US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/29/2024

OPDIV:

AHRQ

Name:

Business Operations and Program Support System

PIA Unique Identifier:

P-5154697-313919

The subject of this PIA is which of the following?

General Support System (GSS)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

Yes

Identify the operator.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

The system received it's ATO 11/13/21.

Describe the purpose of the system.

The Business Operations and Program Support System (BOSS) is a General Support System (GSS) that supports agency operations related to the following areas: planning and analysis, funding and tracking, reporting and dissemination, enterprise data management, and back office support. The BOSS acts as an agency wide unified enterprise system that is comprised of a collection of custom developed modules built to support the entire life cycle of an agency intramural or extramural research project. This starts with concept planning and the development of a funding recommendation memorandum which describes the overall benefit a project to the agency and/or the public health system. At the end of a project, the BOSS provides a mechanism for the general public to search and retrieve abstract information related to grants and contracts funded by the agency as well as any publications related to those projects. The BOSS also provides enhanced

reporting capabilities and data analysis for agency employees and direct contractors.

BOSS provided AHRQ with a means to consolidate system modules supporting agency operations. As part of the agency's efforts to provide outreach and communications, the BOSS provides a module which allows users to order and download agency publications. Users can register to obtain these items or download free items as a guest. The BOSS also contains a module designed to help primary care clinicians identify clinical preventive services that are appropriate for their patients. Clinicians are able to search and browse U.S. Preventive Services Task Force (USPSTF) recommendations on the web, on their PDA or mobile device, or obtain them from the AHRQ Publications Clearinghouse.

The BOSS additionally provides back office and operational management functions to the agency including infrastructure support, correspondence tracking, event planning and registration, and AHRQ's Intranet web site. These modules serve the common goal of supporting AHRQ program activities and communicating information related to AHRQ's mission. The administration of these modules takes place on internal application servers that are only accessible from the AHRQ private network. In coordination with the HHS Office of Information Technology Infrastructure and Operations (ITIO), all internal users (employees and direct contractors) access these modules through Single Sign-On (SSO) access.

Describe the type of information the system will collect, maintain (store), or share.

The BOSS collects, maintains, and stores general information related to AHRQ's intramural and extramural research projects. This includes business contact information for principal investigators and vendors as well as funding information for agency grants, contracts, and inter-agency agreements (IAAs). Business contact related information includes name, address, e-mail, and phone number while funding information includes budget source information, funding amounts, award period dates, and funding evaluation data. The BOSS also collects progress and performance reporting data as a mechanism for communicating project status to agency program officials. This information combined with funding evaluation and award data is used to support ad-hoc reporting and analysis of agency programmatic data.

The BOSS also collects information about agency funded projects and other related programs that are used in outreach and communication efforts to inform constituents about AHRQ's mission. Members of the general public can access this information via a web interface (AHRQ's Project Research Database – PROD) or choose to download or purchase publications related to these efforts through AHRQ's Publications Clearinghouse. USPSTF recommendations data is also available through a searchable web interface (Electronic Preventive Services Selector – ePSS) or via the AHRQ Publications Clearinghouse.

As part of module conversion, the BOSS additionally maintains and uses business contact information (name, position title, office/center, and division) for employees and direct contractors to support back office applications and the agency's Intranet web site. This information is primarily used to track correspondence across agency offices and centers, support Intranet functions, and to assign user accounts to various BOSS modules. Similar information is collected for members of the public who wish to attend conferences, seminars, or workshops sponsored by AHRQ (Conference Management Application - CMA). Information collected from direct contractors and employees that support the system include a username and password as credentials and designated user role to provision access to the system for system maintenance and development.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The BOSS system supports agency operations through the collection, maintenance, and dissemination of data related to intramural and extramural research and programmatic activities. The following information is collected in support of these activities:

Planning and Analysis - The BOSS system collects and maintains data to support the budget planning and formulation process: programmatic data (budget source information, outcome goals); budget data (program budget amounts, funding amounts); and funding decision data (funding recommendations).

Funding and Tracking - The BOSS system collects and maintains funding information related to contracts, inter-agency agreements (IAAs), and grants: principal investigator contact information (name, address, e-mail, and organization); funding evaluation data (funding recommendation, abstracts, and peer reviews); funding award data (award period dates, award type, project officer name and e-mail, award amount); and monitoring/oversight data (progress and performance reporting, funding budget, and finance reporting).

Reporting and Dissemination - The BOSS system collects and maintains data to support outreach and communication efforts to the general public: award information (vendor/grantee name, organization name, award identification number, award title, abstracts/scope, amount, and vendor state); publications order information (name, phone, e-mail address, mailing address); and USPSTF recommendations content and meta-data.

Enterprise Data Management - The BOSS system collects and maintains data to manage and maintain system modules: data analytics (web logs); short/long term data backups (backup logs); and software development artifacts (configuration management procedures and documents, and system source code).

Back Office Support - This module was consolidated into the BOSS system to collect and maintain data to support back office and operational management functions: user credentials (username, password, user role); employee and direct contractor information (employee name, position, title, office/center, and division assignment); correspondence tracking information (control subject, ID, dates, control types, assignments, documents, from name, and to name); and event registration information (name, professional affiliation, organization type, city, zip code, phone number, and e-mail).

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name
E-Mail Address
Mailing Address
Phone Numbers
System administrator and developer username and password and user role as credentials

Principal investigator organization, funding award data
Employee position, employee title, employee office/center and division assignment
Zip code

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees
Public Citizens
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

5,000-9,999

For what primary purpose is the PII used?

