ANNUAL PERSONAL INFORMATION SYSTEM REPORT
Privacy Impact Assessment (PIA)
Deadline for Submission: September 30

Effective January 1, 2009, any government agency that maintains one or more personal information system shall submit to the State of Hawai'i Information Privacy and Security Council an annual report on the existence and character of each personal information system added or eliminated since the agency's previous annual report. The report shall be submitted no later than September 30 of each year. (HRS§ 487N-7)

"Personal information system" means any manual or automated recordkeeping process that contains personal information and the name, personal number, or other identifying particulars of a data subject.

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either name or data elements are not encrypted:

1. Social Security number;
2. Driver's license number or Hawai'i identification card number; or
3. Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.
   Note: Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

PART I.
PIA Contacts and Qualification Questions

A. Contact Information

System Title:	Document Date: Enter the date you are creating or updating this document

Office of Responsibility:

Enter the service, office, division or department name

Program Manager Name:	Program Manager Title:	Phone: eMail:

B. Qualification Questions

1. Does your system collect any information in identifiable form (personal data) on the general public?
❑ Yes ❑ No

Information in identifiable form (also known as personal data/information) refers to any data collected about an individual that can be used for identification purposes.

It includes information that identifies the individual by name or other unique identifier in conjunction with other data elements such as gender, race, birth date, age, geographic indicator, personal e-mail address, home address, home phone number, health records, Social Security Number (SSN), personal credit card information, and similar personal information. Information permitting the physical or online contacting of a specific individual is considered information in identifiable form.

This does not refer to business entities or government agencies, or aggregate data that cannot be traced back to an individual person.

2. Does your system collect any information in identifiable form (personal data/information) on government employees?
❑ Yes ❑ No

Information in identifiable form refers to any data collected about an employee that can be used for identification purposes. It includes information that identifies the employee by name or other unique identifier in conjunction with other data elements such as gender, race, birth date, age, marital status, home e-mail address, home address, home phone number, health records, SSN, performance appraisals, employment history not related to current job, allegations of misconduct/arrests/ complaints/grievances/performance based actions, payroll deductions, personal credit card information, and similar personal information.

3. Has a PIA been done before for the system? ❑ Yes ❑ No	If Yes to 3., enter the date of the last PIA, otherwise leave blank:

NOTE: If you answered NO to BOTH B.1. and B.2. above, STOP HERE.

PART II. System Assessment Part II is for systems that answered YES to EITHER B.1. or B.2. above.	
A. Data in the System	
1. What is the specific purpose of the agency's use of the information and how does that use fit with the agency's broader mission? Agency should use plain language to disclose the purpose(s) of its use of the information. Agency's description should provide enough detail to allow the reader to gain full understanding of the purpose(s).	
1.a. Describe all information to be included in the system. Briefly describe the purpose of the system and the data that will be in the system, including that of any subsystems.	
1.b. Describe all PERSONAL information to be included in the system. Provide the specific privacy data elements that will be maintained in the system.	
1.c. What stage of the life cycle is the system currently in? Select one. ❑ Design/Planning ❑ Operation/Maintenance ❑ Development/Implementation ❑ Disposal	
2.a. What are the sources of the information in the system? Describe where the system data originates, whether the privacy information is provided by the user or entered on behalf of the user and by whom, or if it comes programmatically from another system.	
2.b. What State files and databases are used? Identify any State files and databases that may be used as a source of the information.	
2.c. What Federal agencies are providing data for use in the system? List Federal agencies that are providing the information for use by the system. Specify data provided by each. If none, enter None.	
2.d. What State and local agencies are providing data for use in the system? List any State and local agencies that are providing data for use in this system. Specify the data provided by each. If none, enter None.	
2.e. From what other third party sources will the data be collected? List any other sources of data in the system and the data provided. If none, enter None.	
2.f. What information will be collected from the individual whose record is in the system? List the data that will be collected from the individual.	
3.a. How will the data collected from sources other than State agency records or the individual be verified for accuracy? The accuracy of personal information is very important. Indicate the steps that will be taken to ensure that the data is accurate and the integrity of the data remains intact.	

