Privacy Impact Assessment
for the

Science & Technology Analytical Tracking System (STATS)

DHS/S&T/PIA-032

July 30, 2018

Contact Point
Ashley Stephenson
Department of Homeland Security
Science and Technology Directorate Finance and Budget Division
202-254-5352

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Finance and Budget Division (FBD) supports S&T by efficiently managing S&T's financial resources. The Science & Technology Analytical Tracking System (STATS) is used by FBD for financial, procurement, and acquisition tracking information. STATS provides transparency on S&T project data, and is primarily used to provide Congress and DHS leadership with accurate and timely responses to questions and requests for information contained in STATS. This Privacy Impact Assessment (PIA) identifies FBD's uses of personally identifiable information (PII) in STATS and steps taken by FBD to protect that information.

Overview

FBD's mission is to provide information to authorized DHS S&T staff of S&T project data and to ensure that Congress and other interested parties receive accurate and timely responses to questions and requests for information. STATS is a scalable information technology (IT) system that can deliver accurate and timely information efficiently. Functionalities of the system for minimum viable project (MVP) release on August 1, 2018 are listed below. Using an agile development approach, additional requirements that need STATS to collect PII such as Human Resources (HR) data fields will be implemented over time and will be the basis for amendments to this PIA.

The initial release of STATS will store and maintain program and financial information regarding DHS S&T projects, together with consolidated budget execution information and staffing positions, in one location. The system assists in developing workforce plans, facilities plans, and acquisition plans. STATS also tracks and monitors invoices.

The system is hosted in a DHS facility, connected to an existing, Sensitive But Unclassified DHS network and is available to authorized users through a web-based interface on the DHS network.

STATS collects information related to DHS S&T projects, federal employees, and contractors who support the DHS S&T Directorate. STATS will be capable of tracking and reporting the full budget life cycle, including commitments (procurement requisition activity and workflow); obligations (awards, travel, and purchase card (P-card) activities); and expenditures (all payment transactions) by project, program, and entity-level. STATS will also include a project tracker, electronic procurement request workflow tool, staff management tools, workforce management tools, data analytics, a document repository, and dashboards for staff at all levels of the organization from program managers to the Under Secretary for Science and Technology. Dashboard requirements have not been defined. However, STATS' dashboards will include only information residing in STATS and will not connect to other systems to provide dashboard data.

This PIA will be updated as new STATS functionalities requiring collection of PII is developed and implemented.

STATS will be used to support responses to congressional oversight activities, reporting requirements, and the day-to-day operations of project/program managers. Information in the application database may be manually entered by authorized STATS users from approved DHS/S&T collection instruments or imported from current S&T data sources. The current data source(s) for STATS are discussed in the section 2.2 of this PIA.

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?

Data in STATS is obtained from existing systems used by S&T, noted in section 2.2 of this PIA. Authority for STATS to receive data from these systems is established under the FY 2015 S&T appropriations legislation, through which the House of Representatives, in its Report, directed "S&T to develop a method or system for tracking all S&T-funded projects not later than 90 days after the date of enactment of this Act. Information on each project should include: a unique project number, project name, project description, name of project manager, capability gap addressed, project performer(s), estimated return on investment, and transition success. The Under Secretary is directed to brief the Committee on progress made on this tracking system not later than 60 days after the date of enactment of this Act."[1]

No personal information beyond program and project manager name, work email address, work telephone number, and account user information is being collected by STATS. This system serves as S&T's central repository and tracking tool for reporting to capture this information in a standardized format for internal S&T use and for preparing congressional reports.

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

STATS does not retrieve an individual's PII by the individual's name or other unique personal identifier and is not a system of records. Therefore, a SORN is not required for STATS.

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

A new system security plan has been implemented as a requirement for the Authority to Operate (ATO) package, which is expected to launch August 1, 2018.

