.

Reviewers, which include DHS and other federal agency and military personnel, have access to view the materials submitted by external users in response to the publicized solicitation topics and record detailed evaluations through the application. This evaluation is provided voluntarily by internal users, as part of their official duties, to aid in the proposal selection and contract award process. Only Reviewers can provide comments as part of their role in recording detailed evaluations. Other internal users will not provide comments on proposals. Reviewers' evaluations are visible only to internal users and are provided for the purpose of post-award feedback to offerors in compliance with Federal Acquisition Regulation 15.506.[5] Reviewers only have access to the information submitted for the topics to which they are assigned on a need-to-know basis by the program administrator. In addition to applicants' proposals, Reviewers have access to contractual deliverables and invoices which are submitted through the portal.

Some Reviewers use their support contractors to assist them with the execution of the program. The support contractors are given read-only roles and are only granted access to the data required to provide the necessary assistance to the reviewer. The read-only role prevents these support contractors from making any changes to the portal and the information contained within. Contract support staff roles within the portal will be limited in scope and assigned by federal S&T OIP employees.

Account Management

As a part of the internal user authentication process, in accordance with DHS 4300A Sensitive Systems Policy Handbook,[6] users will submit a request to DHS Office of the Chief Information Officer (OCIO). OCIO will collect PII as a means to grant privileged and general users' access to the OIP Portal. Currently, OCIO primarily uses usernames and passwords to regulate system authentication for the user community, which requires a collection of business email addresses and places of employment. The help desk will coordinate with the users directly to pass on the credentials.

The future state of the system will validate users by using single sign-on (SSO) smart cards, which will include Public Key Infrastructure (PKI), for internal users and a combination of passwords/pins and level 4 authentication for military personnel in other federal agencies. This process enables DHS to ensure that users of the OIP Portal have the access and privileges they need to perform their official duties and/or be responsive to posted solicitations. In addition, this will allow enhanced control of and access to PII used in the OIP Portal.

---

[5] *See* https://www.acquisition.gov/far/15.506.
[6] *See* DHS 4300A Sensitive Systems Policy Handbook (November 15, 2015), *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

The current credentialing and verification process is managed by S&T systems engineers to ensure access management is appropriately limited to validated internal users, per the following process until future state implementation is adopted:

1. The supervisor will submit the justification for the user's access.
2. The user will submit a General User or Privileged Account Request Form (which includes the designation of user roles).
    a. General User – this role has basic system access, predicated on being assigned to a project, and does not have administrative rights.
    b. Privileged User – this role has full access to the entire portal and can create additional privileged users as well as all other account types and access to all of the portal's administrative tools.
3. OCIO will use the user account request form submitted to validate that the person requesting access to the portal has the proper need-to-know.
4. The Information System Security Officer (ISSO) will approve the user request form.
5. The System Owner will approve the user request form.
6. The System Administrator will execute the technical elements of account creation and document the activity.

The External User account registration process is as follows:

1. The new external user selects the account registration button on the login page of the OIP Portal.
2. The external user will be prompted to enter the company Tax Identification Number (TIN) and the state in which the company is registered.
    a. The external user has the option to generate a Temporary Account Number (TAN) instead of a TIN if the TIN is not available.
3. The user is then taken to the registration screen. There are three sections:
    a. User and Account information – this include basic contact information about the external user registering the account, including their username, password, and a secret question and answer that is used for password recovery;
    b. Company Information – this includes basic company information such as location, DUNS Number, Commercial and Government Entity code (CAGE), and Standard Industrial Classification Codes (SIC Codes); and

c. Company POC – this includes the same fields as the External User Information section and is to be used to capture who the company POC will be.

4. The external user saves their registration and receives an auto-generated email from the OIP Portal confirming their account has been created. The account is considered active at this point.
5. Once an external user creates an account, the primary POC for the company will receive an automatic email notification alerting them to the creation of the external user account.

There is also a dedicated OIP Portal help desk. External users can contact the help desk support in order to correct, deactivate, or reactivate an account that has been deactivated due to inactivity in the portal. S&T OIP has developed Standard Operating Procedures (SOP) for the help desk support. An OIP Portal User Guide is also available for external users. The user guide explains the account creation and proposal submission processes, as well as how to contact the help desk regarding incorrect information included in the portal.

