Information Privacy and Security Council
Meeting Agenda
November 18, 2020
1:00 p.m.

Virtual Meeting via Webex

Members of the public may request access for the virtual meeting link by e-mailing: ets@hawaii.gov, Subject line: *IPSC Meeting*, by November 16, 2020, 11:00 a.m.

I. Call to Order

II. Review and Approval of the September 16, 2020 Meeting Minutes

III. Public Testimony on Agenda Items

Any person may submit testimony on any agenda item. Members of the public may give oral testimony at the meeting or submit written testimony via e-mail to ets@hawaii.gov, Subject line: *IPSC Testimony*. Each individual or representative of an organization is allotted three minutes for testimony.

IV. Draft of Annual Summary Report to the Legislature; Discussion and Appropriate Action

V. Annual Personal Information System Report; Discussion and Appropriate Action
- Proposed Revision to Privacy Impact Assessment (PIA) Form

VI. Good of the Order
- Announcements
- Next meeting: To be determined

VII. Adjournment

Information Privacy and Security Council (IPSC)
Meeting Minutes - DRAFT
September 16, 2020

Videoconference meeting via Webex

Members Present

Vince Hoang, Chair	Office of Enterprise Technology Services (ETS)
David Shak	Department of Commerce and Consumer Affairs (DCCA)
Jonathan Chee	Department of Education (DOE)
Gino Merez	Department of Health (DOH)
Kevin Thornton	Judiciary
Jodi Ito	University of Hawai‘i (UH)
Jules Ung	County of Hawai‘i

Members Excused

David Keane	Department of Human Resources Development (DHRD)
Louis “Jack” Giardina	Department of Human Services (DHS)
Carol Taniguchi	Legislature
Mark Wong	City & County of Honolulu
Nyree Norman	County of Kaua‘i
Karen Sherman	County of Maui

Other Attendees

Candace Park	Department of the Attorney General (ATG)
Sal Nicosia	ETS
Janey Yamashita	ETS

I. Call to Order

Quorum was established and Chair Hoang called the meeting to order at 1:01 p.m.

II. Review and Approval of the July 15, 2020 Meeting Minutes

Chair Hoang called for a motion to approve the minutes. Member Thornton made a motion to approve the meeting minutes, which was seconded by Member Hoang. A vote was taken, and the motion passed unanimously.

III. Public Testimony on Agenda Items

None.

IV. House Bill 2572 HD2 SD1, Relating to Privacy

HB 2572 HD2 SD1 had progressed in the 2020 legislative session but died at the end. Chair Hoang asked if the IPSC has comments, proactively, should another bill be introduced in an upcoming session. Member Sherman had offered to review the bill and offer guidance but was unable to attend today.

DRAFT

Member Ito asked if the bill died due to the abbreviated session or its extensiveness. Chair Hoang surmised it was a combination, and thought the bill would have been more likely to pass if limited to the definition amendments for HRS §487N-1.

Chair Hoang noted the bill became an omnibus, addressing larger issues and other statutes, including areas of commerce and law enforcement, and reached far beyond the scope of the IPSC per HRS §487N-5.

Chair Hoang agreed that the definitions in HRS §487N-1 need updating, and those updates would provide for better accountability.

V. Personal Information System Annual Report

Chair Hoang said moving forward, reports would be collected in portable document format (pdf) for simplification and for both transmitting and receiving parties to maintain copies. He noted reports were received from the legislature and the counties of Maui, Hawaii, and Honolulu; and two executive department reports remain due.

Chair Hoang asked if there were any comments, and there were none.

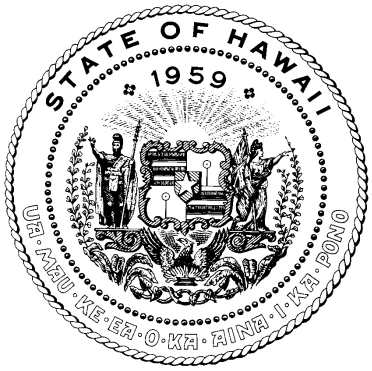
VI. Good of the Order

a. Announcements: Member Ito noted that Chair Hoang will be a panel participant at the Interface Hawaii event, talking about cyber considerations during a pandemic. Chair Hoang noted that Member Ito is the panel moderator.

b. Next meeting: November 18, 2020.

VII. Adjournment

The meeting adjourned at 1:16 p.m.



