PTA / PIA: HRSA - SPST - QTR3 - 2025 - HRSA1446282

Created Date: 10/3/2025 12:21 PM Last Updated: 2/26/2026 3:23 PM

General Information

PTA / PIA Name:	HRSA - SPST - QTR3 - 2025 - HRSA1446282	**PTA / PIA ID:**	3887331
Component Name:	HRSA - Security Program Support Tools	**ATO Boundary Name:**	Security Program Support Tools
Overall Status:	Complete	**# of Days - Open:**	230
Submitter:		**Submit Date:**	1/9/2026
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OpDiv:**	HRSA
Security Categorization:	Moderate		
Make PIA available to Public?:	No	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
General 02:	Is this a FISMA-Reportable system?	Yes
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
General 04:	ATO Date or Planned ATO Date.	5/17/2024
General 05:	Is the system or electronic information collection, agency or contractor operated?	Contractor
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Lionel Combet
PTA 01A:	POC Title and Organization	Title - System Owner Organization - HRSA
PTA 01B:	POC Email Address	lcombet@hrsa.gov
PTA 01C:	POC Phone Number	301.443.1583
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)

PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	Some tools are no longer in service while others have been added.
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	The purpose of the system is to: Develop, implement and disseminate security and privacy policies, standards and guidelines in compliance with the Federal Information Security Management Act (FISMA) and other security and privacy initiatives; Devise techniques for cost-effective security measures to safeguard information systems, core IT infrastructure and proprietary information; Ensure that information is stored, collected and shared in accordance with federal regulations and HHS policies; Ensure that all security and privacy documentation and requirements are accurately completed, including system security plans, privacy impact assessments, system of records notices, risk assessments, etc. Ensure incident response and disaster recovery plans are in place to respond to and recover from disruptive and destructive security events; and Educate the community concerning IT risks, vulnerabilities and security protection requirements. The Security Program Support Tools system is a collection of various tools to achieve the objectives listed above. Those tools include: Archer, Cofense, CrowdStrike, Encase, Palo Alto, Splunk, Qualys, Tenable, Coverity, BlackDuck, Cribl, GitLab & CodeDx (SRM). The datasets within each tool are independent of each other. There is not a single database that includes aggregated information. These tools do not maintain their own Privacy Impact Assessment.
PTA 05:	List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.	The Security Program Support Tools will collect and maintain information regarding Security Assessment and Authorization (SA&A) activities, network monitoring, vulnerability assessments, forensics investigations, device ID, training certificate and other security activities. A subset of this data may be shared with other entities (e.g. HHS Computer Security Incident Response Center) on an as-needed basis. Included in that security information is non-sensitive PII (names, work e-mails, phone numbers, work addresses) that will be collected about some points of contact as well as the personnel within the information security program.

PTA 05A:	Are user credentials used to access the system?	Yes
PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card
PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	Information regarding SA&A activities, network monitoring, vulnerability assessments, forensics investigations, and other security activities is collected to support the program's security activities. Non-sensitive PII is collected so Division of Cyber Security and Privacy (DCSP) has necessary points of contact available to support security activities
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	Yes
PTA 08A:	Provide the URL(s).	Archer - https://soc-archws-p01.hrsa.gov/RSAArcher/default.aspx CrowdStrike - https://falcon.laggar.gcw.crowdstrike.com/login Cofense - https://soc-cofenas-p01.hrsa.gov/auth/sign_in Palo Alto - https://soc-panpkas-p01.hrsa.gov/ Palo Alto - https://soc-panstas-p01.hrsa.gov/ BlackDuck - https://hrsa.app.blackduck.com/ Coverity - https://coverity.hrsa.gov/ Qualys - https://qualysguard.qg3.apps.qualys.com/ SRM (CodeDx) - https://codedx.hrsa.gov/ Tenable - https://securitycenter.hrsa.gov/ Splunk CDM - https://soc-spcdmas-p01.hrsa.gov:8000/ Splunk Cloud - https://hrsa.splunkcloudgc.com/ Splunk ES - https://es.hrsa.splunkcloudgc.com/ Splunk IDM - https://idm.hrsa.splunkcloudgc.com/ GitLab - https://soc-glabas-p01.hrsa.gov Cribl - https://cribl.hrsa.gov:9000/login Encase - No URL for the tool (Users RDP into the server)
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	Yes

PTA 09:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	Archer - Internal website that is accessible only to organizational users on HRSA Virtual Private Network (VPN). This is used for Governance and Risk Management and Incident Response Reporting. Encase: Endpoint Investigator is used by HRSA to acquire, analyze, and preserve digital data in a forensically sound manner.EnCase is primarily used by HRSA forensics analysts responsible for collecting and examining evidence during cyber security incidents, internal investigations, and e-discovery requests. The tool is also used to securely store and transfer forensic evidence to law enforcement, attorneys, or authorized requestors. CrowdStrike is used for Endpoint Security (EDR) and Cloud monitoring (CSPM). The authorized users can access it by logging using Multi-Factor Authentication (MFA) on the web via port 443. Cofense - Internal website that is used to investigate and track user reporting of suspicious emails, and perform phishing campaigns Palo Alto - Internal website used for web content filtering and threat inspection firewalls and Panorama management servers. BlackDuck is a Software Composition Analysis (SCA) tool. It has an internal website and it helps manage the security and compliance of open source. Coverity has an internal website and is used as a Static code analysis tool (SAST). Qualys has an internal website and is used as a DAST web application scanner. SRM (CodeDx) - Internal website used for correlating results from various static and dynamic code analysis tools. Tenable - Internal website used for vulnerability management and scanning. Splunk - Internal URL/website for event management. Cribl - An AWS native tool with the same capabilities as Splunk but the main advantage is all the data, analytic and dashboards are already located within AWS. GitLab - GitLab is open source software to collaborate on code. Manage git repositories with fine-grained access controls that keep code secure. Perform code reviews and enhance collaboration with merge requests.
PTA 10:	Does the website have a posted privacy notice?	Yes