Data Sources and Use

External Users

External users create an account in the OIP Portal using information, including the company president's (i.e., leader's) business contact information, the contact information for an official POC within the company, and the business contact information for the principal investigator who will lead the research effort if the company is awarded a contract. In addition, external users provide information voluntarily as part of the proposal submission process. The OIP Portal requires external users to submit company contact information and upload proposal documentation, which may contain private sector proprietary data regarding the technologies, as well as business contact information for the company and employees, particularly those participating in the proposal, and cost proposal information. The OIP Portal uses this information to automate the administration of solicitations, submissions, evaluations, awards, and deliverable activities for OIP programs.

The OIP Portal also allows external users to submit contract/data deliverables (e.g., test plans, monthly reports, test results) following an award. These deliverables may contain additional, but similar PII beyond information used for OIP Portal registration purposes. For example, the deliverables may contain PII from the company individuals working on the project.

Internal Users

Internal users provide business contact information to create an account in the OIP Portal. After proposals are submitted by external users in response to a solicitation, certain internal users assigned to that specific solicitation conduct a review and evaluation to aid in the proposal selection and contract award process. Following the award of the contract, some federal internal

users will be assigned as Topic Managers and Contracting Officer's Representatives (COR). These Topic Managers and CORs will then have access to the documents submitted for the solicitation(s) to which they are assigned. Topic Managers and CORs also have access to contractual deliverables and invoices submitted by external users through the portal. Topic Managers and CORs only have access to the information submitted for the topics to which they are assigned.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

OIP, as part of S&T, administers the Broad Agency Announcements, Silicon Valley Innovation Program, and the Small Business Innovation Research programs to engage industry and facilitate partnerships with private sector innovators to advance commercial technology solutions that address homeland security challenges, benefit critical DHS missions throughout DHS Components, and fulfill its mission responsibilities under 6 U.S.C. § 182, Responsibilities and Authorities of the Under Secretary for Science and Technology. OIP views S&T authorities under 6 U.S.C § 182 in conjunction with the requirements set forth in the Privacy Act of 1974 and in DHS policy to ensure all data is properly collected.

The federal SBIR program is mandated by the Small Business Research and Development Act of 1982 (Public Law 97-219), the Small Business Research and Development Act of 1992 (Public Law 102-564), and most recently reauthorized under the National Defense Authorization Act of 2017 (Public Law 114–328). Per 15 U.S.C. § 638, the collection of data via the OIP Portal is required for mandatory annual reporting to Congress via the Small Business Administration (SBA) and Government Accountability Office on SBIR programs.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

DHS/ALL-002 Department of Homeland Security Mailing and Other Lists[7] covers the records maintained to facilitate contact with multiple POCs for proposal review and contract award.

DHS/ALL-004 General Information Technology Access Account Records System (GITAARS)[8] covers the records maintained to provide authorized access to the OIP Portal.

[7] *See* DHS/ALL-002 Department of Homeland Security Mailing and Other Lists, 73 Fed. Reg. 228, (November 25, 2008), *available at* https://www.dhs.govystem-records-notices-sorns.
[8] *See* DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 Fed. Reg. 70792, (November 27, 2012), *available at* https://www.dhs.govystem-records-notices-sorns.

DHS/S&T-001 Research, Development, Test, and Evaluation Records[9] covers records collected and maintained by DHS&T in support of, or during the conduct of, S&T-funded research, development, test, and evaluation activities, such as the data deliverables.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

A new system security plan was implemented on October 30, 2020, as a requirement for the Authority to Operate (ATO) package, which will be granted subsequent to the approval of this PIA and other compliance documentation.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Records included in and resulting from use of the OIP Portal are retained and disposed of in accordance with the S&T Records Inventory/File Plan for the OIP Portal System. In order to record potential intellectual property rights for the government and small business, records included in and resulting from the use of the OIP Portal are designated as permanent records. The current SBA SBIR and Small Business Technology Transfer (STTR) Policy Directive (May 2, 2019)[10] indicates that a small business retains data rights (intellectual property) for 20 years from the date of award of a contract.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The Paperwork Reduction Act (PRA) does not apply to this data collection effort.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

Information collected from external users for the purposes of creating an OIP Portal account includes:

- Company president's name;
- Company president's address;

[9] *See* DHS&T-001 Research, Development, Test, and Evaluation Records, 78 Fed. Reg. 3019, (January 15, 2013), *available at* https://www.dhs.govystem-records-notices-sorns.
[10] *Available at* https://www.sbir.govites/default/filesBIR-STTR_Policy_Directive_2019.pdf.