INFORMATION AND PRIVACY SECURITY COUNCIL

ANNUAL SUMMARY REPORT

DECEMBER 18, 2020

SUBMITTED TO

THE STATE LEGISLATURE

Information Privacy and Security Council
Annual Summary Report
December 18, 2020

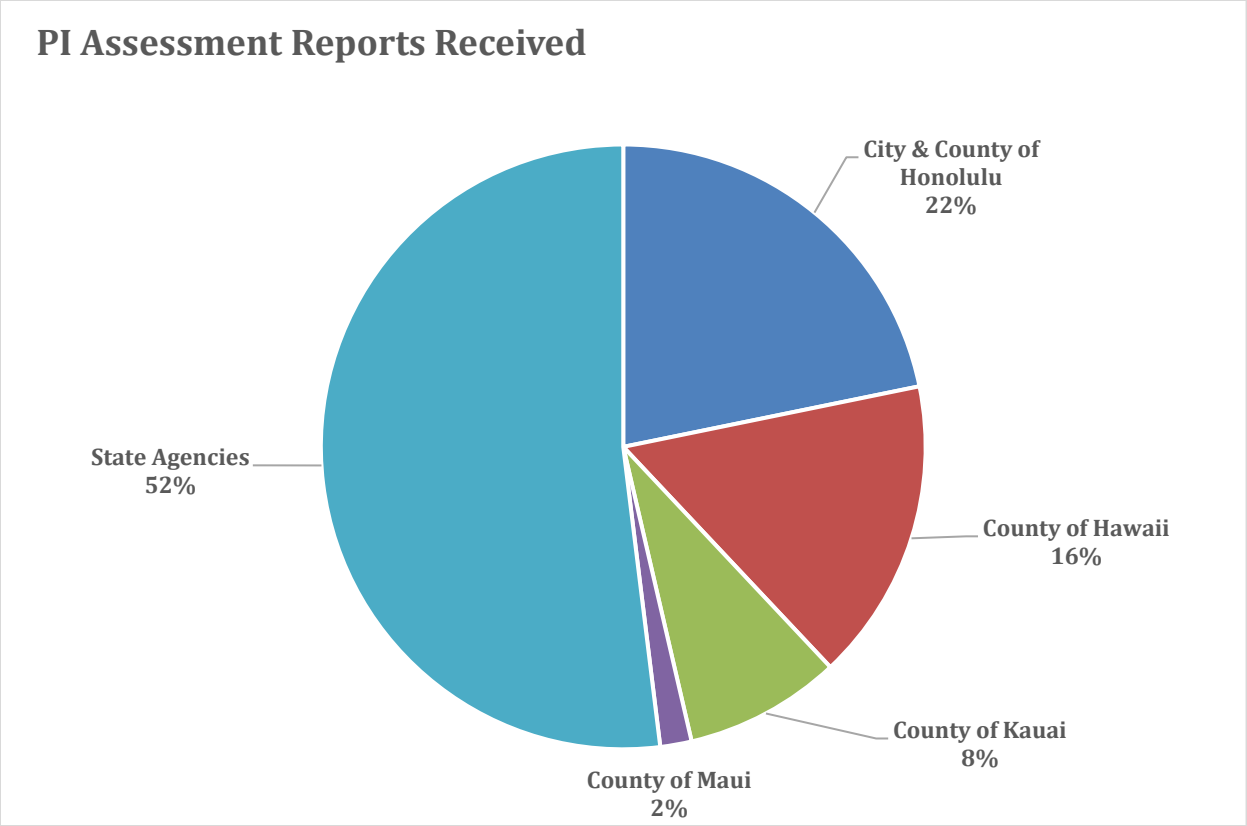
The Information Privacy and Security Council (IPSC) submits the following summary report on the existence and character of government agencies' personal information (PI) systems, pursuant to section 487N-5(d), Hawaii Revised Statutes (HRS).

The IPSC has received the individual annual reports submitted by government agencies of the State of Hawaii, City and County of Honolulu, Hawaii County, Maui County, and Kauai County, in accordance with HRS section 487N-7. Enclosed are the council's findings and summary of recent legislation to protect PI handled by government agencies.

BACKGROUND

Any State or local government agency that maintains one or more personal information systems is required under section 487N-7, Hawaii Revised Statute (HRS), to submit to the IPSC an annual report on the existence and character of each PI system added or eliminated since the agency's previous annual report.