PTA 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA 12:	Does the website use web measurement and customization technology?	No
PTA 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Identifying Numbers Device Identifiers Biographical Information Name User Credentials Certificates (e.g., training certificates) Contact Information Email Address (Business) Mailing Address (Business) Phone Numbers (Business)
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	100 – 499
PIA 25:	For what primary purpose is the PII used?	The PII gathered for the Security Program Support Tools is primarily used so that the security program has necessary points of contact available to support security activities. Email addresses are used for user credentials. This allows each user to have a unique login.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	There are no secondary uses of PII.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	5 USC 301, Departmental regulations; The Privacy Act of 1974; The Freedom of Information Act; The Federal Information Security Management Act; The E-Government Act of 2002; or OMB Memorandum M-03-22
PIA 29:	Are records in the system retrieved by one or more PII data elements?	No

PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Email Online Government Sources Within the OPDIV Other HHS OPDIV
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA 31B:	Explain why an OMB information collection approval number is not required.	N/A
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary
PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	Only work contact information is collected and is necessary to support the program's security activities.
PIA 35:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). If they cannot be notified or have their consent obtained, explain why.	When major changes occur to the system, there is no notification to individuals whose PII is in the system as there are no changes to the PII or how it will be used by the system.
PIA 36:	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. If no process exists, explain why not.	Individuals can report any concerns regarding their PII to the security program and the program will then make updates to the PII within the Security Program Support Tools as needed.
PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	The security program is responsible for maintaining PII contained in the system and ensuring it's integrity, availability, accuracy, and relevancy. Information is reviewed, at a minimum, monthly and updated as necessary.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Contractors
PIA 38A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA 38B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Users - Only users with security responsibilities will have access to PII. Users only have access to PII necessary to perform their responsibilities. Administrators - Administrators have access to all data within the tool. Contractors - Direct contractors have security responsibilities to have access to PII. They only have access to PII necessary to perform their responsibilities.

PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	System users only get access to the information, including PII, necessary for performing their responsibilities. User access is determined when they get access to the system and is updated accordingly as their responsibilities change.
PIA 41:	Describe the technical methods in place to allow those with access to PII to access only the minimum amount of information necessary to perform their job.	System users only get access to the information, including PII, necessary for performing their responsibilities. User access is determined when they get access to the system and is updated accordingly as their responsibilities change.
PIA 42:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) to make them aware of their responsibilities for protecting the information being collected and maintained.	All system users are required to take the annual security awareness training. System users with elevated privileges are also required to take role-base security training.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	N/A
PIA 44:	Describe the process and guidelines in place for the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	General Records Schedule (GRS) 3.2. Item 010, Disposition Authority: DAA-GRS-2013-0006-0001. Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.
PIA 45:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	The Security Program Support tools are hosted at the Data Center. The Data Center supports several key applications and is compliant with HHS security guidelines. The physical access to the data center is restricted to only authorized personnel from the Data Center team. So data center physical security controls and processes will protect any stored PII information. The technical architecture will ensure PII data is encrypted at rest. The tool servers are placed behind the firewalls and will be further protected using virtual local area network for restricting communication between the servers. Additionally, PII data is protected through administrative controls by user roles and permissions. Only authorized roles will have access to PII data and will have policies and procedures to grant them necessary access.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	1/22/2026
Privacy Analyst Review Comments:	PTA 4 >> The list of tools provided doesn't match up with the tool URLs listed in PA 8A (where is Cribl and GitLab?) PTA 8A >> Should BurpSuite be listed? PTA 8A & PTA 9 >> the two lists provided don't match up (i.e., PTA 9 does not have Cribl or GitLab	**# of Days - PA Review:**	13

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	2/5/2026
SOP Review Comments:		**# of Days - SOP Review:**	14

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	2/11/2026
Agency Privacy Analyst Review Comments:	Reviewer: Christopher Akhibi 2/11/2026 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	6

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	2/26/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	15

SAOP Signature

Date	User	Type	Name	Original Value	New Value
2/26/2026 12:08 PM	BAUR, VANESSA	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PTA 08A	Data Feed Service, pta_pia_HSRSA_Release	12/17/2025	All the URL's are current and accessible. Verify from your end the cause of the application access blocked by private access policy.	
PTA 08A	Data Feed Service, pta_pia_HSRSA_Release	12/17/2025	All the URL's are current and accessible. Verify from your end the cause of the application access blocked by private access policy.	
PTA 08A	VILLAFUERTE, NESTOR	12/17/2025	All the URL's are current and accessible. Verify from your end the cause of the application access blocked by private access policy.	
PTA 08A	VILLAFUERTE, NESTOR	12/17/2025	All the URL's are current and accessible. Verify from your end the cause of the application access blocked by private access policy.	