- Company president's email address;
- The name of an official point of contact within the company;
- The address of an official point of contact within the company;
- The telephone number of an official point of contact within the company;
- The email address of an official point of contact within the company;
- The name of the principal investigator who will lead the research effort if the company is awarded a contract;
- The address of the principal investigator who will lead the research effort if the company is awarded a contract;
- The telephone number of the principal investigator who will lead the research effort if the company is awarded a contract;
- The email address of the principal investigator who will lead the research effort if the company is awarded a contract;
- The company Taxpayer Identification Number (TIN);
- The state in which the company is registered; and
- The company's Dun & Bradstreet Data Universal Numbering System (DUNS Number).

Information collected from internal S&T users during OIP Portal account creation includes:

- First name;
- Last name;
- Phone number;
- Email address;
- Whether the user is a federal government employee;
- Agency; and
- The specific role(s) to which they are assigned within the system.

New internal users submit this account creation information to S&T OIP via email at stsbir.program@hq.dhs.gov. OIP Portal Administrators collect this information and enter it into an internal user roster that is stored within the portal.

External users submit proposals in response to solicitations posted by OIP by completing

standard information collection forms and uploading proposal documentation to the portal in various formats, including portable document format (PDF), deck, spreadsheet, and audio/video files. The packages are reviewed by S&T subject matter experts. Proposal submissions may include:

- Private sector proprietary data regarding the technologies in the proposal classified as FOUO;
- Business contact information for the company and employee, particularly those participating in the project;
- Contract/data deliverables (e.g., test plans, monthly reports, test results, technical reports, invoices);[11] and
- Cost proposal information.

This PIA will be updated prior to the OIP Portal collecting additional PII or Sensitive PII (SPII).

2.2 What are the sources of the information and how is the information collected for the project?

External users provide information voluntarily as part of the proposal submission process. Data from external users can be manually entered into fillable forms within the portal and uploaded in the form of a PDF or deck as part of the proposal submission package.

Internal users have the ability to conduct individual and consensus reviews of submitted proposals, which include reviewer ratings and supporting narrative, through fillable forms within the portal. Internal users with an administrator role can upload documentation for contract awards and populate deliverable fields that will need to be uploaded by the offerors.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The OIP Portal does not collect or use data from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

The external user is responsible for the accuracy, completeness, and quality of the data provided via the OIP Portal. Private sector proprietary data is protected appropriately during

[11] Contract/data deliverables submitted by external users following contract award will be classified up to the For Official Use Only (FOUO) level. These deliverables may contain additional, but similar PII beyond what is used for OIP Portal registration purposes. For example, the deliverables may contain PII from the company individuals working on the project.

submission and encrypted while stored within the OIP Portal. Additionally, the OIP Portal limits user access based on the user's role. External users are only able to view their own account and submissions, as well as the information in the OIP Portal that is specifically publicly available.

S&T staff collect, verify, and validate project information collected in the system throughout a project's lifecycle. Internal users are granted access only to the appropriate solicitation application(s) within the OIP Portal and the topics to which they are assigned, on a need-to-know basis. Administrators review OIP Portal information to ensure it is compliant with processes and regulations and recommend approaches to preserve data integrity and usability of the portal.

Role-based training is provided for internal users and includes awareness on proper handling of PII and source selection and intellectual property data rights. OIP conducts training throughout the implementation of the OIP programs. Internal portal users receive this training for every round of BAA or SBIR evaluations. Additionally, training will be conducted for internal portal users to ensure they respond appropriately and consistently if an external user submits unsolicited PII or other data that is classified at a higher level than FOUO. If an internal user sees PII or other data that should not have been uploaded to the portal they will contact the System Administrator and the S&T Privacy Office. If information classified at a higher level than FOUO is uploaded on the OIP Portal the OIP Program Office will report the occurrence to DHS Network Operations Security Center (NOSC); subsequently, DHS would coordinate with the owner of the information to determine the appropriate level of sanitization. The Small Business Innovation Research program will also conduct training with external users to ensure that the submitters understand they are not to submit contract/data deliverables that include unsolicited PII or other data that is classified at a higher level than FOUO.