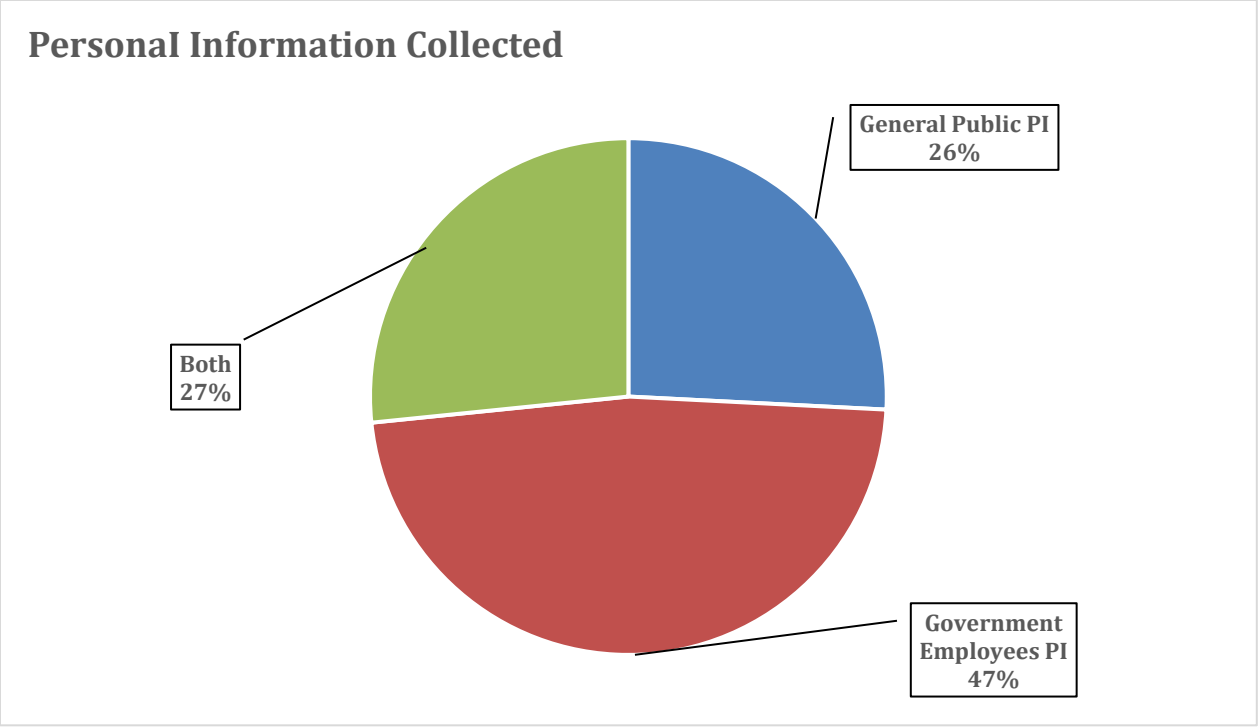
The IPSC continued with the "paperless" method of reporting to all jurisdictions and departments. All agencies had the option of using the IPSC's Privacy Impact Assessment (PIA) fillable PDF, accessible to agencies through the IPSC website (ipsc.hawaii.gov), to comply with their reporting requirement.



GENERAL STATISTICS

We continue to see a decrease in the number of reports received from various government agencies in the State of Hawaii. There was a total of **153** submissions this year compared to **191** from last year. The State of Hawaii government system (comprising of the Executive, Legislature, and Judiciary branches), continue to submit the most PI systems.

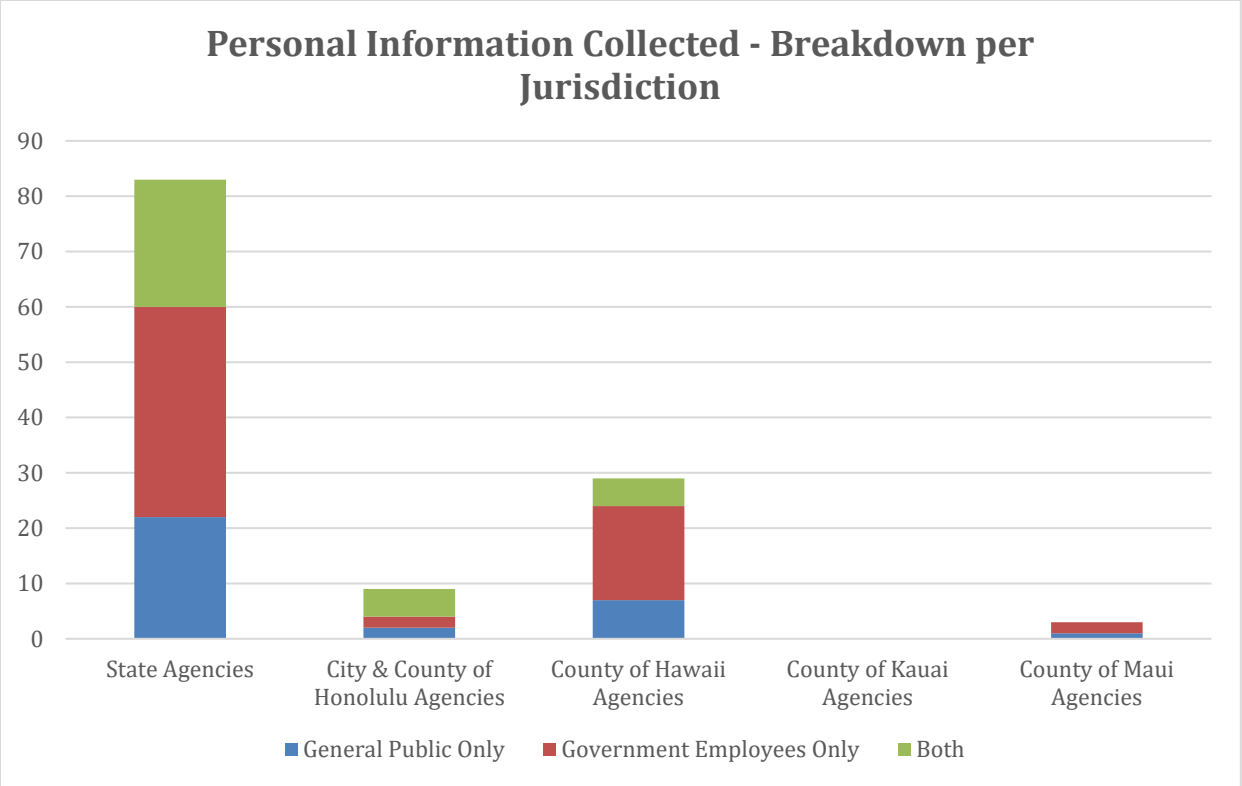
Total Reports Received in 2019	**153**
Report Submitted by State Agencies	**93**
Report Submitted by City & County of Honolulu Agencies (CCH)	**13**
Report Submitted by County of Hawaii Agencies (COH)	**29**
Report Submitted by County of Kauai Agencies (COK)	**15**
Report Submitted by County of Maui Agencies (COM)	**3**



