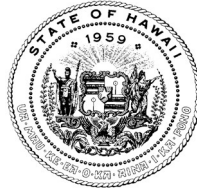DEPT. COMM. NO. 236

DOUGLAS MURDOCK
CHIEF INFORMATION OFFICER

OFFICE OF ENTERPRISE TECHNOLOGY SERVICES

P.O. BOX 119, HONOLULU, HI 96810-0119

November 25, 2022

The Honorable Ronald D. Kouchi
President of the Senate
  and Members of the Senate
Thirty-Second State Legislature
State Capitol, Room 409
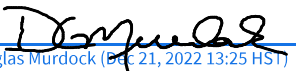Honolulu, Hawaiʻi 96813

The Honorable Scott K. Saiki
Speaker of the House, and Members of the
  House of Representatives
Thirty-Second State Legislature
State Capitol, Room 431
Honolulu, Hawaiʻi 96813

Dear President Kouchi, Speaker Saiki, and Members of the Legislature:

On behalf of the Information Privacy and Security Council, which is assigned to the Department of Accounting and General Services and chaired by the State Chief Information Officer, the Office of Enterprise Technology Services respectfully submits the attached Annual Summary Report on the government agencies' personal information systems, pursuant to HRS section 487N-5(d).

In accordance with HRS section 93-16, this report may be viewed electronically at http://ipsc.hawaii.gov/ .

Sincerely,

Douglas Murdock (Dec 21, 2022 13:25 HST)

Douglas Murdock
Chief Information Officer

Attachment
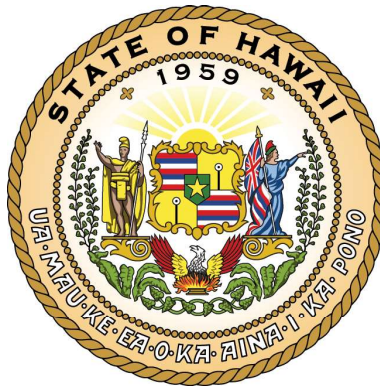
INFORMATION PRIVACY AND SECURITY COUNCIL