The BOSS system primarily uses the PII to support agency operations, communicate with constituents, and to manage, track, and report on agency research projects. The PII is also used to contact business partners and to provision account access for AHRQ employees and direct contractors to BOSS system modules.

Describe the secondary uses for which the PII will be used.

N/A

Identify legal authorities governing information use and disclosure specific to the system and program.

Section 913 and 306 of the Public Health Service (PHS) Act (42 U.S.C. § 299b-2 and 242k(b)). Sections 924(c) and 308(d) of the PHS Act (42 U.S.C. 299c-3(c) and 242m(d)) provide authority for protecting restrictions on identifiable information about individuals.

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-35-0001 (AHRQ Agency Management Information System/Grants and Contracts)

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within the OPDIV

Non-Government Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

OMB No. 0935-0122, Exp. Date 07/31/2026

Is the PII shared with other organizations?

No

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Principal investigators, research training grant program directors, and research fellowship recipients; peer and other special reviewers; grant and contract project directors and other key personnel are notified that their personal information will be collected at the time in which a funding application is created. Members of the general public are asked to provide contact information when they request to register for an event, conference, or workshop and when they request items from the AHRQ Publications Clearinghouse. In these scenarios, the collection of personal information is required as these functions rely on AHRQ's ability to contact these individuals with the information they provide.

AHRQ employees and direct contractors provide information for the purpose of gaining access to the system to maintain and develop BOSS modules. Employees and contractors are informed that they must provide PII in order to be provisioned an account.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

Individuals may opt-out of the collection or use of their PII by contacting AHRQ's Grants Management Officer or Contract Management Officer and stating the corrective action sought and the reason(s) for requesting the correction or elimination of their PII. All other individuals may request to opt-out by submitting a request to the support mailboxes provided for each BOSS module.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

There is no process to obtain consent for major changes to the system such as data use, as no major changes are anticipated after the initial consent is provided.

AHRQ employees and direct contractors are notified of the purpose of the collection of user credentials at the time of collection, and these individuals are aware of the requirement to collect this information to provision system access.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

An individual may contact AHRQ's Grants Management Officer, Contracts Management Officer, or system manager and reasonably identify the record, specify the information being contested, and state the corrective action sought and reason(s) for requesting the correction, along with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

Periodic reviews of PII contained in the system occur during annual reviews of the BOSS System Security Plan (SSP) and through the generation of comparison reports in other related HHS systems (National Institutes of Health (NIH) IMPAC-II grants system and the Program Support Center (PSC) PRISM contracts database). AHRQ employees and direct contractors provide credentialing information for system account provisioning. The information used to log into the system must be correct for account access, or corrected to gain access onto the system.

Identify who will have access to the PII in the system and the reason why they require access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Business and functional requirements dictate who may access PII, and access is provided on a "least privilege" basis such that only AHRQ employees, direct contractors, and users that need access to PII receive it.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Permissions are limited through the use of system roles that were identified during the requirements gathering phase of the project. The system roles only allow access to a minimum amount of information necessary for system administrators to adequately perform their job.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

All AHRQ employees and direct contractors that support the system must complete the AHRQ Information Technology Security and Privacy Annual Training.

Describe training system users receive (above and beyond general security and privacy awareness training).

Individuals with significant security responsibilities take additional role-based training provided by AHRQ's Division of Information Technology (DIT).

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

Grant and cooperative agreement program management records and case files are handled in accordance with National Archives and Records Administration General Records Schedules 1.2. Program management records are considered temporary records and are destroyed 3 years after final action is taken on the file, but longer retention is authorized if required for business use. Case files are also considered temporary records and are destroyed 10 years after final action is taken on file, but longer retention is authorized if required for business use.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

The BOSS is a GSS that hosts and provides system functionality, including administrative, technical, and physical security controls, for the information that is collected by the modules that comprise the BOSS. Access to the BOSS is protected using two-factor authentication through the use of personal identity verification (PIV) cards which are required for system access.

Administrative, technical, and physical security controls required for the system are defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 4, "Security and Privacy Controls for Federal Information Systems and Organizations." These controls strengthen the information systems and the environment in which it operates, and are reviewed on an annual basis.

Physical controls include the use of locked cabinets to store server hardware which are housed in an access-controlled, secure data center and 24x7 on-site professional security staff to monitor access points and make regular rounds of physical security inspections.

Identify the publicly-available URL:

ahrqastest1.ahrq.gov
arrs.ahrq.gov
arrstest.ahrq.gov
cma.ahrq.gov
cmatest.ahrq.gov
docs.ahrq.gov
docstest.ahrq.gov
eft.ahrq.gov
efti.ahrq.gov
epc-src.ahrq.gov
epss.ahrq.gov
epssdata.ahrq.gov
epsstest.ahrq.gov
grs.ahrq.gov

netlinx1.ahrq.gov
origin-archive.ahrq.gov
pcornomination.ahrq.gov
pcornominationtest.ahrq.gov
prod.ahrq.gov
prodtest.ahrq.gov
survey.ahrq.gov
surveytest.ahrq.gov
uspstfnominations.ahrq.gov
uspstfnominationstest.ahrq.gov
uspstftest.ahrq.gov
view.ahrq.gov
view2.ahrq.gov
Note: web address is a hyperlink.

Does the website have a posted privacy notice?
Yes

Is the privacy policy available in a machine-readable format?
Yes

Does the website use web measurement and customization technology?
Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Does the website have any information or pages directed at children uner the age of thirteen?
No

Does the website contain links to non- federal government websites external to HHS?
No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?
null