PERSONAL INFORMATION (PI) COLLECTION

Of the **153** reports received this year, **32** agencies have reported that they only collect personal information from the general public while **59** agencies reported that they only collect personal information on government employees. **33** agencies have reported that they collect personal information from both the general public and government employees while the remaining agencies did not provide an answer or does not collect personal information at all.

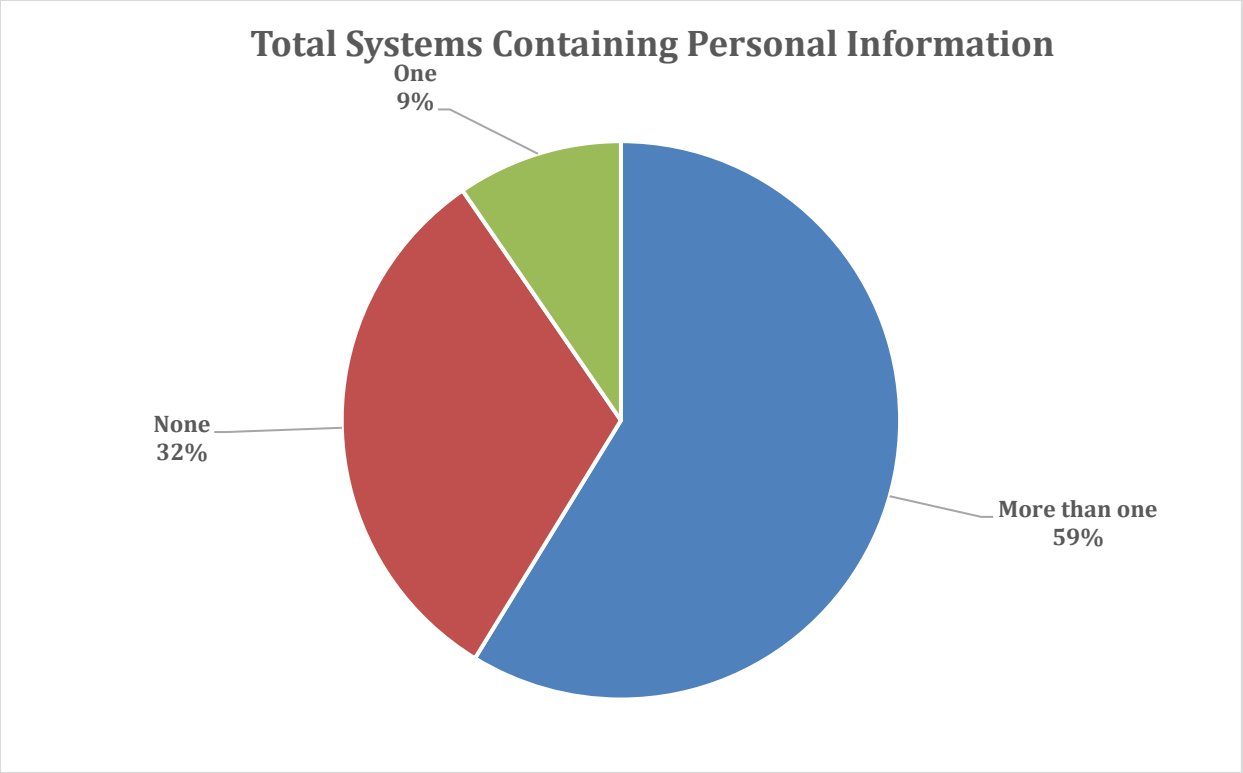
Agencies Reporting Systems Collecting Personal Information only on the General Public	**32**
Agencies Reporting Systems Collecting Personal Information only on the Government Employees	**59**
Agencies Reporting Systems Collecting Both	**33**



	General Public Only	Government Employees Only	Both
State Agencies	**22**	**38**	**23**
City & County of Honolulu Agencies	**2**	**2**	**5**
County of Hawaii Agencies	**7**	**17**	**5**
County of Kauai Agencies	**0**	**0**	**0**
County of Maui Agencies	**1**	**2**	**0**

State agencies continue to collect the most personal identifiable information from either the general public (**22 agencies**) or (**38 agencies**) government employees, or both (**23 agencies**).