ANNUAL SUMMARY REPORT

November 25, 2022

SUBMITTED TO

THE THIRTY-SECOND STATE LEGISLATURE

Information Privacy and Security Council
Annual Summary Report
November 25, 2022

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
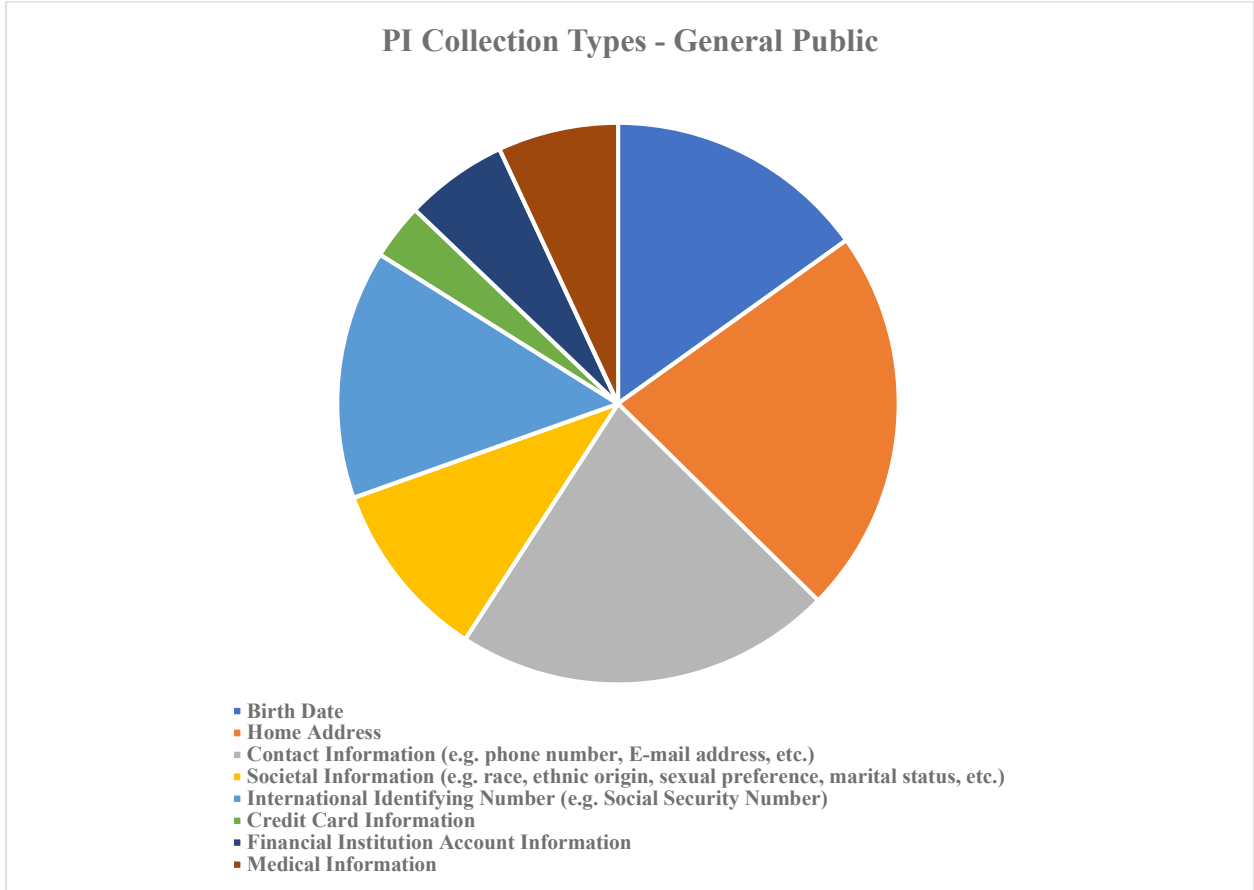
There was a total of **286** reports submitted this year. Of the total reports collected, **25%** were new submissions, while the remaining were existing submissions from the year prior. There was an increase in reports collected this year.