[1] House of Representatives Report H.R. 113-481 on the Department of Homeland Security Appropriations Act, 2015, Public Law 113-481 (June 19. 2014), at page 115.

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

Yes. Records in STATS are retained under the General Records Schedule 1.1, Item 010 promulgated by NARA (Transmittal No. 28, July 2017), Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting.[2] GRS 1.1 requires records be "destroy[ed] 6 years after final payment or cancellation, but longer retention is authorized if required for business use."[3]

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.

STATS is not subject to PRA requirements because it does not collect information directly from the public. Data is entered by STATS users on web forms or is uploaded from feeder systems.

The originating systems from which STATS receives data are in compliance with PRA requirements. Data that pertains to DHS employees and contractors/vendors is not subject to the PRA because the information is not collected directly from the public.

Section 2.0 Characterization of the Information

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

Project/program data collected includes:

- Contracting officer name;
- Project or program manager name, work email address, and work telephone number;
- S&T Contractor Name;
- S&T contractor Point of Contact name;
- Project name;
- Project description;

[2] *See* The General Records Schedule Transmittal 28, *available at* https://www.archives.gov/files/records-mgmt/grs/grs-transmittal-28.pdf.
[3] *Id.*

- Project level milestones;
- Project performer;
- Contract type; and
- Budget information.

This PIA will be updated prior to STATS collecting additional PII or other Sensitive PII (SPII) to support any future releases or new functionalities.

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

Project data entered into the system is entered manually through web forms and uploaded from files from integrated source systems. The source systems currently connected to STATS are:

- Federal Financial Management System (FFMS) - a single integrated application developed by Immigration and Customs Enforcement (ICE) and used by S&T and other DHS components.[4] FFMS captures and records financial data in the General Ledger. FFMS is the official core financial system of record for ICE, S&T, and other DHS components. Systems from which FFMS obtains data includes:
    - The Department of the Treasury's Financial Management System provides limited data to FFMS in connection with its Secure Payment System and its Intra-Governmental Payment and Collection System;[5] and
    - The Government Accountability Office (GAO) Central Contract Registry, which has transitioned to the System for Award Management (SAM) system.[6] In addition to CCR, functionalities transitioned to SAM include Federal Agency Registration (Fedreg), and Online Representations and Certifications Application (ORCA).

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

Data that STATS collects, other than through FFMS or directly from CCR/SAM, is not collected from commercial sources or publicly available data. CCR/SAM users include contracting officials, grant-makers, contractors, and members of the public. CCR/SAM registrants include

[4] *See* DHS/ICE/PIA-026 Federal Financial Management System, *available at* www.dhs.gov/privacy.
[5] *See* Secure Payment system (SPS) PIA, *available at* https://www.fiscal.treasury.gov/fsreports/rpt/fspia/SPS-pia.pdf
[6] *See* GSA PIA for System for Award Management (SAM), *available at* https://app_gsagov_prod_rdcgwaajp7wr.s3.amazonaws.com/privacyimpactSAM.docx.

those doing business with the Federal Government, which may include an individual who is doing business with the Federal Government directly or as a sole proprietorship; and grant seekers and grantees.

The CCR/SAM database, which is the source of some data STATS obtains from FFMS, is available for public searching; however, payment technicians have privileged access to CCR in order to gather additional contractor/vendor information in CCR/SAM that is not made available to the public (e.g., DUNS[7] number, TIN[8], or information not made public by the vendor). Payment technicians also use CCR/SAM to verify the contractor/vendor is in good standing with the Federal Government. The contractor/vendor information gathered by the payment technicians is then manually entered into the FFMS vendor table, which is a smaller repository of contractors/vendors that provide services to DHS. This information is used when generating payments for services rendered and transmitting required information to the Treasury for tax purposes (e.g., 1099- INT and 1099-MISC forms).[9] A business' TIN, or any other potential PII derived from FFMS, is not stored in STATS.

