06.1 HHS Privacy Impact Assessment (Form) **/ NIH NIEHS GuLF Worker Study System (GWSS)** (Item)

Primavera
ProSight

Form Report, printed by: Minneman, Kim, **Jan 17, 2013**

PIA SUMMARY

1

The following required questions with an asterisk (*) represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget (OMB) and public posting in accordance with OMB Memorandum (M) 03-22.

Note: If a question or its response is not applicable, please answer "N/A" to that question where possible. If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of personally identifiable information (PII). If no PII is contained in the system, please answer questions in the PIA Summary Tab and then promote the PIA to the Senior Official for Privacy who will authorize the PIA. If this system contains PII, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

2 Summary of PIA Required Questions

**Is this a new PIA?*

No

If this is an existing PIA, please provide a reason for revision:

PIA Validation

**1. Date of this Submission:*

Aug 14, 2012

**2. OPDIV Name:*

NIH

**4. Privacy Act System of Records Notice (SORN) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):*

09-25-0200

**5. OMB Information Collection Approval Number:*

OMB Control Number: 0925-0626; ICR Reference Number: 201012-0925-004

**6. Other Identifying Number(s):*

N/A

**7. System Name (Align with system item name):*

NIH NIEHS GuLF Worker Study System (GWSS)

**9. System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:*

Point of Contact Information	
POC Name	David Johndrow

**10. Provide an overview of the system:*

The GuLF Worker Study System (GWSS) is a minor application whose purpose is to support the GuLF STUDY's subject recruitment and data collection efforts. This system will collect data pertaining to participant clean-up-related tasks, demographic and socioeconomic factors, occupational and health histories, psychosocial factors, and physical and mental health. A total of approximately 55,000 persons are expected to be enrolled into the cohort. The GWSS is a secure IT system which consists of commercially available research study software from DatStat (http://www.datstat.com), Microsoft SQL Server 2008 databases, and Avaya Dialer telephone software running on Windows 2008 Rel. 2. The DatStat product, Illume, is the tool used to design, build, test, and manage questionnaires (surveys). Illume is also the tool used for importing and exporting data and managing the data. The DatStat product, Discovery, manages the workflow of the trained personnel who administers computer-assisted telephone interviews (CATI) and computer-assisted personal interviews (CAPI).

**13. Indicate if the system is new or an existing one being modified:*

Existing

**17. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system?*

TIP: If the answer to Question 17 is "No" (indicating the system does not contain PII), only the remaining PIA Summary tab questions need to be completed and submitted. If the system does contain PII, the full PIA must be completed and submitted. (Although note that "Employee systems," – i.e., systems that *collect PII “permitting the physical or online contacting of a specific individual … employed [by] the Federal Government – only need to complete the PIA Summary tab.)*

Yes

17a. Is this a GSS PIA included for C&A purposes only, with no ownership of underlying application data? If the response to Q.17a is Yes, the response to Q.17 should be No and only the PIA Summary must be completed.

No

**19. Are records on the system retrieved by 1 or more PII data elements?*

Yes

**21. Is the system subject to the Privacy Act? (If the response to Q.19 is Yes, the response to Q.21 must be Yes and a SORN number is required for Q.4)*

Yes

**23. If the system shares or discloses PII, please specify with whom and for what purpose(s):*

N/A

**30. Please describe in detail: (1) The information the agency will collect, maintain, or disseminate (clearly state if the information contained in the system ONLY represents federal contact data); (2) Why and for what purpose the agency will use the information; (3) Explicitly indicate whether the information contains PII; and (4) Whether submission of personal information is voluntary or mandatory:*

Collection of this information is authorized under 5 U.S.C. 552a. The primary use of this information is for use in a research study entitled GuLF STUDY: GuLF Long-Term Follow Up Study, sponsored by the National Institute of Environmental Health Sciences (NIEHS). The mission of NIEHS is to reduce the burden of human illness and disability by understanding how environment influences the development and progression of disease. NIEHS pursues this mission through multidisciplinary biomedical research and through communication of research results to regulatory agencies, clinicians, the scientific community, and the general public. The GWSS enables this research.