PI Reports Collected per Jurisdiction

- County of Hawaii
- County of Kauai
- County of Maui
- City & County of Honolulu
- State of Hawaii Government, Executive Branch
- State of Hawaii Government, Legislative Branch
- State of Hawaii Government, Judiciary Branch
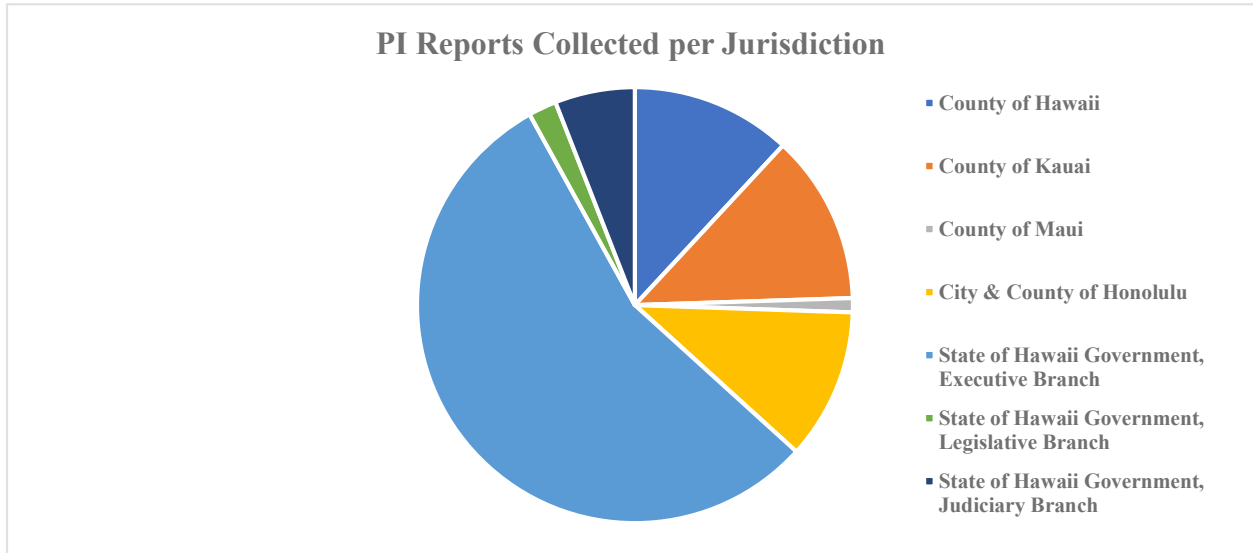
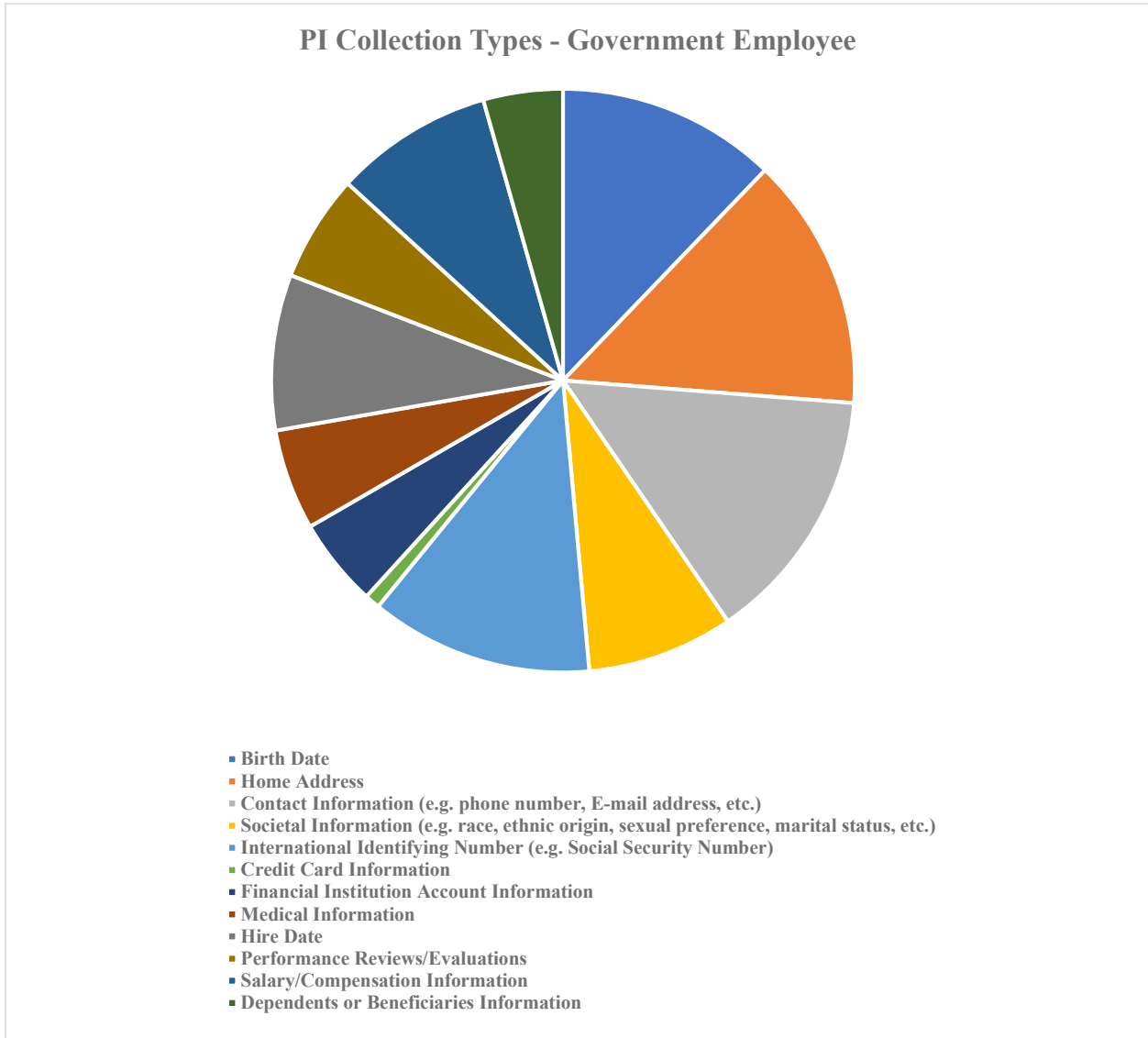|		
Total Reports Received in 2022	286	
County of Hawaii	34	12%
County of Kauai	36	13%
County of Maui	3	1%
City & County of Honolulu	32	11%
State of Hawaii Government, Executive Branch	15	55%
State of Hawaii Government, Legislative Branch	6	2%
State of Hawaii Government, Judiciary Branch	17	6%

