



**Information Privacy and Security Council (IPSC)
Meeting Agenda**

May 17, 2023, 1:00 p.m.

1151 Punchbowl Street, Conference Room 410, Honolulu, Hawai'i

This meeting will be conducted remotely by interactive conference technology (ICT). Members of the public may participate via ICT or in person at the location indicated above.

Join on your computer or mobile app: [Click here to join the meeting](#)

Meeting ID: 256 065 620 299; Passcode: zNNwat

Or call in (audio only): [+1 808-829-4853](tel:+18088294853).,[614645431#](tel:+18088294853)

- I. Call to Order
- II. Review and Approval of the February 15, 2023, Meeting Minutes
- III. Public Testimony
Individuals may provide oral testimony during the meeting, or submit written testimony in advance, on any agenda item. Oral testimony will be limited to three minutes per person or organization. Written testimony may be sent via e-mail to ets@hawaii.gov, Subject: *IPSC Testimony*; or mailed to IPSC, 1151 Punchbowl Street, Room B-10, Honolulu, HI, 96813.
- IV. 2023 Legislation; Discussion and Appropriate Action
 - SB1178 – Update the definition of “personal information” in Chapter 487N, Hawaii Revised Statutes
 - Other Bills
- V. Annual Personal Information System Report; Discussion and Appropriate Action
 - Review and Update Privacy Impact Assessment form
- VI. Information Technology Security Controls
The committee anticipates going into executive session, pursuant to Hawai'i Revised Statutes (HRS) section 92-5(a)(6), to consider sensitive matters related to public safety or security.
- VII. Good of the Order
 - Announcements
 - Next scheduled meeting: June 21, 2023
- VIII. Adjournment

This ICT meeting will allow closed caption transcription to be activated by participants.

If you need an auxiliary aid/service or other accommodation due to a disability, contact Susan Bannister at (808) 586-6000 or susan.bannister@hawaii.gov as soon as possible. Requests made as early as possible have a greater likelihood of being fulfilled. Upon request, this notice is available in alternate/accessible formats.



Information Privacy and Security Council (IPSC)
Meeting Minutes - DRAFT
February 15, 2023

Meeting held via videoconference interactive conferencing technology

Members Present

| | |
|--|--|
| Vincent Hoang, CISO, Chair Designee | Office of Enterprise Technology Services (ETS) |
| Jonathan Chee | Department of Education |
| Courtney Kinder | Department of Health |
| David Keane | Department of Human Resources Development |
| Mark Choi | Department of Human Services |
| Jodi Ito | University of Hawai'i |
| Kelly Agena | County of Kauai |
| Karen Sherman | County of Maui |

Members Excused

| | |
|-----------------|---|
| David Shak | Department of Commerce and Consumer Affairs |
| Mai Nguyen Van | Judiciary |
| Carol Taniguchi | Legislature |
| Mark Wong | City & County of Honolulu |
| Scott Uehara | County of Hawaii |

Other Attendees

| | |
|-----------------|-----|
| James Gonser | ETS |
| Arnold Kishi | ETS |
| Susan Bannister | ETS |

I. Call to Order

Quorum was established and Chair Hoang called the meeting to order at 2:04 p.m.

II. Review and Approval of the November 16, 2022, Meeting Minutes

Member Choi made a motion to approve the minutes as presented, which was seconded by Member Ito. A vote was taken and passed unanimously.

III. 2023 Legislation - SB1178 Update the definition of "personal information" in Chapter 487N, Hawaii Revised Statutes

Chair Hoang noted that SB1178 resembles versions that were introduced twice before. It amends the definition of "personal information" and expands it to include an identifier in combination with one or more of specified data elements. Member Sherman asked if revisions can be made and if the bill will go through this year. Chair Hoang stated that

recommendations to amend the bill can still be made and encouraged agencies to submit testimony. He commented that the current language is dated and needs to be updated. Member Choi voiced concerns with implementation once it becomes law. Systems would need to be modified, processes updated, involve additional funding. Member Ito stated that one identifier must be combined with one of the specified data elements to constitute a breach. Those elements are already protected and encrypted and not available to the public.

IV. Annual Personal Information System Report – Review and Update the Privacy Impact Assessment Form

Chair Hoang asked the members to review the form to see if the questions are clear and data collected is relevant to better protect and provide better safeguards in maintaining that information. For starters, Chair Hoang recommended deleting Part 3. The information collected is not pertinent and created confusion among the agencies. He asked that proposed changes be made at the next IPSC to allow time for implementation.

V. Good of the Order

Next scheduled meeting: March 15, 2023

Chair Hoang made a motion to adjourn the meeting, which was seconded by Member Keane. With no objections, the meeting adjourned at 2:27 p.m.

**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. ([HRSS 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 office, division or department name) | |
| Program Manager Name | Phone |
| Program Manager Title | E-Mail |

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, 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 system?

Briefly describe the purpose of the system and its mission to the reporting organization

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.