3.b. How will data be checked for completeness? Missing information can be as damaging as incorrect information. Indicate the steps that will be taken to ensure that all of the data is complete.	
3.c. Is the data current? How do you know? Indicate the process that will be used to ensure that the data is relevant and up-to-date.	
4. Are the data elements described in detail and documented? If yes, what is the name of the document? Each of the data elements must be defined and described. Descriptions should include the name, data type, and purpose for collection.	
B. Access to the Data	
1.a. Who will have access to the data in the system? Provide a list of users or groups of users of the entire system (i.e. government agencies, public access, etc.) and a separate list of people who will have access to privacy data.	
1.b. Is any of the data subject to exclusion from disclosure under the Federal Freedom of Information Act (FOIA)? If yes, explain the policy and rationale supporting this decision. If so, reference the specific exemption under the FOIA (5 U.S.C. Section (b)(1) through (9)), to support your rationale. Dept. of Justice guidance on exemptions: http://www.usdoj.gov/oip/foi-act.htm FOIA text: http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm	
1.c. Is any of the data subject to exclusion from disclosure under the State of Hawai'i Uniform Information Practices Act (UIPA)? If yes, explain the policy and rationale supporting this decision. If so, reference the specific exemption under UIPA. Otherwise enter NONE. Office of Information Practices, State of Hawai'i: http://oip.hawaii.gov/laws-rules-opinions/uipa/	
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented? List any policies or procedures used to implement access to the system and privacy data. If there are supporting documents such technical and operational manuals or a system security plan, list them here.	
3. Will users have access to all data in the system or will the users' access be restricted? Explain. Specify to what degree users can access their own privacy data after it has been entered. If there are any restrictions on access to this data, identify the restrictions.	

4. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access? Reference technical, managerial, administrative, and operational controls in place supporting management of the data.	
5.a. Do other systems share data or have access to data in this system? If yes, explain, otherwise enter NO. List any systems that will either send or receive data in this system. Explain the purpose of the connection and the methods used to ensure integrity and security of the data being exchanged.	
5.b. Who will be responsible for protecting the privacy rights of the clients and employees affected by the interface? List the title and office of the person(s) responsible to ensure that the privacy data is being handled properly. This typically should be the System Manager.	
6.a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)? List any entities that may access the data in this system and specify which data. If there are none, enter None.	
6.b. How will the data be used by the agency? Describe in detail how each piece of data will be used, including programmatic functions, indexing, aggregation, reporting, etc.	
6.c. Who is responsible for assuring proper use of the data? This should typically be the same person(s) listed for question 5.b.	
6.d. How will the system ensure that agencies only get the information to which they are entitled? List the controls and security mechanisms in place to ensure that exchange of data is appropriate.	
7. What is the life expectancy of the data? Indicate whether the data will be collected and used for a one-time process or whether the data will be maintained in a database. Indicate how long the one-time process typically takes or how long data will be maintained. If shared with other systems, provide indication on life expectancy from those systems as well.	
8. How will the data be disposed of when it is no longer needed? Provide explanation of data disposal process. Indicate methods for disposing of data from operational databases as well as for archiving systems.	
C. Attributes of the Data	
1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? List each data element and the relevance to the system.	

2.a.1. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected? ❑ Yes ❑ No. If yes, provide details on the derivation of the data. An example would be to create a credit risk rating based on credit history.	
2.a.2. If YES to 2.a.1 above, describe how the system derive new data or create previously unavailable data about an individual through aggregation from the information collected.	
2.b. Will the new data be placed in the individual's record (client or employee)? ❑ Yes ❑ No.	
2.c. Can the system make determinations about individuals that would not be possible without the new data? ❑ Yes ❑ No. Explain why or why not.	
2.d. How will the new data be verified for relevance and accuracy? Since this is privacy data about an individual that was not provided by the individual, the relevance and accuracy are very important. Provide details on processes used to verify this information.	
3.a. If the data is being consolidated, what controls are in place to protect the data and prevent unauthorized access? Explain. Enter N/A if the data is not being consolidated. Otherwise, describe the controls used to ensure that aggregated or consolidated privacy data remains protected.	
3.b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? If yes, explain. Enter N/A if the processes are not being consolidated. Otherwise, describe the controls used to ensure that aggregated or consolidated privacy data remains protected.	
4. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain. Explain all processes for retrieving the data. If personal identifiers (i.e. name, SSN, employee number, etc.) are used, list the identifiers.	
5. What are the potential effects on the privacy rights of individuals of: a. Consolidation and linkage of files and systems; b. Derivation of data; and c. Use of new technologies. How are the effects to be mitigated? Explain how the privacy rights of the individual may be protected or jeopardized based on a, b, and c. List all mitigation strategies used to ensure that the rights of the individuals are not compromised.	