Data Usage
General Public Information

Based on the responses from agencies that collect information from the General Public, the following types of PI are being collected:

PI Collection Types - General Public

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

|	
Birth Date	15%
Home Address	22%
Contact Information (e.g. phone number, E-mail address, etc.)	22%
Societal Information (e.g. race, ethnic origin, sexual preference, marital status, etc.)	10%
International Identifying Number (e.g. Social Security Number)	14%
Credit Card Information	3%
Financial Institution/Account Information	6%
Medical Information	7%

Government Employee Information

Based on the responses from agencies that collect information from Government Employees, the following types of PI are being collected:

PI Collection Types - Government Employee

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

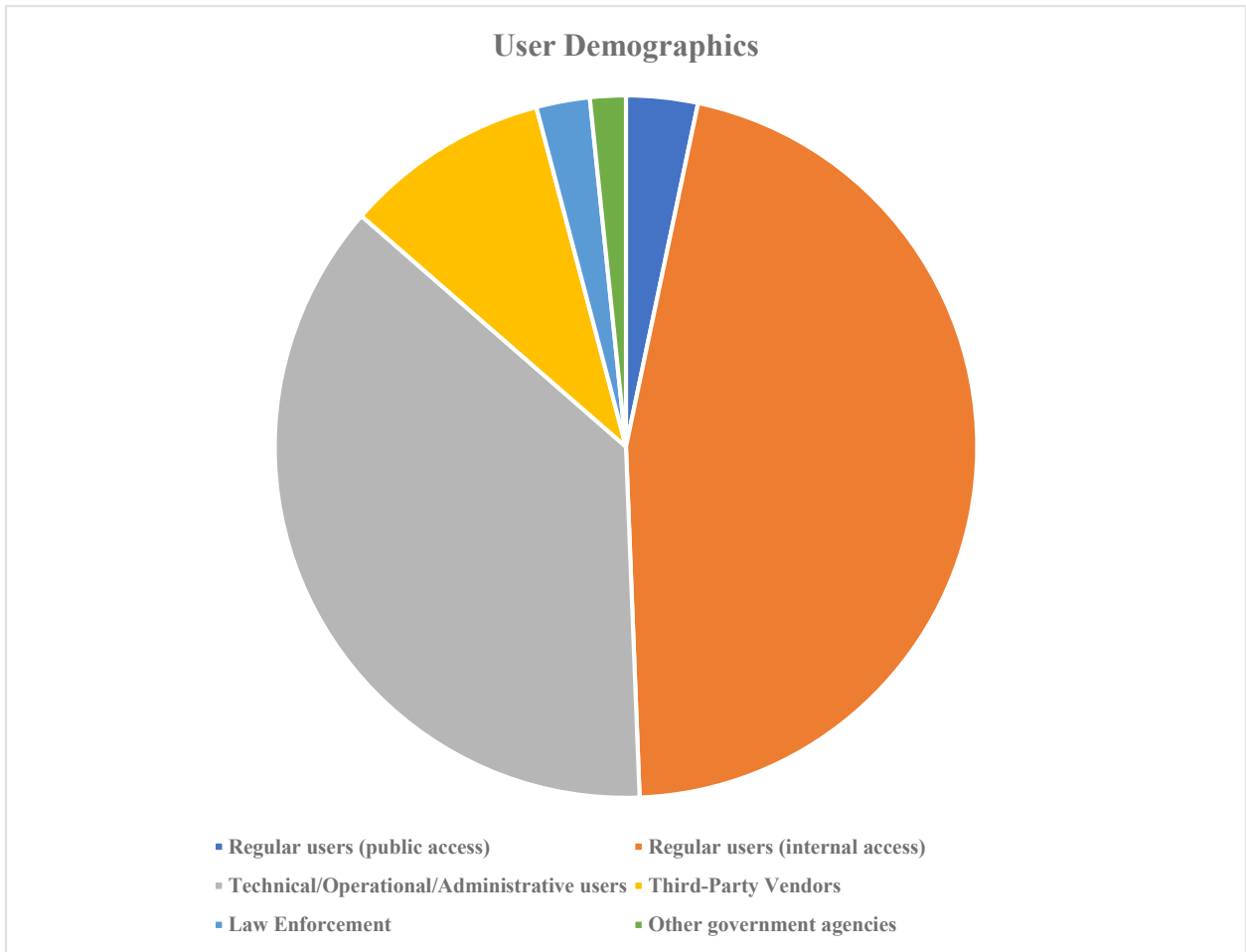|	
Birth Date	12%
Home Address	14%
Contact Information (e.g. phone number, E-mail address, etc.)	14%
Societal Information (e.g. race, ethnic origin, sexual preference, marital status, etc.)	8%
International Identifying Number (e.g. Social Security Number)	12%
Credit Card Information	1%
Financial Institution/Account Information	5%
Medical Information	6%
Hire Date	9%
Performance Reviews/Evaluations	6%
Salary/Compensation Information	9%
Dependents or Beneficiaries Information	4%