Further, all users are required to review and acknowledge Rules of Behavior (ROB), ensuring that they actively participate in a successful program for information security. Non-Disclosure Agreements (NDA) are required for contractor support users prior to access to the system. Lastly, all new S&T workforce members receive introductory privacy and security training at orientation, and all OIP Portal users are subject to user agreements to protect the integrity of the data.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: The OIP Portal may collect more information than necessary.

Mitigation: This risk is mitigated. External users provide information voluntarily. As part of the user registration process, the OIP Portal only solicits information relevant to establishing and maintaining user accounts. External users also voluntarily provide all information when completing fillable forms or uploading proposal documentation. Topic and solicitation calls

include instructions regarding what information to include in a proposal submission. In addition, external uses have the ability to edit or delete information or documentation from their proposal package prior to formal submission.

Further, the SBIR program will conduct training with external users to ensure that the submitters understand they are not to submit contract/data deliverables that include unsolicited PII or other data that is classified at a higher level than FOUO. Training will be conducted for internal portal users to ensure they respond appropriately and consistently if an external user submits unsolicited PII.

Additionally, S&T OIP is developing a Terms of Service for portal users. The Terms of Service will require users to acknowledge and agree to submit only PII that is specifically solicited by the OIP Portal.

Privacy Risk: There is a risk OIP Portal data may be compromised after it is submitted through the portal.

Mitigation: This risk is mitigated. Private sector proprietary data is encrypted while stored within the OIP Portal. OIP conducts training throughout the implementation of the OIP programs. Role-based training is provided for internal users and includes awareness on proper handling of PII and source selection and intellectual property data rights. Internal users do not receive access to the proposals to which they are assigned until they have completed the training associated with the specific proposal. Additionally, program-specific training may be implemented as well. For example, for every round of SBIR evaluations, internal portal users receive this training. All users are also required to review and acknowledge Rules of Behavior, ensuring that they actively participate in a successful program for information security. NDAs are required for contractor support users prior to access to the system. Lastly, all new S&T workforce members receive introductory privacy and security training at orientation, and all OIP Portal users are subject to user agreements to protect the integrity of the data.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

External users provide company information and employee contact information during the account creation process. Internal users also provide contact information during the account creation process.

External users also provide information voluntarily as part of the proposal submission process. The OIP Portal requires the collection of company information and proposal uploads, which may contain private sector proprietary data regarding the technologies in the proposal, as well as business contact information for the company and employee—particularly those participating in the project—and cost proposal information in order to automate the administration

of solicitations, submissions, evaluations, awards, and deliverable activities for OIP programs.

The data collected is required for the determination of eligibility and for contract award. Per 15 U.S.C. § 638, this data collection is also required for mandatory annual reporting to Congress via the SBA and Government Accountability Office on SBIR programs.

Following the contract award, the OIP Portal allows external users to submit contract/data deliverables (e.g., test plans, monthly reports, test results, technical reports, invoices). These deliverables are required per SBIR contract requirements and are provided by external users and may contain private sector proprietary information.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

The OIP Portal is not used to perform data or data pattern analysis, nor does it provide the functionality to perform data or data pattern analysis.

3.3 Are there other components with assigned roles and responsibilities within the system?

External users, or offerors, are users from industry who have the ability to submit proposals to solicitations posted by OIP. Internal users include S&T and contractor staff, as well as military personnel and employees from other federal agencies.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk OIP Portal data may be used for purposes beyond its original collection.

Mitigation: This risk is mitigated. Potential misuse of OIP Portal data is mitigated through management, operational, and technical controls. Role-based training for internal users is provided and includes awareness on proper handling of PII and source selection and intellectual property data rights. OIP conducts training throughout the implementation of the OIP programs. Additionally, program-specific training may be implemented as well. For every round of Broad Agency Announcements and Small Business Innovation Research evaluations, internal portal users receive this training. Training is also provided for BAA portal users annually. Further, all users are required to review and acknowledge Rules of Behavior, and NDAs are required for contractor support users prior to access to the system. Lastly, all new S&T workforce members receive introductory privacy and security training at orientation.