PII collected as part of this study includes name, address, phone numbers, date of birth, race/ethnicity, social security number, demographic and socioeconomic factors, and medical information. Information is not disclosed to persons outside of the study team, as protected by a Certificate of Confidentiality. Submission of this information is required if a participant wishes to participate in the research study.

**31. Please describe in detail any processes in place to: (1) 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 the original collection); (2) Notify and obtain consent from individuals regarding what PII is being collected from them; and (3) How the information will be used or shared. (Note: Please describe in what format individuals will be given notice of consent [e.g., written notice, electronic notice, etc.]):*

Individuals whose PII is collected undergo an informed consent process with a trained member of the study team. Participants are told that their information is protected through a Certificate of Confidentiality and that it may be placed, in a coded or de-identified format, in a database to be used by other researchers. There are no major system changes planned for this research study database that would require participant notification.

**32. Does the system host a website? (Note: If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of PII)*

Yes

**37. Does the website have any information or pages directed at children under the age of thirteen?*

No

**50. Are there policies or guidelines in place with regard to the retention and destruction of PII? (Refer to the C&A package and/or the Records Retention and Destruction section in SORN)*

Yes

**54. Briefly describe in detail how the PII will be secured on the system using administrative, technical, and physical controls:*

The GWSS adheres to SRA corporate policies, CO-POL-27 Information Security Governance Policy and IT-POL-14 Information Security Policy, which detail the formal policy and guidelines for the Security Assessment and Authorization of SRA systems. These policies are reviewed annually. The GWSS is a standalone system with no interconnections to other information systems outside of the authorization boundary. The System Security Plan (SSP) documents an initial security control assessment and is provided to the authorizing official (AO) as a part of the NIEHS authorization to operate process. The SSP uses the NIST SP 800-53 security baseline for a moderate impact system to evaluate the security controls in the GWSS in order to document the extent to which the controls are implemented. The SSP requires substantial administrative, technical and physical controls for access to all project data. Specifically: all project data that contains PII is restricted to project folders, SurveyNet and the SAVVIS data center for study outcomes. As such, administrative controls in effect include the SSP, corporate access policies that restrict access to cleared project personnel only, backup plans that restrict the inclusion of PII for offsite storage, and the in-process system certification and accreditation. Access to PII is physically controlled through the use of two-factor user authentication, a dedicated Firewall and VPN architecture, database encryption methods and forced password reset/change policies. Physical access to systems that contain PII is controlled via required guards, personnel ID badges, cipher locks, biometrics access-control and is subject to regular monitoring via closed circuit television. Physical access to systems is granted to only project IT support staff and is logged. Sensitive PII adheres to the same controls listed above except that it is restricted to only the SAVVIS datacenter which is the system component that contains by far the most controls in terms of access and go well beyond those that are listed here (mantraps, 24x7 monitoring, etc.)

PIA REQUIRED INFORMATION

1 HHS Privacy Impact Assessment (PIA)

The PIA determines if Personally Identifiable Information (PII) is contained within a system, what kind of PII, what is done with that information, and how that information is protected. Systems with PII are subject to an extensive list of requirements based on privacy laws, regulations, and guidance. The HHS Privacy Act Officer may be contacted for issues related to Freedom of Information Act (FOIA) and the Privacy Act. Respective Operating Division (OPDIV) Privacy Contacts may be contacted for issues related to the Privacy Act. The Office of the Chief Information Officer (OCIO) can be used as a resource for questions related to the administrative, technical, and physical controls of the system. Please note that answers to questions with an asterisk (*) will be submitted to the Office of Management and Budget (OMB) and made publicly available in accordance with OMB Memorandum (M) 03-22.

Note: If a question or its response is not applicable, please answer ''N/A'' to that question where possible.