Data Volume

Below summarizes the volume of data being collected and stored by State of Hawaii government agencies. The graph and table summarize the volume by reporting agency.

Volume of Data

- Less than 10,000
- 10,000 to 49,999
- 50,000 to 499,999
- Greater than 500,000
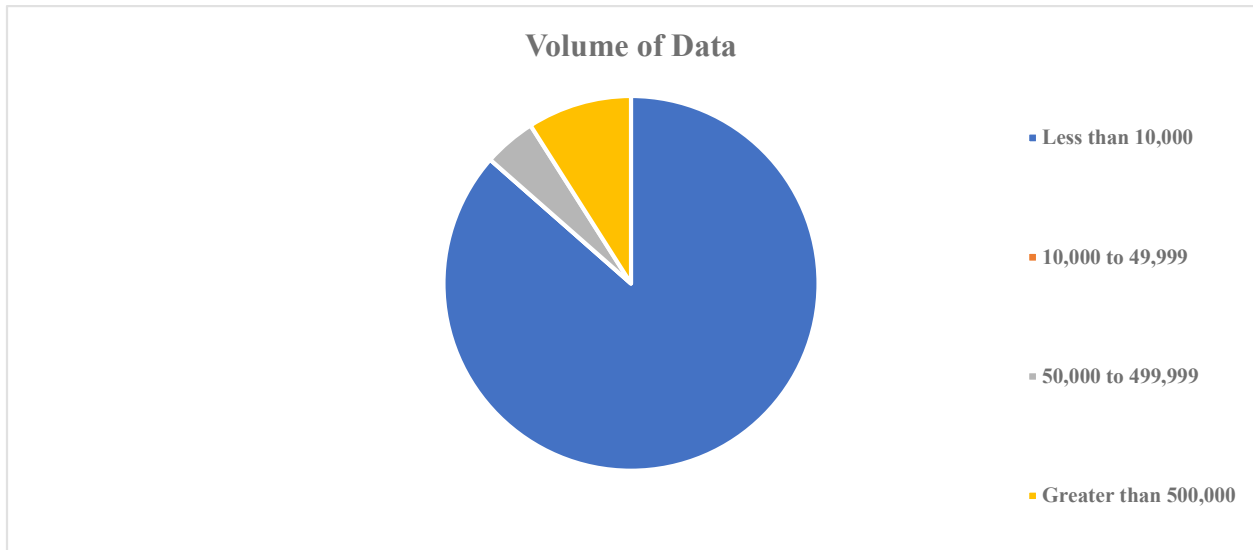
Less than 10,000	86%
10,000 to 49,999	0%
50,000 to 499,999	4%
Greater than 500,000	9%

Demographics

The following table and graph summarize the demographics of the types of users accessing and handling personal information.