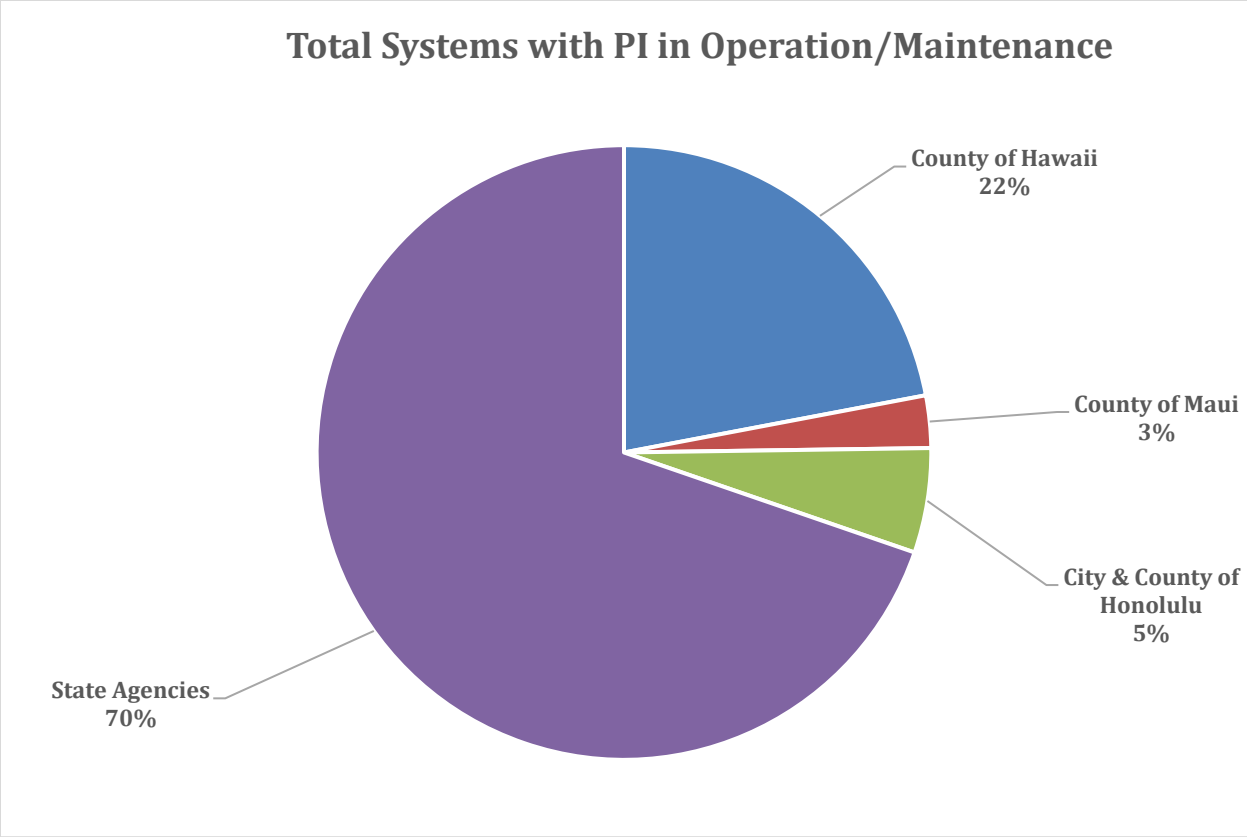
No agencies from both the County of Kauai have reported that they do not have a system containing both types of PII; general public and government employees. Only one agency from the County of Maui only collect from the general public and **2** agencies only collect PII from government employees. The remaining agencies that submitted a PIA report this year have not answered the following qualifying question(s).



Reference: *Annual Personal Information System Report – Privacy Impact Assessment (PIA) Part II Section A. Question 1.b.*

TOTAL SYSTEMS CONTAINING PERSONAL INFORMATION

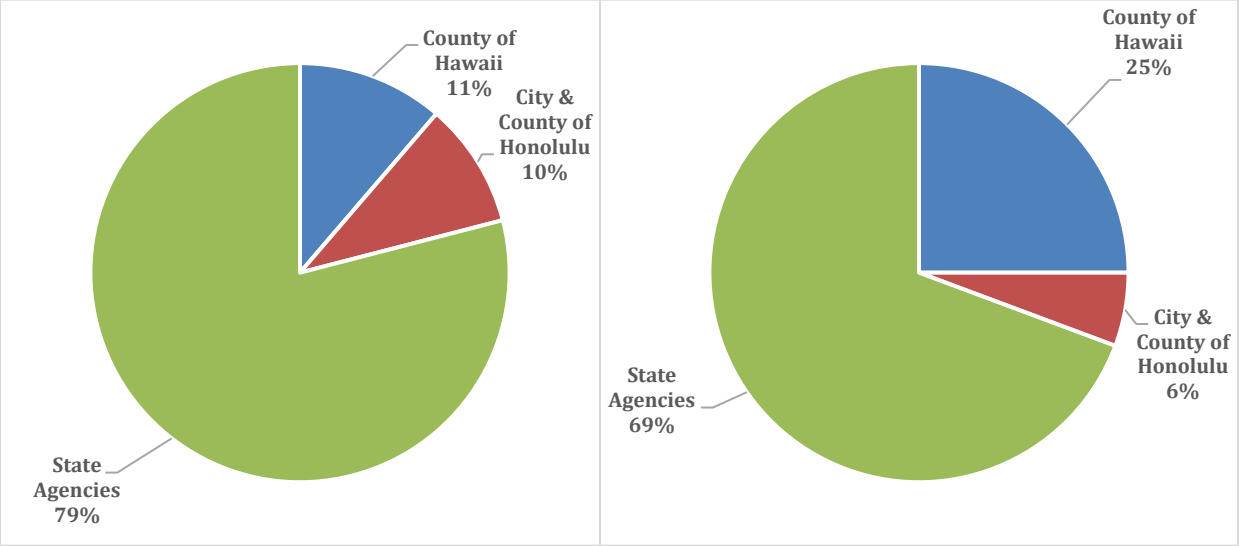
	None	One	More than One
State Agencies	11	12	56
City & County of Honolulu Agencies	5	0	8
County of Hawaii Agencies	23	5	23
County of Kauai Agencies	14	0	14
County of Maui Agencies	0	0	3