D. Maintenance of Administrative Controls	
1.a. Explain how the system and its use will ensure equitable treatment of individuals. Describe the processes in place to ensure fair and equitable treatment of individuals and their privacy data. If judgments are to be made based on the privacy data, indicate the rationale to be used to make the judgments and how the judgments will be kept fair and equitable.	
1.b. If the system is operated in more than one site, how will consistent use of the system be maintained at all sites? Describe technical, managerial, and operational controls in place to ensure that data integrity and protection is maintained across sites. Also, describe how data will be kept current and consistent between locations.	
1.c. Explain any possibility of disparate treatment of individuals or groups. Describe any potential situation where data could be evaluated differently. List the data elements that may impact disparate treatment (i.e. race, gender, etc.).	
2.a. What are the retention periods of data in this system? How long will data be kept (years, months, day, hours)? Use State of Hawai'i records disposition schedules to determine requirements.	
2.b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented? Provide detailed explanation of the data disposal process. Indicate methods for disposing of data from operational databases as well as archiving procedures. List documents supporting these procedures and the locations of these documents.	
2.c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations? Describe data management procedures and updating requirement.	
3.a. Is the system using technologies in ways that Federal agencies have not previously employed (e.g. Caller-ID)? ❑ Yes ❑ No. If yes, describe any technologies that may be used to collect or display privacy data.	
3.b. How does the use of this technology affect individuals' privacy? Is the data more vulnerable to inadvertent or unintentional display? Does it improve the protection of the privacy data?	
4.a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain. Describe the rationale and processes for identifying, locating, and monitoring individuals. This can include street address, e-mail, cell phone, as well as GPS data.	

4.b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain. Describe the rationale and processes for identifying, locating, and monitoring groups of individuals. This can include street address, email, cell phone, as well as GPS data.	
4.c. What controls will be used to prevent unauthorized monitoring? Describe managerial, technical, and operational controls used to manage monitoring activities.	
5.a. Under which Privacy Act System of Records notice (SOR) does the system operate? Provide number and name. *If this is a Federal associated system, under which Privacy Act System of Records notice (SOR) does the system operate? Provide number and name. If not Federal associated, enter N/A.*	
5.b. If the system is being modified, will the SOR require amendment or revision? Explain. *If this is a Federal associated system, AND if any of the information in the SOR is altered, such as acquisition of new privacy information, new implementations, etc., explain how or why the SOR should be amended. Coordinate preparation of a revised SOR with the Privacy Act Officer. IF there are no modifications or if not Federal associated, enter N/A.*	

PART III.
Use of Third Party Website or Application
Fill out Part III only if this system utilizes a third party website or application (e.g. SAAS).

A. Use of a Third-Party Website or Application	
1. What is the specific purpose of the agency's use of the third-party website or application, and how does that use fit with the agency's broader mission? Agency should use plain language to disclose the purpose(s) of its use of the third-party websites or applications.	
2. Is the agency's use of the third-party website or application consistent with all applicable laws, regulations, and policies? Agency should make clear that it will comply with all applicable laws, regulations, and policies, in particular those pertaining to privacy, accessibility, information security, and records management. Provide examples showing how it will comply with policies. Agency should indicate that it will work with its counsel to ensure that its use of third-party websites and applications remains compliant.	
B. Third-Party Website Application Assessment Use of PII	
1. Is there any PII that is likely to become available to the agency through the use of the Third-Party website or application? Answer should be tailored to address the specific websites and applications being used.	

2.a. Will REGISTRATION PII be made available to Agency?	2.b. Will SUBMISSION PII be made available to Agency?
❑ Yes ❑ No Many third-party websites or applications request PII at the time of registration. Agencies should make clear whether they will have access to this information and whether users can take steps to limit agencies access.	❑ Yes ❑ No An individual can make information available to agencies when he or she provides, submits, communicates, links, posts, or associates PII while using the third-party website or application. This can include such activities as "friend-ing," "following," "liking," joining a "group," becoming a "fan," and comparable functions.