User Demographics

Legend:
- Regular users (public access)
- Regular users (internal access)
- Technical/Operational/Administrative users
- Third-Party Vendors
- Law Enforcement
- Other government agencies

|	
Regular users (public access)	**3%**
Law Enforcement	**2%**
Other government agencies	**2%**
Regular users (internal access)	**46%**
Third-Party Vendors	**9%**
Technical/ Operational/ Administrative users	**37%**

Access and Authentication

The collection summarized that there are **145** systems accessible via website **(7%)**, internal network via a virtual private connection **(89%)**, or terminal access **(4%).** On average, **115** systems require basic authentication (e.g. username and password). Out of the general population, **34%** agency systems reported required an additional form of authentication (multi-factor authentication) while **68%** of agencies systems reported it was not required. Common multi-factor authentications are as followed:
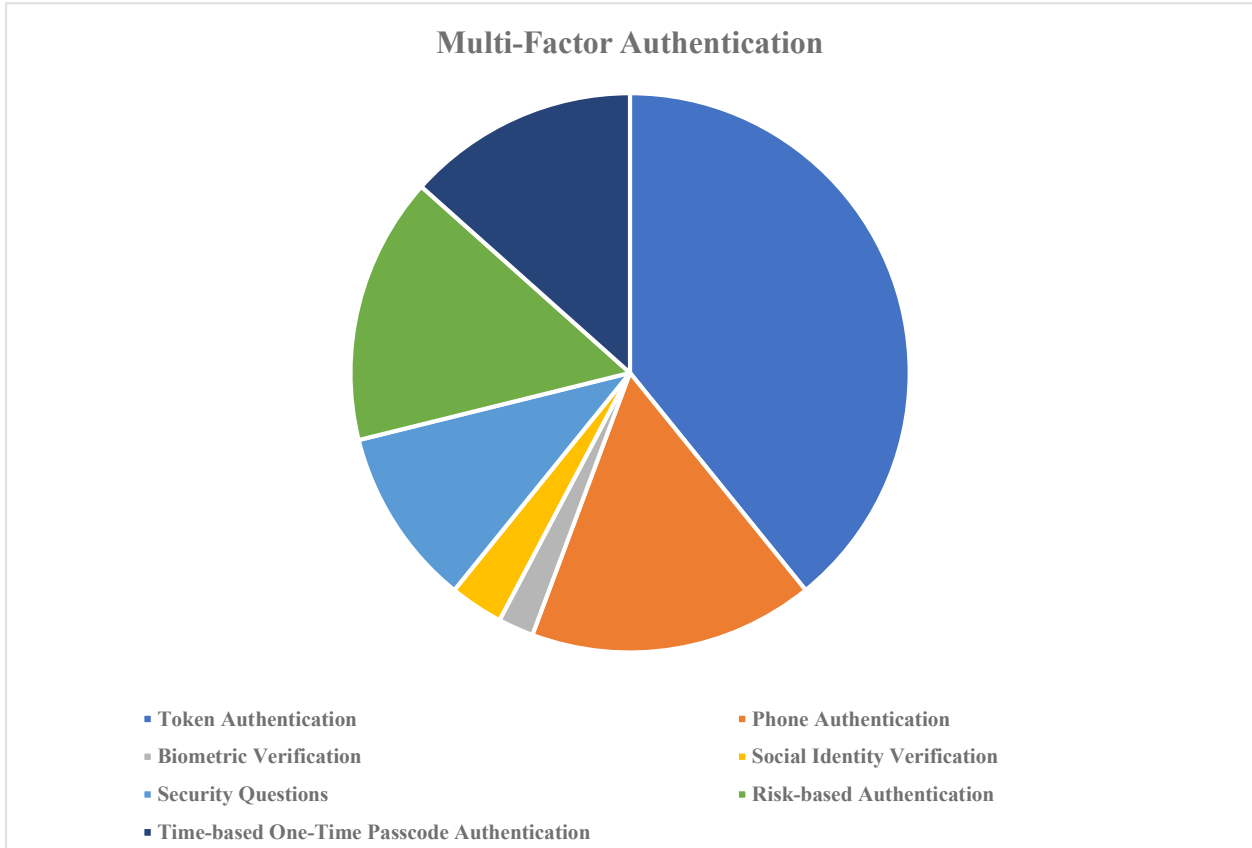
Token Authentication	39%
Phone Authentication	16%
Biometric Verification	2%
Social Identity Verification	3%
Security Questions	10%
Risk-based Authentication	15%
Time-based One-Time Passcode Authentication	13%