Reference: *Annual Personal Information System Report – Privacy Impact Assessment (PIA) Part II Section A. Question 1.c.*

SYSTEMS WITH PERSONAL INFORMATION IN OPERATION/MAINTENANCE

State Agencies	**80**
City & County of Honolulu Agencies	**11**
County of Hawaii Agencies	**36**
County of Kauai Agencies	**0**
County of Maui Agencies	**4**



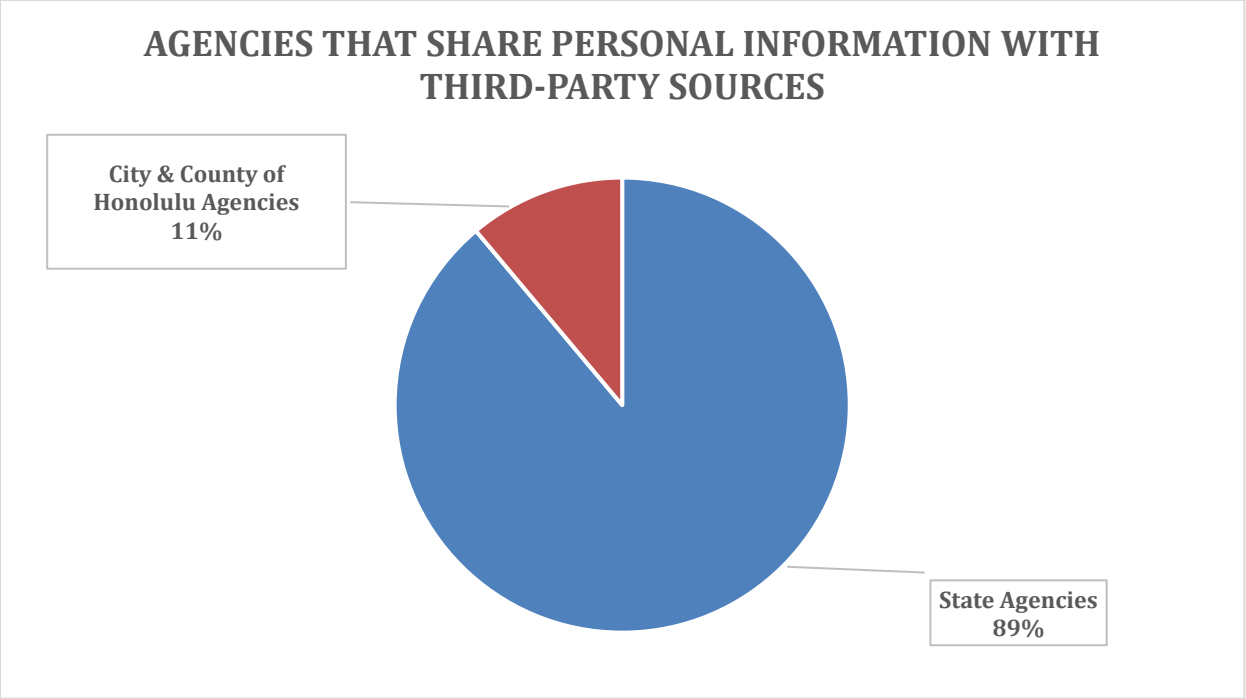
Reference: (**Left**) Systems excluded from FOIA (*Annual Personal Information System Report – Privacy Impact Assessment Part II Section B. Question 1.b.*); (**Right**) Systems excluded from UIPA (*Annual Personal Information System Report – Privacy Impact Assessment Part II Section B. Question 1.c.*)

SYSTEMS EXCLUDED FROM THE FREEDOM OF INFORMATION ACT (FOIA) AND THE UNIFORM INFORMATION PRACTICE ACT (UIPA)

	FOIA	UIPA
State Agencies	49	61
City & County of Honolulu Agencies	6	5
County of Hawaii Agencies	7	22
County of Kauai Agencies	0	0
County of Maui Agencies	0	0