OIP also conducts routine reviews and audits to verify the integrity of the data included in

the portal. All activities executed by users with administrative privileges are audited and logged by the system and monitored by S&T personnel.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

External users are provided notice of the information collected by the OIP Portal as part of the registration and proposal submission process via a DHS Privacy Notice on the portal webpage. Internal users are provided notice of the information collected by the OIP Portal as part of the registration and use of the portal via a Privacy Act Statement on the portal webpage or user account request form. This PIA also provides a measure of notice.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Information used by the OIP Portal is collected directly from external users who provide this information voluntarily. External users have the right to decline to provide the information during the account creation and submission processes. External users may decline to share their personal information, but doing so may prevent their ability to contract for services with S&T.

Internal users provide information for account creation and proposal evaluations as part of their job responsibilities. Internal users may decline to share their personal information, however doing so may delay or prevent them from accessing the OIP Portal, reviewing submitted proposals, and providing evaluations.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals do not have notice of how their information will be used.

Mitigation: This risk is mitigated. Publication of this PIA as well as the associated SORNs provide general notice. Users of the OIP Portal are presented with a DHS Privacy Notice or Privacy Act Statement describing how their information will be used as part of the registration and proposal submission process. The OIP Portal User Guide also provides information to potential users regarding the account creation and submission process.

Section 5.0 Data Retention by the Project

5.1 Explain how long and for what reason the information is retained.

The OIP Portal maintains a repository of all proposals and awards as a part of overall data

management and retains this information for data calls and reporting. All information will be retained throughout the system's lifecycle to document the intellectual property. In order to record potential intellectual property rights, documents included in and resulting from the use of the OIP Portal are designated as permanent records and will be retained indefinitely.

OIP retains user account data in accordance with DHS records schedules. Data regarding each user are stored for administrative functionality throughout the system's lifecycle. Additionally, data regarding the company and company point of contact are stored for functionality for the lifecycle of OIP-administered programs. Accounts can be made inactive by internal administrators but cannot be deleted as these accounts need to be retained for records management purposes.

OIP must retain data developed under contract for transparency purposes. For SBIR, the contract awardee has certain rights in its proposal and obtains other rights in the work it performs under contract for the government. For other efforts, the data rights may be negotiated or subject to other regulations. Retention of proposal information via the OIP Portal aids in differentiating between the offeror's proposal (e.g., background information) in comparison to data first produced under contract (e.g., foreground information). The OIP Portal's ability to document this information provides additional transparency and ensures SBIR data is protected for the proper duration.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk data will be retained for longer than necessary for the purpose of collection.

Mitigation: This risk is mitigated. Data is retained and disposed of in accordance with the S&T Records Inventory/File Plan for OIP Portal System. In order to record potential intellectual property rights for the government and small business, records included in and resulting from the use of the OIP Portal are designated as permanent records. OIP conducts routine reviews and audits to verify the integrity of the data included in the portal.

User accounts are automatically deactivated when they have been inactive for 60 days with no successful account logins. External users receive a notice via email that their account will be automatically deactivated due to inactivity. The notice will be sent seven days and then again three days prior to deactivation. The external user will also receive a notice the day of deactivation.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Per DHS Policy Directive 262-05, Information Sharing and Safeguarding,[12] information submitted during the proposal submission process may be shared with any of the DHS Operational Components. Per the SBA SBIR and STTR Program Policy Directive,[13] information submitted during the proposal submission process may also be shared with the Department of Defense or other federal agencies. SBIR does not provide DHS sensitive information to private sector awardees.

DHS government staff and subject matter experts from other federal agencies may be granted access to the appropriate solicitation application(s) within the OIP Portal and their assigned topics after verification from Topic Managers confirming these individuals as the intended proposal Reviewers. Reviewers have access to view the materials submitted by applicants in response to the publicized topics and provide detailed evaluations through the application.

Reviewers only have access to the information submitted for the topics to which they are assigned. Additionally, all internal users must review and acknowledge Rules of Behavior, ensuring that they actively participate in a successful program for information security, and NDAs are required for contract support users for access to the system.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The OIP Portal's sharing of information it collects is consistent with Routine Use F of the DHS/ALL-004 General Information Technology Access Account Records System SORN, which permits sharing with contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

The OIP Portal's information sharing is consistent with Routine Use F of the DHS&T-001 Research, Development, Test, and Evaluation Records, which permits sharing with contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records.