2.4 Discuss how accuracy of the data is ensured.

DHS S&T staff will collect, verify, and validate project information collected in the system throughout a project's lifecycle. The owners of the information systems from which STATS obtains data are responsible for ensuring the accuracy of the data in their system(s) that is made available to STATS. Daily validation checks are conducted for imported files. S&T conducts weekly reconciliation against system data and FFMS data to ensure accurate financial data.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: STATS may collect more information than necessary

Mitigation: Agile requirements gathering sessions are used to identify information required to support the STATS mission, which in turn dictates information incorporated into the application. Additionally STATS implements role based security providing users with access only to STATS data and modules for which they have been approved. Creation and manipulation of

[7] DUNS is a unique nine digit identification number assigned to a physical location of a business. The number is assigned by Dun & Bradstreet, Inc. which is a company that provides commercial data, analytics and insights for businesses. DUNS numbers are required to register with US Federal government for contracts or grants. More information about Dun & Bradstreet's privacy policy is *available at* https://www.dnb.com/utility-pages/privacy-policy.html.

[8] TIN is a Taxpayer Identification Number. It is assigned by the IRS to certain organizations such as small businesses. More information *available at* https://www.irs.gov/individuals/international-taxpayers/taxpayer-identification-numbers-tin.

[9] See DHS/ICE PIA-026, Federal Financial Management System (March 23, 2011), *available at* www.dhs.gov/privacy.

data in the STATS database is tracked via auditing functionality.

Privacy Risk: STATS data may be inaccurate, outdated, incomplete or, or irrelevant.

Mitigation: Data quality and integrity are verified through management, operational, and technical controls. S&T includes numerous steps aimed at mitigating the identified risks, such as daily validation checks for imported files. S&T conducts weekly reconciliation against system data and FFMS data to ensure accurate financial data.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

S&T is required by law to provide periodic reports to Congress regarding its project and programs over their life cycles, including project/program manager name. Data collected in STATS provides a current, consolidated database from which the information required in those reports is made available. STATS also brings together in a single database the data necessary to populate its project tracker, procurement work flow tool, staff management tools, data analytic tools, and dashboards for staff at all levels of the organization. The tools and dashboards generated provide for timely fiscal management of S&T appropriations, financial oversight of S&T programs and projects, route program management information, enforce fiscal responsibility in S&T, and provide accurate and timely responses to questions and requests for 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 system does not provide the functionality to perform data or data pattern analysis. It is meant as a data repository and process management tool, rather than a data analytics tool. Users are able to narrow datasets based on search parameters; however, no facility for intelligent analysis is provided.

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

No other DHS components are assigned roles or responsibilities within the system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: STATS data may be used for purposes beyond its original collection.

Mitigation: Potential misuse of STATS data is mitigated through management, operational, and technical controls. S&T has taken several steps aimed at mitigating the identified

risks. STATS users are instructed as to the appropriate use and protection of information through annual privacy and security awareness training, and specific system user training. Clear operating instructions for users and administrators are documented and available to all users of STATS. Individuals are required to sign Rules of Behavior, and a Non-Disclosure Agreement and obtain their supervisor's approval to gain access to STATS. A privacy policy and security statement is presented to the users on the STATS login screen reminding them of proper uses of the system. Finally, STATS has robust audit logs that are checked weekly by the designated Information System Security Officer.

STATS employs audit capabilities on critical system data such as user information, program information, and project information based on user requirements. Audit tables are created for the system to track any addition or update to specified information as well as any deletion of information. In addition to tracking the data itself the schemas will track common audit attributes such as the user initiating the data change, date, and time. For updates the schema will track old vs. new values. STATS is able to create scheduled reports against this information and authorized users will be able generate ad hoc queries against the audit schemas as necessary. Any unauthorized or inappropriate changes to information can be quickly recognized and corrected by authorized users.

Privacy Risk: STATS data may be accessed or used by unauthorized persons.

