US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/14/2016

OPDIV:

OS

Name:

Strategic Planning System

PIA Unique Identifier:

P-2868050-338382

The subject of this PIA is which of the following?

Minor Application (child)

Identify the Enterprise Performance Lifecycle Phase of the system.

Implementation

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?

No

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

No

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

Describe the purpose of the system.

The Strategic Planning System (SPS) provides HHS senior leadership the capability to track progress on strategic plans, provide flexibly with varying workgroup structures, timelines and mandates, enhances the current planning and reporting process to make it simpler and less time-consuming, increases opportunity for coordination of effort to reduce duplication, and informs leadership about high-visibility plans on an ongoing basis. Each step in the sequence of strategic planning is tracked and tied to varying Administrator, Plan Owner, and Plan Contributor based on their roles and set permissions. Plans are maintained and stored on the SPS website.

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

Office of the Assistant Secretary for Planning and Evaluation’s Strategic Planning System (ASPE SPS): The specific PII data elements we collect are as follows:

--HHS staff (primary users): Name, work email address, work phone number
--Non-HHS federal staff (secondary users): Name, work email address, work phone number

--Contractor emails addresses for the purpose of gaining administrative and development access to the SPS system. NOTE: Contractors are not direct contractors.

The above information (about staff) is kept for as long as the account is active; if the staff above change positions or no longer have a role requiring their access to the Strategic Planning System, their account is deleted. We refer to these staff as "accountholders." Currently there are about 500 accountholders in the SPS. These staff are responsible for implementing at least one of the Department's 150 strategic
plans.

The Strategic Planning System collects and stores strategic plan information, including information about implementation of strategic plans. This includes content included in publicly available strategic plans, such as the plan title, the years that the plan is active, a short description of the plan, goals, objectives, and strategies. The system also collects information on plan implementation, such as action steps, specific method of action, which HHS Strategic Plan objective the action step best aligns with, the agency responsible for implementing the action, performance measures (including baselines, targets, and data sources), progress reports, dates of progress reports, individuals responsible for the reports, barriers to progress, solutions to address barriers, and additional notes.

The above information (about plans) is kept until the plan information is updated or completed. For example, if a plan is entered into the SPS for the period 2010-2015, the plan will be archived in 2015. If someone enters a goal of a plan into the SPS, and then updates the goal a week later, the original goal language will be overwritten. An accountholder may send a request to the administrators that content be deleted from the system as well.

The first time a user ("accountholder") accesses the SPS to set up an account, they enter their name, email address, and phone number. The SPS sends them an email to set up a password and associate their account with the Operating Division(OpDiv) or Staff Divisions (StaffDiv) in which they work. User access is not validated by a separate system.

There is no maximum or minimum length of time that information about accountholders or plans will be retained.

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

Overview: The Strategic Planning System is a central resource for HHS staff to report progress on implementation of strategic plans. Approximately 150 strategic plans are included in the SPS. The SPS uses a five tier hierarchy for strategic plans: Goals, Objectives, Strategies, Action Steps, and Progress Reports. The basic components (Goals, Objectives, and Strategies) of plans included in the SPS are available through various other public facing websites; the Strategic Planning System enables reporting of progress on implementation of these strategic plans (Action Steps and Progress Reports). Users use their email and a password to access the SPS. All users can see the basic components (Goals, Objectives, and Strategies) of all plans included in the SPS. Users are able to see Action Steps and Progress Reports, and enter their own unique Progress Reports, only for those strategic plans to which they have been given access. The average user ("Accountholder") has reporting responsibility for 1-2 plans.
Accountholders have restricted access to plans. Each plan has an associated "Workgroup" comprised of staff with one of four roles: Primary Plan Owners, Plan Owners, Action Step Managers, and Progress Reporters. If an accountholder is not a member of the workgroup, they cannot see details of implementation progress (Action Steps and Progress Reports). Primary Plan Owners and Plan Owners have the ability to add people to the Workgroup, and to assign them one of the above roles.

The Strategic Planning System collects and stores strategic plan information, including information about implementation of strategic plans. This includes content included in publicly available strategic plans, such as the plan title, the years that the plan is active, a short description of the plan, goals, objectives, and strategies. The system also collects information on plan implementation, such as action steps, specific method of action, which HHS Strategic Plan objective the action step best aligns with, the agency responsible for implementing the action, performance measures (including baselines, targets, and data sources), progress reports, dates of progress reports, individuals responsible for the reports, barriers to progress, solutions to address barriers, and additional notes.

Information collected by the SPS is for the use of our users ("accountholders"), who can choose to keep it in the system in the long term, archive it, or delete it. It tracks implementation information to ensure progress is being made on plans to support ongoing management of a project; it is not built to be a permanent record of plan implementation.

The specific PII data elements we collect are as follows:

--HHS staff (primary users): Name, work email address, work phone number
--Non-HHS federal staff (secondary users): Name, work email address, work phone number
--Contractor emails addresses for the purpose of gaining administrative and development access to the SPS system. NOTE: Contractors are not direct contractors.

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

Phone Numbers

Usernames

Passwords

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

Employees

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

The email addresses and passwords are used to log into the system as Administrators, Plan Owners, and/or Plan Contributors.

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

Access to the SPS Resource center to look at past webinars, documents, and training materials.