The OIP Portal's information sharing is consistent with Routine Use F of the DHS/ALL-002 Mailing and Other Lists, which permits sharing with contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related

[12] *Available at* https://www.dhs.gov/publication/information-and-technology-management.
[13] *Available at* https://www.sbir.govites/default/filesBIR-STTR_Policy_Directive_2019.pdf.

to this system of records.

6.3 Does the project place limitations on re-dissemination?

External users' access is restricted so that they can only access, view, and download their own previously uploaded documents and other information in the OIP Portal that is made available to all users.

Internal users' access is restricted via the limitations placed on their role in the portal. Reviewers only have access to the information submitted for the topics to which they are assigned. Additionally, all internal users are required to review and acknowledge the Rules of Behavior, ensuring that they actively participate in a successful program for information security, and NDAs are required for contract support users for access to the system.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

The OIP Program Office will control disclosures by developing a Terms of Service to provide data handling guides developed for the use, disclosure, and disposition of data related to OIP Portal activities.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk information shared with other DHS Operational Components may be used beyond the original purpose of its collection.

Mitigation: This risk is mitigated. The OIP Portal mitigates any risks related to re-dissemination by requiring contract support users to sign NDAs prior to accessing the system. Information shared with DHS Operational Components is limited via user access restrictions. Additionally, S&T adheres to DHS Directive 262-05, Information Sharing and Safeguarding. DHS has set policy and requirements for Information Sharing and Safeguarding for internal and external use cases, which minimizes the risk of improper sharing. SBIR does not provide DHS sensitive information to the private sector awardees.

DHS Components may share DHS sensitive information with contract awardees, if appropriate. This DHS sensitive information would not be shared through the portal. Per DHS policy, information sharing agreements will be put in place between DHS Components and contract awardees before any sensitive information is appropriately accessed. Contract awardees that will have access to DHS sensitive information will go through the DHS suitability process and will receive appropriate training prior to accessing any DHS sensitive information.

Privacy Risk: There is a risk information may be shared with and used by other federal agencies beyond the original purpose of its collection.

Mitigation: This risk is mitigated. Information shared with external federal agencies is limited via user access restrictions. Additionally, any information sharing with other federal agencies will be conducted in accordance with the SBA Small Business Innovation Research and Small Business Technology Transfer Program Policy Directive. OIP cannot divulge any information included in or resulting from the use of the OIP Portal relating to solicitation proposal submissions or awards outside of the federal government due to intellectual property rights held by the government and small business.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

External users can view their own submitted proposals at any time. For internal users, OIP Portal access is based on roles providing access to specific areas of the portal. Assignment is made based on least required privilege, meaning internal users are not granted roles for functionality or access they do not require.

If a user seeks to access their limited information in the OIP Portal, they may contact the dedicated OIP Portal help desk which provides support to both internal and external users.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

External OIP Portal users may correct inaccurate or erroneous information in their OIP Portal user profile by contacting dedicated OIP Portal help desk support. Internal S&T users are able to correct inaccurate or erroneous external user account information themselves directly in the portal.

Additionally, any individual who may desire to access or correct their information may do so by submitting a Privacy Act or Freedom of Information Act (FOIA) request to the DHS FOIA Office at https://foiarequest.dhs.gov/ or by mail to:

Privacy Office, Mail Stop 0655
U.S. Department of Homeland Security
2707 Martin Luther King Jr. Avenue, SE
Washington, D.C. 20528-065

7.3 How does the project notify individuals about the procedures for correcting their information?

An OIP Portal User Guide is available for external users. The User Guide explains the account creation and proposal submission processes, as well as how to contact the help desk

regarding incorrect information included in the portal. This PIA also provides notice as do the general training users are required to take.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk an individual may be unaware of how the system provides for redress, including access and correction.