2 General Information

**Is this a new PIA?*

No

If this is an existing PIA, please provide a reason for revision:

PIA Validation

**1. Date of this Submission:*

Aug 14, 2012

**2. OPDIV Name:*

NIH

3. Unique Project Identifier (UPI) Number for current fiscal year (Data is auto-populated from the System Inventory form, UPI table):

N/A

**4. Privacy Act System of Records Notice (SORN) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):*

09-25-0200

**5. OMB Information Collection Approval Number:*

OMB Control Number: 0925-0626; ICR Reference Number: 201012-0925-004

5a. OMB Collection Approval Number Expiration Date:

Jan 31, 2014

**6. Other Identifying Number(s):*

N/A

**7. System Name: (Align with system item name)*

NIH NIEHS GuLF Worker Study System (GWSS)

8. System Location: (OPDIV or contractor office building, room, city, and state)

System Location:	
OPDIV or contractor office building	SAVVIS Datacenter
Room	21110
City	Sterling
State	VA

**9. System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:*

Point of Contact Information	
POC Name	David Johndrow

The following information will not be made publicly available:

POC Title	Director, Research Computing, SRA
POC Organization	SRA International
POC Phone	919-313-7580
POC Email	david_johndrow@sra.com

**10. Provide an overview of the system: (Note: The System Inventory form can provide additional information for child dependencies if the system is a GSS)*

The GuLF Worker Study System (GWSS) is a minor application whose purpose is to support the GuLF STUDY's subject recruitment and data collection efforts. This system will collect data pertaining to participant clean-up-related tasks, demographic and socioeconomic factors, occupational and health histories, psychosocial factors, and physical and mental health. A total of approximately 55,000 persons are expected to be enrolled into the cohort. The GWSS is a secure IT system which consists of commercially available research study software from DatStat (http://www.datstat.com), Microsoft SQL Server 2008 databases, and Avaya Dialer telephone software running on Windows 2008 Rel. 2. The DatStat product, Illume, is the tool used to design, build, test, and manage questionnaires (surveys). Illume is also the tool used for importing and exporting data and managing the data. The DatStat product, Discovery, manages the workflow of the trained personnel who administers computer-assisted telephone interviews (CATI) and computer-assisted personal interviews (CAPI).

SYSTEM CHARACTERIZATION AND DATA CATEGORIZATION

1 System Characterization and Data Configuration

11. Does HHS own the system?

Yes

11a. If no, identify the system owner:

N/A

12. Does HHS operate the system? (If the system is operated at a contractor site, the answer should be No)

Yes

12a. If no, identify the system operator:

N/A

**13. Indicate if the system is new or an existing one being modified:*

Existing

14. Identify the life-cycle phase of this system:

Operations/Maintenance

15. Have any of the following major changes occurred to the system since the PIA was last submitted?

No

Please indicate “Yes” or “No” for each category below:	Yes/No
Conversions	No
Anonymous to Non-Anonymous	No
Significant System Management Changes	No
Significant Merging	No
New Public Access	No
Commercial Sources	No
New Interagency Uses	No
Internal Flow or Collection	No
Alteration in Character of Data	No

16. Is the system a General Support System (GSS), Major Application (MA), Minor Application (child) or Minor Application (stand-alone)?

General Support System

**17. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system?*

Yes

TIP: If the answer to Question 17 is ‘‘No’’ (indicating the system does not contain PII), only the remaining PIA Summary tab questions need to be completed and submitted. If the system does contain PII, the full PIA must be completed and submitted. (Although note that ‘‘Employee systems,’’ – i.e., systems that collect PII ‘‘permitting the physical or online contacting of a specific individual … employed [by] the Federal Government – only need to complete the PIA Summary tab.)

Please indicate "Yes" or "No" for each PII category. If the applicable PII category is not listed, please use the Other field to identify the appropriate category of PII.

Categories:	Yes/No
Name (for purposes other than contacting federal employees)	Yes
Date of Birth	Yes
Social Security Number (SSN)	Yes

Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	Yes
Personal Phone Numbers	Yes
Medical Records Numbers	No
Medical Notes	Yes
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web Uniform Resource Locator(s) (URL)	No
Personal Email Address	Yes
Education Records	No
Military Status	Yes
Employment Status	No
Foreign Activities	No
Other	

17a. Is this a GSS PIA included for C&A purposes only, with no ownership of underlying application data? If the response to Q.17a is Yes, the response to Q.17 should be No and only the PIA Summary must be completed.

No

18. Please indicate the categories of individuals about whom PII is collected, maintained, disseminated and/or passed through. Note: If the applicable PII category is not listed, please use the Other field to identify the appropriate category of PII. Please answer "Yes" or "No" to each of these choices (NA in other is not applicable).

