Information Privacy and Security Council (IPSC)
Meeting Agenda

August 16, 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,,614645431#

I. Call to Order

II. Review and Approval of the May 17, 2023, IPSC 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. Annual Personal Information System Report; Discussion and Appropriate Action

- Updated Privacy Impact Assessment Form
- Formal Notification Procedures

V. IT Internal 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.

VI. Good of the Order

- Announcements
- Next scheduled meeting: September 20, 2023

VII. 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
May 17, 2023

Meeting was held via Microsoft Teams (videoconference interactive conferencing technology). Physical location: 1151 Punchbowl Street, Room 410, Honolulu, Hawaiʻi.

Members Present via Teams

Vincent Hoang, CISO, Chair Designee	Office of Enterprise Technology Services (ETS)
David Shak	Department of Commerce and Consumer Affairs
Jonathan Chee	Department of Education
Courtney Kinder	Department of Health
David Keane	Department of Human Resources Development
Mark Choi	Department of Human Services
Mai Nguyen Van	Judiciary
Jodi Ito	University of Hawaiʻi
Stephen Courtney	City & County of Honolulu
Matthew Iaukea	County of Hawaiʻi
Kelly Agena	County of Kauaʻi
Karen Sherman	County of Maui

Members Excused

Carol Taniguchi	Legislature

Other Attendees

Candace Park	Department of the Attorney General
Tom Ku	ETS
James Gonser	ETS
Susan Bannister	ETS
Kiyo	Public

I. Call to Order

With quorum established, Chair Hoang called the meeting to order at 1:04 p.m.

II. Review and Approval of the February 15, 2023, Meeting Minutes

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

III. Public Testimony

None.

DRAFT

IV. 2023 Legislation

- SB1178 – Update the definition of "personal information" in Chapter 487N, Hawaii Revised Statutes

  The bill did not pass. However, Chair Hoang suggested incorporating the data elements mentioned in the bill to the Privacy Impact Assessment Form.

- Other Bills – none.

V. Annual Personal Information System Report, Review and Update the Privacy Impact (PI) Assessment Form

As discussed at the last IPSC meeting, Chair Hoang recommended simplifying the PI Assessment Form to better reflect personal information impacting agencies. The form will include new data elements that would impact personal information and remove Part 3 in its entirety. With no objections, Chair Hoang will work on a draft and present it at the next meeting.

VI. Information Technology Security Controls

Chair Hoang made a motion to enter executive session pursuant to Hawai`i Revised Statutes (HRS) section 92-5(a)(6), to consider sensitive matters related to public safety or security, which was seconded by Member Ito. At 1:10 p.m. the committee went into executive session.

The committee returned to the public meeting at 2:20 p.m.

VII. Good of the Order

Next meeting on June 21, 2023.

VIII. Adjournment

With no other announcements the meeting adjourned at 2:23 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 Hawaiʻi 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 record keeping process that contains personal information and the name, personal number, or other identifying particulars of a data subject.

“Personal information” means an identifier in combination with one or more specific data elements. "Identifier" means a common piece of information related specifically to an individual that is commonly used to identify the individual across technology platforms, including:

1. A first name or initial, and last name;
2. A user name for an online account;
3. A mobile phone number; or
4. An email address specific to the individual.

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 birth date, age, geographic indicator, personal e-mail address, home address, home phone number, health records, Social Security Number (SSN), personal credit card information, security codes, unique biometric data, 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 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, security codes, unique biometric data, 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
□ Home Address
□ Security Codes or Passwords
□ Unique Biometric Data (e.g. Finger Prints)
□ Private Authentication Key
□ International Identifying Number (e.g. Social Security Number)
□ Credit Card Information
□ Financial Institution Account Information
□ Medical Information

Government Employee(s)

□ Birth date
□ Home Address
□ Security Codes or Passwords
□ Unique Biometric Data (e.g. Finger Prints)
□ Private Authentication Key
□ Hire Date
□ Performance Reviews/Evaluations
□ International Identifying Number (e.g. Social Security
□ Number Credit Card Information
□ Financial Institution Account Information
□ Medical Information
□ Salary/Compensation Information
□ Dependents or Beneficiaries

2. Approximately how much active PII records is the system storing?	● < 10,000 ○ 10,000 to 99,999 ○ 100,000 to 999,999 ○ > 1,000,000
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?	● Yes ○ No If yes, check all that applies: □ 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):	□ 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?	□ 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?	● Yes ○ No
3.a. If Yes, does the system or application require additional authentication (e.g. token code, etc.)? (Check all that apply)	□ 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?	● Yes ○ No
4.a. If Yes, what security measures are implemented? (Check all that apply)	□ 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	□ 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?	● Yes ○ No
C. Data Retention	
1. Will PI data be collected and retained until disposed?	● Yes ○ No

1.a. If PI data is retained on a system; how long is the retention period?	● < 1 year ○ 2 to 5 years ○ 6 to 10 years ○ > 10 years ○ No retention period
1.b. Is PI data retained and available offsite?	● Yes ○ No If yes, select all that best describes the back-up site: □ Local (e.g. within miles from the organization) □ U.S. Mainland □ International □ Cloud-computing environment
2. How will the data be disposed of when it is no longer needed?	□ Physical Destruction (e.g. shredding, etc.) □ Degauss (e.g. erasure of magnetic field on storage media, etc.) □ Overwrite (e.g. overwrites old data, etc.)
D. Regulatory Requirements	
1. Is any of the data subject to exclusion from disclosure under the Federal Freedom of Information Act (FOIA)?	● Yes ○ No
2. Is any of the data subject to exclusion from disclosure under the State of Hawaiʻi Uniform Information Practices Act (UIPA)?	● Yes ○ No
3. Does the system operate under a Privacy Act System of Records notice (SOR)? **If yes, provide number and name.**	● Yes ○ No
4. Is any of the data subject to any other regulatory requirements? **If yes, provide number and name**	● Yes ○ No

E. Business Impact Analysis Refer to APPENDIX A: DEFINITIONS for Low, Moderate, and High ratings in this questionnaire	
1. Rate the overall *confidentiality* needs (the consequences of unauthorized disclosure or compromise of data stored, processed, or transmitted by the resource) of the information resource:	● Low ○ Moderate ○ High
2. Rate the overall *integrity* needs (the consequences of unauthorized modification/destruction or compromise of data stored, processed, or transmitted by the resource) of the information resource:	● Low ○ Moderate ○ High
3. Rate the overall *availability* needs (the consequences of loss or disruption of access to data the resource stores, process, or transmits) of the information resource to its internal users (excluding access to support the application or system itself):	● Low ○ Moderate ○ High
4. Rate the overall *availability* needs (the consequences of loss or disruption of access to data the resource stores, process, or transmits) of the information resource to general public users:	● Low ○ Moderate ○ High
5. Rate the overall *accountability* needs (the consequences of the inability or compromised ability to hold users accountable for their actions in the resources) of the information resource to its internal users:	● Low ○ Moderate ○ High
6. Rate the overall *accountability* needs (the consequences of the inability or compromised ability to hold users accountable for their actions in the resources) of the information resource to its general public users:	● Low ○ Moderate ○ High
7. Rate the overall *reputational* damage to the agency if it was known that the information resource has been breached or compromised?	● Low ○ Moderate ○ High