2.c. Will ASSOCIATION PII be made available to Agency? ❑ Yes ❑ No Even when individuals do not actively post or submit information, they can potentially make PII available to the agency by "associating" themselves with the websites or applications. Such acts of association may include activities commonly referred to as "friending," "following," "liking," joining a "group," becoming a "fan," and comparable functions.	2.d. Will ACCOUNT PII be made available to Agency? ❑ Yes ❑ No Even individuals who do not have an account with a third-party website or application may make PII available to agencies if certain functions of the website or application are available to individuals without an account. Agencies should make clear whether they will have access to this information and whether users can take steps to limit agencies' access.
3. How will agency use the PII as described above in section 2?	
4. The types of uses that PII will be subjected to in this system are: (answer in following list 4.a. - 4.d.)	
4.a. PII will be subjected to Public interaction / open government activities use ❑ Yes ❑ No This could include surveys, contests, or message boards that provide a forum for the public to comment on the agency's activities.	4.b. PII will be subjected to Recruitment and/or employee outreach use ❑ Yes ❑ No In order to recruit and hire from the widest possible pool of candidates, the agency may consider using third-party websites or applications to attract new hires or to inform or receive feedback from current employees.
4.c. PII will be subjected to Participation in agency programs or systems use ❑ Yes ❑ No The agency may consider using third-party websites or applications in order to facilitate access to programs or systems. The agency should consider and address whether this use will result in the PII being combined, matched, or otherwise used in concert with PII that is already maintained by the agency.	4.d. PII will be subjected to Web measurement and/or customization use ❑ Yes ❑ No The agency may use third-party websites or applications to conduct measurement and analysis of web usage, or to customize the user's experience.
5. How will the data be retrieved on third-party website or application? Can it be retrieved by personal identifier? If yes, explain. Explain all processes for retrieving the data. If personal identifiers (i.e. name, SSN, employee number, etc.) are used, list the identifiers. Registration process should also be considered.	
C. Identification and Mitigation of Other Privacy Risks – Sharing and Disclosure of PII	
1.a. The following risk exists: Disclosure of PII by Users ❑ Yes ❑ No The agency must choose to delete or hide comments or other user interactions when a user's sensitive information is included. Agency should provide a notice to users on the third-party site, warning individuals to avoid sharing or disclosing sensitive PII.	1.b. The following risk exists: Third-Party advertising and tracking ❑ Yes ❑ No Advertisements may contain cookies or bugs and PII may be shared by website operator with advertiser.
1.c. The following risk exists: Spam, Unsolicited communications, Spyware and other threats ❑ Yes ❑ No Users may receive spam or other unsolicited or fraudulent communication from a third party as a result of their interactions with the agency on the website. To avoid harm, users should be wary of responding to such communications.	1.d. The following risk exists: Accounts or pages that misrepresent agency authority or affiliation ❑ Yes ❑ No Certain accounts or pages on the website may not be officially authorized by or affiliated with, the agency, even if they use official insignia or otherwise appear to represent the agency or the Federal Government.

1.e. The following risk exists: External Links and embedded third-party applications ❑ Yes ❑ No If the agency posts a link that leads to a third-party website or any other location that is not part of an official government domain, agency should provide notice to user to explain that users are being directed to a nongovernment website that may have different privacy policies (and risks) from those agency's own official website.	1.f. The following risk exists: Monitoring future requirements and future technology ❑ Yes ❑ No Agency should establish and maintain procedures to identify, evaluate, and address any new additional privacy requirements that may result from new statutes, regulations or policies.
2. If the answer is YES to 1a-1f, how will the agency mitigate those risks? If the answer is YES to 1a, how will the agency mitigate those risks? Describe technical, managerial, and operational controls in place to ensure that data integrity and protection is maintained across sites. Also describe how data will be kept current and consistent between locations	
3. Have employees and contractors been trained and instructed not to solicit sensitive information when interacting with users on behalf of the agency? Describe any potential situation where data could be evaluated differently. List the data elements that may impact disparate treatment (i.e. race, gender, etc.)	
4. How does the use of this technology affect individuals' privacy? Is the data more vulnerable to inadvertent or unintentional display? Does it improve the protection of the privacy data?	
4.a. Will this third-party website or application provide the capability to identify, locate, and monitor individuals? If yes, explain. Describe the rationale and processes for identifying, locating, and monitoring individuals. This can include street address, e-mail, cell phone, as well as GPS data available while using third-party website or application.	
4.b. Will this third-party website or application provide the capability to identify, locate, and monitor groups of people? If yes, explain. Describe the rationale and processes for identifying, locating, and monitoring groups of individuals. This can include street address, email, cell phone, as well as GPS data.	
4.c. What controls will be used to prevent unauthorized monitoring? Describe managerial, technical, and operational controls used to manage monitoring activities.	
When you have completed all questions, save this document and email it to ipsc@hawaii.gov.	