Categories:	**Yes/No**
Employees	No
Public Citizen	Yes
Patients	No
Business partners/contacts (Federal, state, local agencies)	No
Vendors/Suppliers/Contractors	No
Other	

**19. Are records on the system retrieved by 1 or more PII data elements?*

Yes

Please indicate "Yes" or "No" for each PII category. If the applicable PII category is not listed, please use the Other field to identify the appropriate category of PII.

Categories:	**Yes/No**
Name (for purposes other than contacting federal employees)	Yes
Date of Birth	No

SSN	No
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	No
Personal Phone Numbers	No
Medical Records Numbers	No
Medical Notes	No
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web URLs	No
Personal Email Address	No
Education Records	No
Military Status	No
Employment Status	No
Foreign Activities	No
Other	Participant Identification Number

20. Are 10 or more records containing PII maintained, stored or transmitted/passed through this system?

Yes

**21. Is the system subject to the Privacy Act? (If the response to Q.19 is Yes, the response to Q.21 must be Yes and a SORN number is required for Q.4)*

Yes

21a. If yes but a SORN has not been created, please provide an explanation.

INFORMATION SHARING PRACTICES

1 Information Sharing Practices

22. Does the system share or disclose PII with other divisions within this agency, external agencies, or other people or organizations outside the agency?

No

Please indicate "Yes" or "No" for each category below:	Yes/No
Name (for purposes other than contacting federal employees)	No
Date of Birth	No
SSN	No
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	No
Personal Phone Numbers	No
Medical Records Numbers	No
Medical Notes	No
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web URLs	No
Personal Email Address	No
Education Records	No
Military Status	No
Employment Status	No
Foreign Activities	No
Other	

**23. If the system shares or discloses PII please specify with whom and for what purpose(s):*

N/A

24. If the PII in the system is matched against PII in one or more other computer systems, are computer data matching agreement(s) in place?

Not Applicable

25. Is there a process in place to notify organizations or systems that are dependent upon the PII contained in this system when major changes occur (i.e., revisions to PII, or when the system is replaced)?

Not Applicable

26. Are individuals notified how their PII is going to be used?

Yes

26a. If yes, please describe the process for allowing individuals to have a choice. If no, please provide an explanation.

Individuals whose PII is collected undergo both a telephone survey and, potentially, a home visit. For the phone survey, an advanced mailing of a invitational lead letter, a privacy statement, a study brochure and a work history form is mailed to potential participants. During the phone interview, verification of receipt of the mailing is obtained and if not received, candidates have the right to request a subsequent mailing or are provided with information to view the privacy statement on the study website.

Participants are provided with the opportunity during the phone interview and informed consent process to not participate in the study.

27. Is there a complaint process in place for individuals who believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate?

Yes

27a. If yes, please describe briefly the notification process. If no, please provide an explanation.

SRA International, Inc., policy requires that if any complaint or concern is registered regarding the potential breach of personally identifying information, the project team will immediately report such an occurrence to the SRA Cyber Security and Privacy Department and the NIH principal investigator(s). This requirement is upheld by the project team and is in effect regardless of the source of the complaint.

28. Are there processes in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy?

Yes

28a. If yes, please describe briefly the review process. If no, please provide an explanation.

The information collected and processed throughout the life cycle of the GWSS will be afforded the protections required to safeguard its confidentiality, integrity and availability. Data within the GWSS, both at rest and in transit will be encrypted using FIPS-140-2 compliant mechanisms and applications.
The GWSS has been evaluated for impact on its confidentiality, integrity, and availability requirements. The results for each security objective are as follows:
· Confidentiality: The GWSS contains personally identifying information (PII) and medical information. The unauthorized disclosure of GWSS information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Thus, the confidentiality of the system is rated Moderate.
· Integrity: The mission of NIEHS is to reduce the burden of human illness and disability by understanding how environment influences the development and progression of disease. NIEHS pursues this mission through multidisciplinary biomedical research and through communication of research results to regulatory agencies, clinicians, the scientific community, and the general public. The GWSS enables this research. Therefore, the unauthorized modification of GWSS information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Thus, the integrity of the system is rated Moderate.
Availability: The unavailability of the GWSS information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Thus, the information and protection measures are rated as Low.