ACCESS TO THE DATA

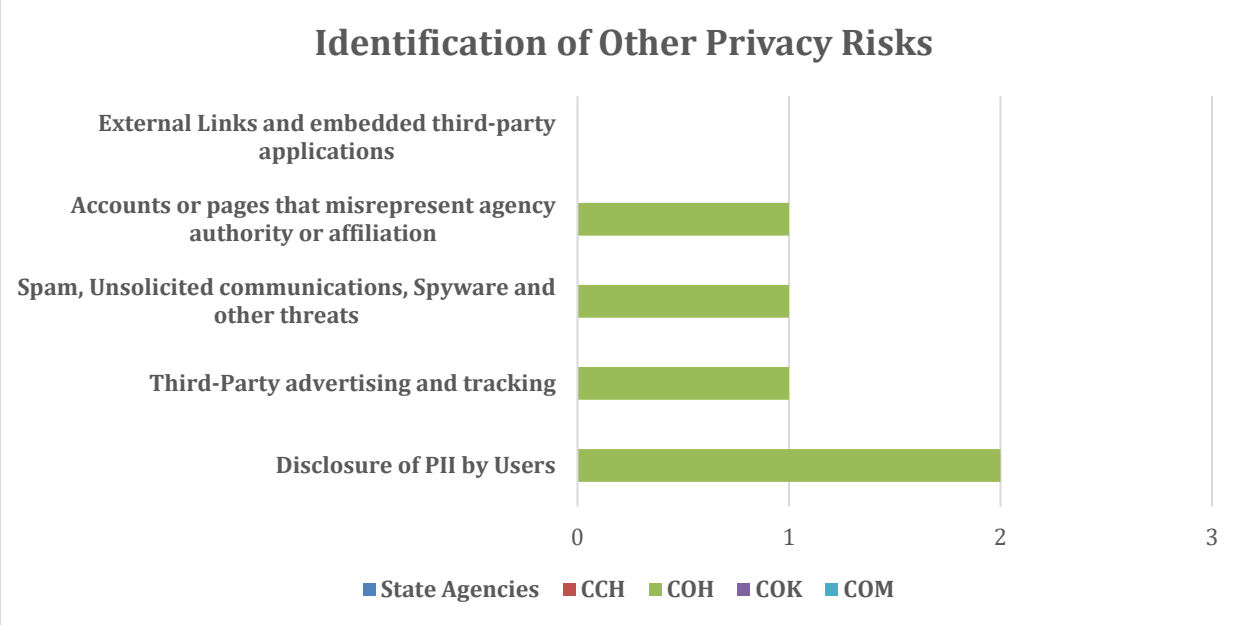
Of the **153** reports received, **62** agencies have reported that their data are subject to exclusion from disclosure under the Federal Freedom of Information Act (FOIA). In addition, **88** agencies reported their data is also subject to exclusion from disclosure under the State of Hawaii Uniform Information Practices Act (UIPA).



AGENCIES THAT SHARE PERSONAL INFORMATION WITH THIRD-PARTY SOURCES

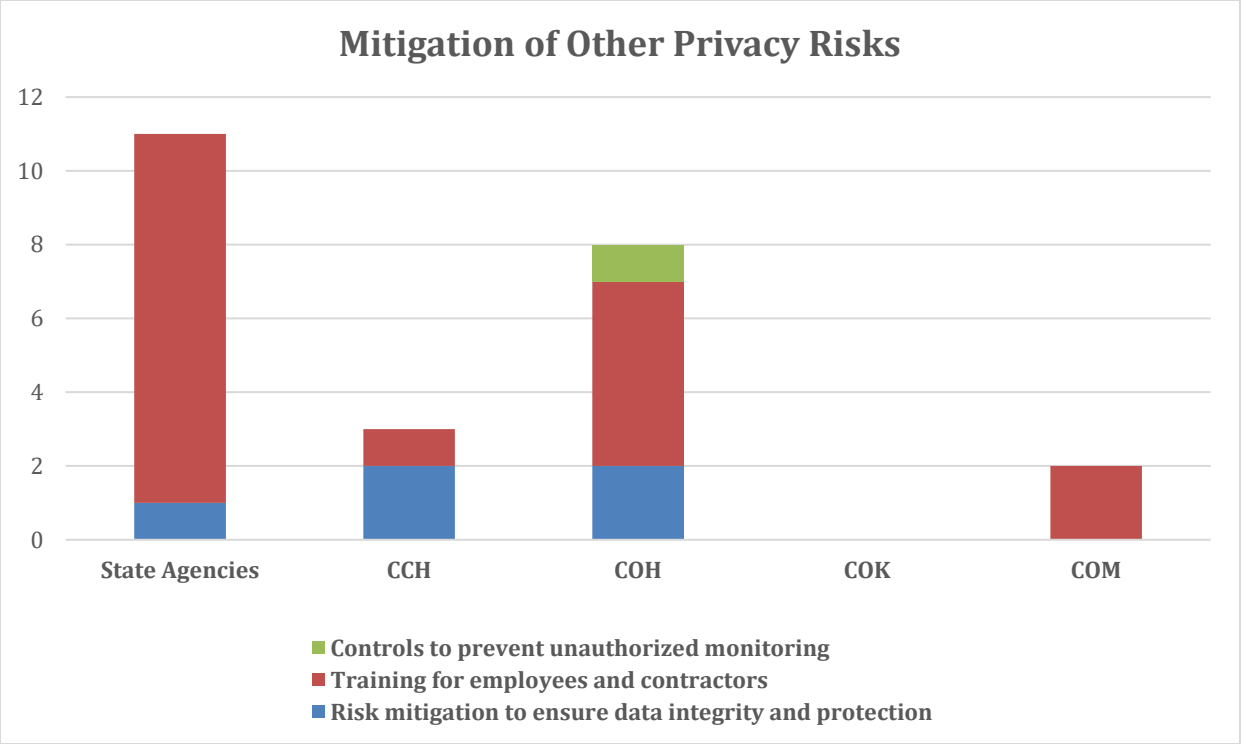
State Agencies	24
City & County of Honolulu Agencies	3
County of Hawaii Agencies	0
County of Kauai Agencies	0
County of Maui Agencies	0