Mitigation: This risk is mitigated. An OIP Portal User Guide is available for external users to explain the proposal submission process, how users are able to view their own submissions and information, and how to contact the help desk for support. There is dedicated OIP Portal help desk support, which can be accessed by phone at (571) 446-4869. For internal users, there is a process for users to be redirected to internal OIP support to access and/or correct inaccurate or erroneous information in the portal. Internal users can contact the SBIR office by email at stsbir.program@hq.dhs.gov or by phone at (202) 254-7000. Additionally, the provisions of the Privacy Act and FOIA are available to individuals, as described above.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

S&T ensures that practices stated in this PIA comply with federal, DHS, and S&T policies and procedures, including SOPs, orientation, and training; ROBs; and auditing and accountability procedures. Audit and accountability policies and procedures are documented and maintained to ensure that risks, vulnerabilities, and threats are properly identified, analyzed, and documented, and that significant risks are managed. The OIP Portal adheres to the DHS security access control policies contained in DHS 4300A Sensitive Systems Policy Handbook and NIST Special Publication 800-53,[14] that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The system is scanned weekly for security vulnerabilities.

S&T employs technical and security controls to preserve the confidentiality, integrity, and availability of the data, which are validated during the security authorization process. These technical and security controls limit access to authorized users and mitigate privacy risks associated with unauthorized access and disclosure to non-authorized users. Further, DHS established and maintains an audit and accountability control policy in accordance with the requirements of the Federal Information Security Management Act (FISMA). All activities executed by users with administrative privileges are audited and logged by the system. Audit logs

[14] *See* NIST Special Publ. 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations (September 2020), *available at* https://csrc.nist.gov/publications/detailp/800-53/rev-5/final.

are checked daily by S&T. All S&T systems employ auditing measures and technical safeguards to prevent the misuse of data.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

Role-based training for internal users is provided and contains awareness on PII handling and source selection and intellectual property data rights. All internal users are required to review and acknowledge the Rules of Behavior, and NDAs are required for contract support users for access to the system. All new S&T workforce members receive introductory privacy and security training at orientation. Additional project-specific training may be required.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

As a part of the internal and external user authentication process, in accordance with DHS 4300A Sensitive Systems Policy Handbook, users will submit a request to DHS OCIO. OCIO will collect PII as a means to grant privileged and general users' access to the OIP Portal. Currently, the OCIO primarily uses usernames and passwords to regulate system authentication for the user community. The future state of the system will validate users by using single sign-on (SSO) smart cards, which will include Public Key Infrastructure (PKI), for internal users. A combination of passwords/pins and level 4 authentication will be required for military personnel in other federal agencies. Only federal employees have access to the internal portal using their government email address (.gov or .mil.) This process enables DHS to ensure that users of the OIP Portal have the access and privileges they need to perform their official duties and/or be responsive to posted solicitations. In addition, this will allow enhanced control of and access to PII used in the OIP Portal security environment.

For internal users, the OIP Portal has a user interface design that includes a user-tailorable dashboard with assigned roles and projects. Portal accessibility is segregated by User Roles corresponding with appropriate function requirements. Internal users will only have access to the specific solicitation(s) to which they are assigned and have a need-to-know.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Information is shared with DHS Components in accordance with DHS Policy Directive 262-05, Information Sharing and Safeguarding, and with other federal agencies in accordance with the SBA SBIR and STTR Program Policy Directive. Information collected by the OIP Portal

during the proposal submission process is only shared with DHS government staff and subject matter experts from other federal agencies on a topic-specific basis and is not subject to an MOU. Should this change, any MOUs would be reviewed by the program manager, component Privacy Officer, and counsel and then sent to DHS for formal review.

At this time, information is passed to OPO at the request of the contracting officer. In the future, the OIP Portal may allow for role-based access for the contracting officer to access solicitation information directly within the portal. This access would be limited to the information submitted for the topics to which the contracting officer is assigned.

8.5 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk: There is a risk that DHS will not have an appropriate accounting or auditing capability of privacy-sensitive information maintained.

Mitigation: This risk is mitigated. DHS established and maintains an audit and accountability control policy in accordance with the requirements of FISMA. S&T adheres to the audit and accountability control policy and associated security controls outlined in DHS 4300A Sensitive Systems Handbook. The policy addresses the purpose, scope, roles, responsibilities, and procedures to implement and comply with the DHS audit and accountability control policies. The System Security Plan also addresses how DHS conducts regular reviews on how data is maintained.

Contact Official

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

Responsible Official

Dusty Lang
Director, SBIR Programs
Office of Innovation and Collaboration
DHS Science and Technology Directorate

Approval Signature

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

_____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717