29. Are there rules of conduct in place for access to PII on the system?

Yes

Please indicate "Yes," "No," or "N/A" for each category. If yes, briefly state the purpose for each user to have access:

Users with access to PII	Yes/No/N/A	Purpose
User	Yes	To run reports; assist with scheduling.
Administrators	Yes	To run reports and to update the system as needed.
Developers	Yes	To update the system as needed.
Contractors	No	
Other	Yes	Research Telephone Center Interviewers & Managers; Home Visit Agents - To enter data; assist with scheduling

**30. Please describe in detail: (1) The information the agency will collect, maintain, or disseminate (clearly state if the information contained in the system ONLY represents federal contact data); (2) Why and for what purpose the agency will use the information; (3) Explicitly indicate whether the information contains PII; and (4) Whether submission of personal information is voluntary or mandatory:*

Collection of this information is authorized under 5 U.S.C. 552a. The primary use of this information is for use in a research study entitled GuLF STUDY: GuLF Long-Term Follow Up Study, sponsored by the National Institute of Environmental Health Sciences (NIEHS). The mission of NIEHS is to reduce the burden of human illness and disability by understanding how environment influences the development and progression of disease. NIEHS pursues this mission through multidisciplinary biomedical research and through communication of research results to regulatory agencies, clinicians, the scientific community, and the general public. The GWSS enables this research.

PII collected as part of this study includes name, address, phone numbers, date of birth, race/ethnicity, social security number, demographic and socioeconomic factors, and medical information. Information is not disclosed to persons outside of the study team, as protected by a Certificate of Confidentiality. Submission of this information is required if a participant wishes to participate in the research study.

**31. Please describe in detail any processes in place to: (1) 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 the original collection); (2) Notify and obtain consent from individuals regarding what PII is being collected from them; and (3) How the information will be used or shared. (Note: Please describe in what format individuals will be given notice of consent [e.g., written notice, electronic notice, etc.])*

Individuals whose PII is collected undergo an informed consent process with a trained member of the study team. Participants are told that their information is protected through a Certificate of Confidentiality and that it may be placed, in a coded or de-identified format, in a database to be used by other researchers. There are no major system changes planned for this research study database that would require participant notification.

WEBSITE HOSTING PRACTICES

1 Website Hosting Practices

**32. Does the system host a website? (Note: If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of PII)*

Yes

Please indicate "Yes" or "No" for each type of site below. If the system hosts both Internet and Intranet sites, indicate "Yes" for "Both" only.	**Yes/ No**	**If the system hosts an Internet site, please enter the site URL. Do not enter any URL(s) for Intranet sites.**
Internet	Yes	http://www.nihgulfstudy.org
Intranet	Yes	
Both	Yes	

33. Does the system host a website that is accessible by the public and does not meet the exceptions listed in OMB M-03-22?

Note: OMB M-03-22 Attachment A, Section III, Subsection C requires agencies to post a privacy policy for websites that are accessible to the public, but provides three exceptions: (1) Websites containing information other than "government information" as defined in OMB Circular A-130; (2) Agency intranet websites that are accessible only by authorized government users (employees, contractors, consultants, fellows, grantees); and (3) National security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology (see section 202(i) of the E-Government Act.).

Yes

34. If the website does not meet one or more of the exceptions described in Q. 33 (i.e., response to Q. 33 is "Yes"), a website privacy policy statement (consistent with OMB M-03-22 and Title II and III of the E-Government Act) is required. Has a website privacy policy been posted?

No

35. If a website privacy policy is required (i.e., response to Q. 34 is ''Yes''), is the privacy policy in machine-readable format, such as Platform for Privacy Preferences (P3P)?

Yes

35a. If no, please indicate when the website will be P3P compliant:

36. Does the website employ tracking technologies?

No

Please indicate "Yes", "No", or "N/A" for each type of cookie below:	**Yes/No/N/A**
Web Bugs	No
Web Beacons	No
Session Cookies	No
Persistent Cookies	No
Other	No

**37. Does the website have any information or pages directed at children under the age of thirteen?*

No

37a. If yes, is there a unique privacy policy for the site, and does the unique privacy policy address the process for obtaining parental consent if any information is collected?