General Public

| | |
|--|--|
| Birth date | International Identifying Number (e.g. Social Security Number) |
| Home Address | Credit Card Information |
| Contact Information (e.g. phone number, email address, etc.) | Financial Institution Account Information |
| Societal Information (e.g. race, ethnic origin, sexual preference, marital status, etc.) | Medical Information |

Government Employee(s)

| | |
|--|--|
| Birth date | International Identifying Number (e.g. Social Security Number) |
| Home Address | Credit Card Information |
| Contact Information (e.g. phone number, email address, etc.) | Financial Institution Account Information |
| Societal Information (e.g. race, ethnic origin, sexual preference, marital status, etc.) | Medical Information |
| Hire Date | Salary/Compensation Information |
| Performance Reviews/Evaluations | Dependents or Beneficiaries |

| | | |
|--|-------------------|------------------|
| 2. Approximately how much active PII records is the system storing? | < 10,000 | 10,000 to 49,999 |
| | 50,000 to 499,999 | > 500,000 |

| | | |
|--|-----------------------|----------------------------|
| 3. What stage of the life cycle is the system currently in? Select one. | Design/Planning | Development/Implementation |
| | Operation/Maintenance | Disposal/Decommissioned |

| | |
|--|--|
| 4. 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. | Provided/inputted by the user |
| | Entered on behalf of the user by an internal staff or third-party source |
| | Programmatically from another system |

| | |
|--|--|
| 5. What State files and databases are used? Identify any State files and databases that may be used as a source of the information. | State, Local, Tribal, and Territorial (SLTT) government entities |
| | Federal government entities |
| | Authorized Third-Party Vendors |
| | Private Corporations, Non-profits, etc. |
| | None |
| | Other (if other, please specify below) |

| | | |
|--|--|----|
| 6. Will this system provide the capability to physically identify, locate, and monitor individuals? | Yes | No |
| | If yes, check all that applies: | |
| | Physical Address | |
| | Email Address | |
| | Phone Number(s) | |
| | GPS data | |
| | Other (if other, please specify below) | |

| | |
|--|--|
| 7. Will this system provide the capability to physically identify, locate, and monitor groups of people? | <p style="text-align: center;">Yes No</p> <p>If yes, check all that applies:</p> <ul style="list-style-type: none"> Physical Address Email Address Phone Number(s) GPS data Other (if other, please specify below) |
| B. Data Access | |
| 1. What types of users have access to this system or application? (Select all that apply): | <ul style="list-style-type: none"> Regular users (public access) Regular users (internal access) Technical/Operational/Administrative users Third-Party Vendors Law Enforcement Other government agencies outside the State of Hawaii jurisdiction |
| 2. How is access granted to systems and/or to PII data? | <ul style="list-style-type: none"> Internal role-based access controls (e.g. granted on behalf of the organization based on user's job duties) Public Account Creation – via Website (e.g. via “Create an account via website”, etc.) Public Account Creation – via Representative (e.g. external party aids set up account, etc.) Other (if other, please specify below) |
| 3. Does the system or application require basic user authentication (e.g. username, password/passphrase, etc.) to access the data? | <p style="text-align: center;">Yes</p> <p style="text-align: center;">No</p> |
| 3.a. If Yes, does the system or application require additional authentication (e.g. token code, etc.)? (Check all that apply) | <ul style="list-style-type: none"> Token Authentication (e.g. SMS, email, hardware, software, etc.) Phone Authentication Biometric Verification Social Identity Verification (e.g. logins via social media accounts, etc.) Security Questions Risk-based Authentication (e.g. monitoring sign-in activities via location, device, etc.) Time-based One-Time Passcode Authentication None |
| 4. Can the data be remotely accessed securely? | <p style="text-align: center;">Yes</p> <p style="text-align: center;">No</p> |
| 4.a. If Yes, what security measures are implemented? (Check all that apply) | <ul style="list-style-type: none"> Website access (e.g. HTTPS/TLS, etc.) Network access (e.g. virtual private networks, virtual desktops, etc.) Terminal access (e.g. Secure Shell access, etc.) Other (if other, please specify below) |
| 5. What controls will be used to prevent unauthorized monitoring? Check all that apply | <ul style="list-style-type: none"> Administrative (e.g. separation of duties, acceptable use policy, etc.) Technical (e.g. log analytics, etc.) Operational (e.g. routine log reviews etc.) |
| 6. Are employees and contractors trained and instructed not to solicit sensitive information when interacting with users on behalf of the agency? | <p style="text-align: center;">Yes</p> <p style="text-align: center;">No</p> |
| C. Data Retention | |
| 1. Will PI data be collected and retained until disposed? | <p style="text-align: center;">Yes</p> <p style="text-align: center;">No</p> |

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?

| | |
|--|--|
| | |
|--|--|

| | |
|--|-----------|
| 2. Is there any PII that is likely to become available to the agency through the use of the Third-Party website or application? | Yes No |
| If Yes, answer the remaining questions below. | |

| | |
|--|-----------|
| 2 a. Will REGISTRATION 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. | |

| | |
|--|-----------|
| 2 b. Will SUBMISSION PII be made available to Agency? | 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 "friend-ing," "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. | |

| | |
|--|-----------|
| 2 e. Will PII 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. | |

| | |
|---|-----------|
| 2 f. Will PII 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 | |

| | |
|--|-----------|
| 2 g. Will PII 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. | |

| | |
|--|-----------|
| 2 h. 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. | |

When you have completed all questions, save this document and email it to ipsc@hawaii.gov.

APPENDIX A: DEFINITIONS

| Rating | Definition |
|----------|--|
| Low | <ul style="list-style-type: none">• A compromise would be limited and generally acceptable for the organization, resulting in minimal monetary, productivity, or reputational losses• There would be only minimal impact on normal operations and/or business activity |
| Moderate | <ul style="list-style-type: none">• A compromise would be marginally acceptable for the organization, resulting in certain monetary, productivity, or reputational losses• Normal operations and/or business activity would be noticeably impaired, including the potential for breaches of contractual obligations |
| High | <ul style="list-style-type: none">• A compromise would be unacceptable for the organization, resulting in significant monetary, productivity, or reputational losses• The ability to continue normal operations and/or business activity would be greatly impaired, potentially resulting in noncompliance with legal or regulatory requirements and/or loss of public confidence in the organization |