Mitigation: The risk of unauthorized access to information is mitigated through management, operational, and technical controls. S&T has taken several steps aimed at mitigating the identified risks. Role based access controls are implemented throughout STATS, providing access to only the specific data required by individuals to perform their respective job functions. Boundary protection devices (firewalls) will be used to prevent unauthorized access to the DHS network and the system. Intrusion detection capabilities will be installed at the network level to detect system and network anomalies. Transport Layer Security (TLS) 1.1/1.2 encryption to securely transmit data between the user's web browser and the servers to mitigate risk of data compromise while in transit.

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.

Small amounts of data regarding each user are stored for administrative functionality including name (first, last, middle), work phone number, and work email address. Vendors and grantees are provided notice of the information by the STATS source information systems at the time those systems collected PII.

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 STATS was collected directly from individuals with their consent. Individuals have the right to decline to provide the information during the contracting process. Information collected, used, or shared is required by statute or regulation. Individuals may decline to share their personal information, but doing so may prevent contracting with S&T.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: An individual may be unaware that his or her information is being used by STATS for tracking and reporting purposes.

Mitigation: The risk is mitigated by the publishing of this PIA, and strong policies requiring notice at the time of collection for the source systems from which STATS collects information. Notice of STATS's use of the information is provided in the source system SORNs.

Section 5.0 Data Retention by the project

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

Project information is tracked throughout the system's lifecycle and retained for data calls and reporting. Records in STATS will be retained under GRS 1.1, Item 010 (Transmittal No. 28, July 2017), which provides for "destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use."

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: Data will be retained for longer than necessary, increasing other privacy risks over the life of the system.

Mitigation: The risk is mitigated through the encryption of PII data at rest in the database to guard against unauthorized access. STATS will be enhanced in future STATS releases to ensure destruction of project data in compliance with NARA GRS 1.1, Item 010 (Transmittal No. 28, July 2017). Pending development of automated processes within STATS to assure timely data destruction, manual processes will be defined and enforced to ensure all records retention schedules are enforced. In addition, audit procedures will be implemented to ensure appropriate data destruction is undertaken.

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.

Information in STATS is shared with Congress in congressional reports. The information shared consists of:

- Unique Program/Project Number
- Program/Project Name
- Program/Project Description
- Program/Project Manager's Name[10]
- Capability Gap
- Program/Project Performer(s)[11]
- Estimated Return on Investment
- Transition Success

This information will be displayed separately and not be connected to any additional data. STATs will not share PII, other than program manager name, with external organizations.

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

STATS is currently not a system of records. The Privacy Act, however, does permit agencies to share data that may be sourced from a SORN with Congress.[12]

6.3 Does the project place limitations on re-dissemination?

There are no limitations on Congress re-disseminating STATS data. All other STATS uses are limited to DHS S&T and follow DHS S&T re-dessimination limitations and requirements.

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

STATS maintains audit trails of information provided to Congress. No Sensitive PII is disclosed to Congress.

---

[10] House of Representatives Report H.R. 113-481 on the Department of Homeland Security Appropriations Act, 2015, Public Law 113-481 (June 19. 2014), at page 115.
[11] Program/Project Performer(s) are the entity or organization contracting with DHS S&T.
[12] *See* 5 U.S.C. 552a(b)(a)

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: Information shared with Congress may be used beyond the original purpose of its collection.

Mitigation: This risk is partially mitigated. STATS mitigates any risks related to re-dissemination by ensuring that the only PII provided to Congress is the program/project manager name, which was a data element required by Congress. However, once a disclosure has been made outside the executive branch, S&T cannot place limits on congressional uses of that information.

Section 7.0 Redress

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

STATS user access is based on roles providing access to specific areas of the application. Assignment is made based on least required privilege, meaning users are not granted roles for functionality or access they do not require. If a contractor seeks to access his or her limited information in STATS, he or she may contact the STATS Help Desk. STATS users and contractors may also contact the owners of systems from which STATS obtains their information for access.