N/A

38. Does the website collect PII from individuals?

No

Please indicate “Yes” or “No” for each category below:	Yes/No
Name (for purposes other than contacting federal employees)	No
Date of Birth	No
SSN	No
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	No
Personal Phone Numbers	No
Medical Records Numbers	No
Medical Notes	No
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web URLs	No
Personal Email Address	No
Education Records	No
Military Status	No
Employment Status	No
Foreign Activities	No
Other	No

39. Are rules of conduct in place for access to PII on the website?

Not Applicable

40. Does the website contain links to sites external to HHS that owns and/or operates the system?

Yes

40a. If yes, note whether the system provides a disclaimer notice for users that follow external links to websites not owned or operated by HHS.

Not currently. A disclaimer will be active by October 15, 2011.
AHS cannot guarantee the privacy or security of information you provide to these other Web sites. You should review their privacy policies as well if you have concerns.
Reference in this Web site to any specific commercial products, process, service, manufacturer, or company does not constitute endorsement or recommendation by the US Government or AHS.

ADMINISTRATIVE CONTROLS

1 Administrative Controls

Note: This PIA uses the terms "Administrative," "Technical" and "Physical" to refer to security control questions—terms that are used in several Federal laws when referencing security requirements.

41. Has the system been certified and accredited (C&A)?

No

41a. If yes, please indicate when the C&A was completed:

41b. If a system requires a C&A and no C&A was completed, is a C&A in progress?

Yes

42. Is there a system security plan for this system?

Yes

43. Is there a contingency (or backup) plan for the system?

Yes

44. Are files backed up regularly?

Yes

45. Are backup files stored offsite?

No

46. Are there user manuals for the system?

No

47. Have personnel (system owners, managers, operators, contractors and/or program managers) using the system been trained and made aware of their responsibilities for protecting the information being collected and maintained?

Yes

48. If contractors operate or use the system, do the contracts include clauses ensuring adherence to privacy provisions and practices?

Yes

49. Are methods in place to ensure least privilege (i.e., "need to know" and accountability)?

Yes

49a. If yes, please specify method(s):

The GWSS is designed such that users are only able to access parts of the system based on their designated permissions and assigned roles. For example, telephone interviewers are permitted to enter data but not to retrieve data. When contractors are terminated, call center and field operations management inform the GWSS system administrators and facility management to terminate the contractor's accounts and physical access. Management ensures the retrieval of all project assets and property.

**50. Are there policies or guidelines in place with regard to the retention and destruction of PII? (Refer to the C&A package and/or the Records Retention and Destruction section in SORN):*

Yes

50a. If yes, please provide some detail about these policies/practices:

On January 12, 2010, SRA received notice and guidance pursuant to SRA's work on clinical contract number N01-ES-55553, work assignment 44, entitled "Gulf Oil Spill Cohort Study," for the U.S. Department of Health and Human Services. The letter requests that SRA preserve and not destroy certain information. This letter confirmed that all HHS personnel and entities must preserve all documents, business records and information or communications related in any way to the explosion and fire on April 20, 2010 in the Gulf of Mexico, off the coast of Louisiana, and the resulting oil spill ("Gulf Oil Spill") and any damages, costs or effects. NIH's Manual Chapter (MC) 1743, http://oma.od.nih.gov/manualchapters/management/1743/, does not apply for BP Deepwater Litigation Hold information. This MC is normally used to determine the disposition of records. However, for the Deepwater Horizon Litigation Hold records, it has been superseded by guidance provided in the attached files: BP Frequently Asked Questions FINAL version (Date corrected).pdf; BP Instructions on Digital Cameras.pdf; BP Instructions on Hard Drives of Departing Employee.pdf; and Deepwater Horizon Litigation Hold.pdf. In reference to the BP Deepwater Horizon Litigation Hold, do not delete, throw out, shred, or otherwise discard or destroy potentially relevant information or allow deletion to happen by automatic deletion operations. Any records pertaining to the BP Deepwater Litigation Hold cannot be destroyed.