IDENTIFICATION AND MITIGATION OF OTHER PRIVACY RISKS: SHARING AND DISCLOSURE OF PII



IDENTIFICATION OF OTHER PRIVACY RISKS

	State Agencies	CCH	COH	COK	COM
Disclosure of PII by Users	0	0	2	0	0
Third-Party advertising and tracking	0	0	1	0	0
Spam, Unsolicited communications, Spyware and other threats	0	0	1	0	0
Accounts or pages that misrepresent agency authority or affiliation	0	0	1	0	0
External Links and embedded third-party applications	0	0	0	0	0
Monitoring future requirements and future technology	0	0	0	0	0



MITIGATION OF OTHER PRIVACY RISKS

	State Agencies	CCH	COH	COK	COM
Risk mitigation to ensure data integrity and protection	1	2	2	0	0
Training for employees and contractors	10	1	5	0	2
Controls to prevent unauthorized monitoring	0	0	1	0	0

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

Asset Name:	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:	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. Briefly describe the purpose of this system?

1.a. Please specify the data used or collected (select all that apply):

General Public

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

Government Employee(s)

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

3. What is the volume of data records that resides on the system?	( ) < 10,000	( ) 10,000 to 49,999
	( ) 50,000 to 499,999	( ) > 500,000
4. What stage of the life cycle is the system currently in? Select one.	( ) Design/Planning	( ) Development/Implementation
	( ) Operation/Maintenance	( ) Disposal/Decommissioned

5. What are the sources of the information in the system? Describe where the system data originates (select all that apply):	( ) Provided/inputted by the user ( ) Entered on behalf of the user by an internal staff or third-party source ( ) Programmatically from another system.
6. Does the system collect, process, send, or retrieve information from external information systems and/or data sources (select all that apply):	( ) 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)
7. 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)
8. 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? (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. Are role-based access controls implemented to restrict access, modification, or misuse of the data stored in the system? If yes, please describe	
3. 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.)
4. Have employees and contractors been trained and instructed not to solicit sensitive information when interacting with users on behalf of the agency?	( ) Yes ( ) No
C. Data Retention	
1. Will data be collected and used for a one-time process or will be retained until disposed? If 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
2. How will the data be disposed of when it is no longer needed? Provide a brief explanation of the data disposal process	
D. Regulatory Requirements	
1. Is any of the data subject to exclusion from disclosure under the Federal Freedom of Information Act (FOIA)?	
2. Is any of the data subject to exclusion from disclosure under the State of Hawai'i Uniform Information Practices Act (UIPA)?	
3. Does the system operate under a Privacy Act System of Records notice (SOR)? ( ) Yes ( ) No If yes, provide number and name.	
4. Is any of the data subject to any other regulatory requirements? ( ) Yes ( ) No If yes, provide number and name	.

E. Business Impact Analysis	
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:	( ) High ( ) Moderate ( ) Low
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:	( ) High ( ) Moderate ( ) Low
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):	( ) High ( ) Moderate ( ) Low
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**:	( ) High ( ) Moderate ( ) Low
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**:	( ) High ( ) Moderate ( ) Low
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**:	( ) High ( ) Moderate ( ) Low

7. Rate the overall ***reputational*** damage to the agency if it was known that the information resource has been breached or compromised?	( ) High ( ) Moderate ( ) Low

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 there any PII that is likely to become available to the agency through the use of the Third-Party website or application? If Yes, answer the remaining questions below.	( ) Yes or ( ) No
2 a. Will REGISTRATION PII be made available to Agency? 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 or ( ) No
2 b. Will SUBMISSION PII be made available to Agency? 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.	( ) Yes or ( ) No
2 c. Will ASSOCIATION PII be made available to Agency? 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.	( ) Yes or ( ) No
2 d. Will ACCOUNT PII be made available to Agency? 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.	( ) Yes or ( ) No
2 e. Will PII be subjected to Public interaction/open government activities use? This could include surveys, contests, or message boards that provide a forum for the public to comment on the agency's activities.	( ) Yes or ( ) No
2 f. Will PII be subjected to Recruitment and/or employee outreach use? 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	( ) Yes or ( ) No
2 g. Will PII be subjected to Participation in agency programs or systems use? 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.	( ) Yes or ( ) No
2 h. PII will be subjected to Web measurement and/or customization use? The agency may use third-party websites or applications to conduct measurement and analysis of web usage, or to customize the user's experience.	( ) Yes or ( ) No
When you have completed all questions, save this document and email it to ipsc@hawaii.gov.	