At this time, STATS is not a system of records under the Privacy Act of 1974, as amended (Privacy Act). However, individuals may request access to information about them that may have been retained in STATS pursuant to the applicable provisions of the Freedom of Information Act (FOIA). An Individual may submit a FOIA request to S&T by mail to the S&T FOIA Coordinator, Mail Stop: 0210, Department of Homeland Security, 245 Murray Lane, SW, Washington, DC 20528

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

STATS users may correct inaccurate or erroneous information in their STATS user profile by contacting the STATS user Help Desk. Program and Project Offices are able to correct inaccurate or erroneous program/project manager names, work email addresses, and work telephone numbers in STATS or in systems from which STATS data is collected.

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

The S&T Office of Security explains the process of correcting information in STATS to new hires and contractors during S&T on-boarding activities. Notice is also provided through this PIA.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: STATS may not afford an individual opportunity to access or correct information transferred or stored by STATS

Mitigation: At this time, STATS is not a system of records under the Privacy Act. To the extent an individual seeks redress, the individual must pursue that redress either through the STATS help desk or in accordance with the redress provisions applicable to the information system from which his or her information was provided to STATS. Individuals who wish to access their information may also write to the S&T FOIA Coordinator, Mail Stop: 0210, Department of Homeland Security, 245 Murray Lane, SW, Washington, DC 20528

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?

Audit and accountability policies and procedures are documented and maintained to ensure that risks, vulnerabilities, and threats are properly identified; analyzed, documented, and significant risks are adequately managed. STATS adheres to the DHS security access control policies contained in DHS Sensitive Systems Policy Handbook 4300A, that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.[13] The system is scanned for vulnerabilities twice a week, and a Security Information and Event Management (SIEM) tool is used to continuously monitor audit logs.

The policies and procedures encompass user activity during the operational and maintenance phase of the system.

Audit trails for a variety of system-related events and activities are logged to allow the system administrator and system information system security officer (ISSO) to check for associated security issues. The items recorded provide an accurate representation of the actions taking place, the user or host responsible for initiating the action, as well as the date and time.

[13] *See* Section 5.3, DHS Sensitive Systems Policy Handbook 4300A *available at* https://www.dhs.gov/sites/default/files/publications/4300A%20Sensitive-Systems-Handbook-v12_0-508Cs.pdf.

Additionally the level of user activity logging is tailored to the needs of the system, with specific focus upon the Program Management and Reviewer users, who have access to sensitive information. Each time an attempt is made to login to the system with an invalid username, the system logs the username, date/time, and IP address of the computer trying to gain access. Additionally, after three unsuccessful access attempts a user's access is locked until the situation can be reviewed and remediated by an appropriate system administrator. These logs are reviewed weekly by the ISSO to determine the appropriate course of action. The audit facility logs insert, update, and delete operations to the system log file and to the database audit tables including identification of: DHSNET username (associated with user session), date/time, database table, database operation performed, and specific content modified.

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

Privacy training is provided during STATS user training, prior to providing access to the system. All S&T staff receive training regarding appropriate use and management of personal information. All new S&T workforce members receive introductory privacy and security training at orientation.

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

Documented policy and procedures will be in place for approving access to users for personnel information, at the direction of the Chief of Staff, DHS S&T. The users of this system who have access to personal information are: the S&T Office Directors/Deputies, S&T Security, S&T Human Capital, and S&T Chief Financial Officer.

The system has pre-determined user access roles based upon the support functions performed by the assigned user. The office director or supervisor will determine a user's need for access to the system. Once determined, the director will submit in writing a request for access to the system to the S&T Chief of Staff. The Chief of Staff will direct the administrator to create the appropriate user account and provide training to the new user.

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?

S&T does not share personnel information outside of DHS. Project information is only shared with Congress 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.

Responsible Officials

Carol Cribbs
Director, Finance and Budget Division
Science and Technology
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security