Retention and Storage

There are **50** systems that are designed to have information to be stored offsite (e.g. outside of the reporting agencies building premise). **48%** stated that they back-up personal information locally within vicinity of the agency, **12%** reported storing information in U.S. Mainland locations while **58%** of agencies back-up their information to cloud environments. No agencies reported storing information in international locations. From the general reporting population, **95 (65%)** reported that the system does not have a retention period while the remaining responses stated that they have a retention period.

Data Retention

■ Less than 1 year   ■ 2 to 5 years   ■ 6 to 10 years   ■ More than 10 years   ■ No retention period
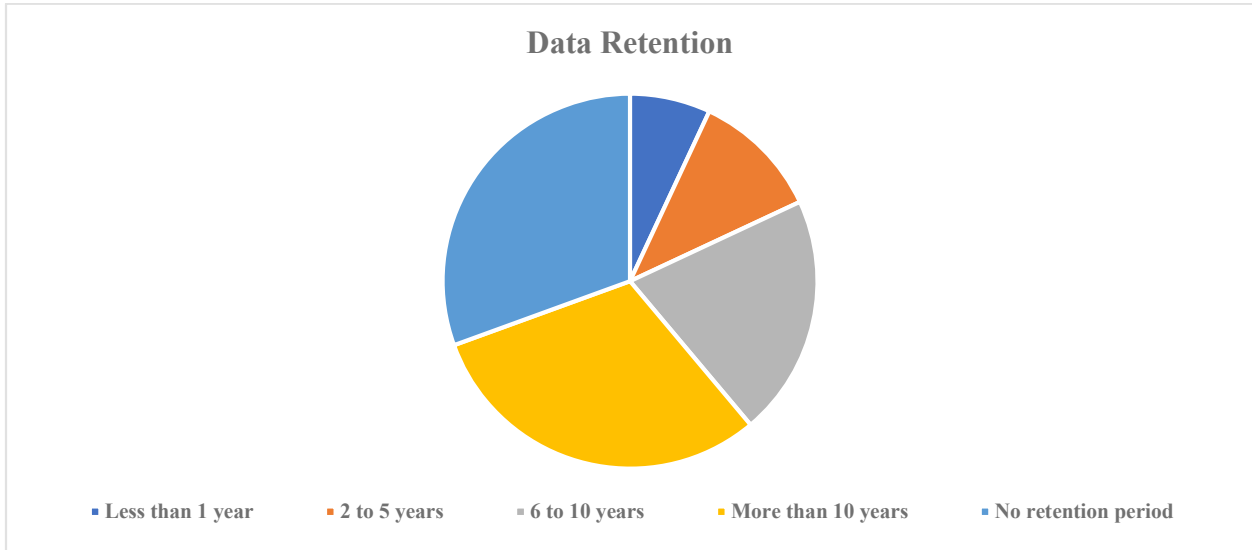
Less than 1 year	7%
2 to 5 years	11%
6 to 10 years	21%
More than 10 years	31%
None	31%