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

5 USC 301, Departmental regulations

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

No

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Other HHS OpDiv

Other Federal Entities

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

N/A

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Within HHS

Users from all agencies within HHS are able to register as system accountholders and see the personal information about other users

Other Federal Agencies

Users from below Federal Agencies are currently in the Strategic Planning System as accountholder:
Office of Personnel Management
Department of Veterans Affairs

A user of the SPS (accountholder) is able to see the following information about other users:

-- If they are responsible for overall implementation of a strategic plan, they have a designation of "Primary Plan Owner" for that plan. If they are responsible for implementing a section of a strategic plan, they are designated as “Action Step Managers.” If they are only responsible for reporting progress on a plan, they have a designation of “Progress Reporter” for that plan. Primary Plan Owners and Plan Owners are able to see the email addresses of anyone who also has access to that plan (because they are responsible for plan implementation). “Progress Reporters” can only see the email addresses for Primary Plan Owners and Plan Owners. So for example, if Bill is a Plan Owner for Strategic Plan A, and Nancy is an Action Step Manager, and Bob is a Progress Reporter for Strategic Plan A, Bill can see a list of workgroup members that will show Nancy and Bob’s names and email addresses; Nancy and Bob can see Bill’s email address.

--A general accountholder (any user of the system, regardless of whether they have access to a plan, can see the email address of the Primary Plan Owner for every plan in the SPS.

Private Sector

Contractors making enhancements to the systems.

Describe any agreements in place that authorizes the information sharing or disclosure.

Below clause regarding Information Sharing Agreement is in all contracts with contractors:

Rights in Data: Restrictive provisions (e.g., prior COR approval) on the contractor’s right to use and disclose data and information obtained through the contract are not to be included, unless very unusual circumstances exist. The default FAR Clause that will apply will be the General Clause FAR 52.227-14.

The Contractor agrees not to release or disclose, verbally or in writing, information pertaining to the results or findings of work (including data collection, analyses, draft or final papers and reports) for the period of this task order without first notifying the COR in writing at least 21 days prior to the release or disclosure. The Contractor must provide notification (minimum 21 days prior to release) and in writing, specifying: who or what is generating the request for advance information; when and how project results/information would be released; and what information would be released.

Describe the procedures for accounting for disclosures.

N/A

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

Federal employees are aware that their names, work email addresses, and work phone numbers are in the system because they are entering this information themselves when they create their accounts.

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.

There is no opt-out feature since the email address and password combination is required to access the system. However, account access can be terminated when sending an email to SPS Administrators.

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

If the ASPE Strategic Planning Team were to determine that disclosure and/or data uses were to change since the notice at the time of the original collection, the ASPE Strategic Planning team would notify the individuals who have accounts about the change in the system via email and would request their consent. If the primary purpose of the system changed , the ASPE Strategic Planning Team would notify the individuals who have accounts about the change in the system and request their consent about different uses of their names, work email addresses, or work phone numbers; however, there are no plans to change the function of the system.

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.

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, is for the accountholder to contact the Help Desk (the link to Help is provided on every page) and request that the issue be addressed. The ASPE Strategic Planning Team would work with the accountholder to correct their information or remove their account from the system if they had concerns.

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

SPS Administrators on an annual basis conducts an audit of all user's registration records to confirm their accuracy, and also removes any inactive user accounts from the system. Additionally, users notify the SPS Administrators of any name or email address changes so that the changes can be updated in the system.

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

Users:

HHS Employees who are members of a plan can view other members' information in order to work together to implement a strategic plan

Administrators:

ASPE employees who administer the system, whose responsibility may include approve, decline, archive plans which contain all members' information.

Developers:

Contractors who make enhancements to the systems will access all elements to a plan, which contains user information

Contractors:

Contractors who make enhancements to the systems will access all elements to a plan, which contains user information

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

At a minimum, anyone with an account can see the work email addresses of people on the system who have a "Plan Owner" role on any plan in the system. This access was granted to support staff using the site to collaborate on plans. For example, if a person is creating a new plan on Global Health, they are able to see plans related to Global Health in the system through the Search feature, and then reach out to the Plan Owners for those plans to collaborate – preventing duplication of effort.

People who have access to a specific plan's details, because they have a role in reporting on that plan's implementation – known as Plan Owners, Action Step Managers, and Progress Reporters – can see the names, work phone numbers, and work email addresses of other people who also report on that strategic plan. For example, the team reporting progress on the National Vaccine Plan can see the names, work phone numbers, and work email addresses of other people on that team. However, the team reporting progress on the National Vaccine Plan would not be able to see the names, work phone numbers, or work email addresses of people working on a different plan, such as the National HIV/AIDS Strategy, except as noted in the paragraph above. This restricted access was built into the system at the request of staff, so that teams implementing plans could collaborate with each other on reporting progress, without involving staff who do not have a reporting role on plan implementation.

Administrators are able to see the names, work phone numbers, and work email addresses of anyone who has an account in the system; this enables them to manage accounts.

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.

A person's role, workflow level and user type is controlled by the system. The controls limit a user's access to only the type and amount of information needed to perform their job duties.

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 HHS employees and contractors are required to complete annual privacy and security training.

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

SPS has a Resource Section that contains detailed user guides, prerecorded webinars, and helpful tools and tips on writing effective Strategic Plans. SPS Administrators frequently provide training using webinars as a format.

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

No

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

The General Records Retention Schedule 4.3, Item 040 applies: Destroy immediately after copying to a record keeping system or otherwise preserving, 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 system is accessed over a Secure Socket Layer (SSL) authentication. The system only contains low level PII such as names and email address. This information is not publicly accessible. All PII is stored in the Relational Database Service (RDS) databases for the SPS hosted Drupal instances. The only access to these databases is from the environment specific application servers. Those application servers additionally can only be logged in to through a Bastian Host that has an IP address Whitelist. The connection to the Bastian Host and system is over Secure Shell (SSH). A person would also have to have an account and the appropriate permissions to access the PII.

Session Cookies that do not collect PII.

Persistent Cookies that do not collect PII.