TECHNICAL CONTROLS

1 Technical Controls

51. Are technical controls in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system?

Yes

Please indicate "Yes" or "No" for each category below:	Yes/No
User Identification	Yes
Passwords	Yes
Firewall	Yes
Virtual Private Network (VPN)	Yes
Encryption	Yes
Intrusion Detection System (IDS)	No
Common Access Cards (CAC)	No
Smart Cards	No
Biometrics	No
Public Key Infrastructure (PKI)	No

52. Is there a process in place to monitor and respond to privacy and/or security incidents?

Yes

52a. If yes, please briefly describe the process:

The System Administrators will monitor the GWSS security controls on an ongoing basis through the use of vulnerability scanning, log analysis, configuration management, change control, and security impact analysis. GWSS System Administrators will identify and assess a subset of "volatile" controls for the information system on an annual basis. The security state of the SRA network is maintained in this SSP and the GWSS POA&M list.

PHYSICAL ACCESS

1 Physical Access

53. Are physical access controls in place?

Yes

Please indicate “Yes” or “No” for each category below:	Yes/No
Guards	Yes
Identification Badges	Yes
Key Cards	Yes
Cipher Locks	Yes
Biometrics	Yes
Closed Circuit TV (CCTV)	Yes

**54. Briefly describe in detail how the PII will be secured on the system using administrative, technical, and physical controls:*

The GWSS adheres to SRA corporate policies, CO-POL-27 Information Security Governance Policy and IT-POL-14 Information Security Policy, which detail the formal policy and guidelines for the Security Assessment and Authorization of SRA systems. These policies are reviewed annually. The GWSS is a standalone system with no interconnections to other information systems outside of the authorization boundary. The System Security Plan (SSP) documents an initial security control assessment and is provided to the authorizing official (AO) as a part of the NIEHS authorization to operate process. The SSP uses the NIST SP 800-53 security baseline for a moderate impact system to evaluate the security controls in the GWSS in order to document the extent to which the controls are implemented. The SSP requires substantial administrative, technical and physical controls for access to all project data. Specifically: all project data that contains PII is restricted to project folders, SurveyNet and the SAVVIS data center for study outcomes. As such, administrative controls in effect include the SSP, corporate access policies that restrict access to cleared project personnel only, backup plans that restrict the inclusion of PII for offsite storage, and the in-process system certification and accreditation. Access to PII is physically controlled through the use of two-factor user authentication, a dedicated Firewall and VPN architecture, database encryption methods and forced password reset/change policies. Physical access to systems that contain PII is controlled via required guards, personnel ID badges, cipher locks, biometrics access-control and is subject to regular monitoring via closed circuit television. Physical access to systems is granted to only project IT support staff and is logged. Sensitive PII adheres to the same controls listed above except that it is restricted to only the SAVVIS datacenter which is the system component that contains by far the most controls in terms of access and go well beyond those that are listed here (mantraps, 24x7 monitoring, etc.)

APPROVAL/DEMOTION

1 System Information

System Name:	NIH NIEHS GuLF Worker Study System (GWSS)

2 PIA Reviewer Approval/Promotion or Demotion

Promotion/Demotion:	Promote
Comments:	
Approval/Demotion Point of Contact:	Kim Minneman
Date:	Aug 14, 2012

3 Senior Official for Privacy Approval/Promotion or Demotion

Promotion/Demotion:	Promote
Comments:	

4 OPDIV Senior Official for Privacy or Designee Approval

Please print the PIA and obtain the endorsement of the reviewing official below. Once the signature has been collected, retain a hard copy for the OPDIV's records. Submitting the PIA will indicate the reviewing official has endorsed it

This PIA has been reviewed and endorsed by the OPDIV Senior Official for Privacy or Designee (Name and Date):

Name: ______________________________________ **Date:** ____

Name:	Karen Plá
Date:	Sep 28, 2012

5 Department Approval to Publish to the Web

Approved for web publishing	
Date Published:	
Publicly posted PIA URL or no PIA URL explanation:	

PIA % COMPLETE

1	PIA Completion
PIA Percentage Complete:	100.00
PIA Missing Fields:	