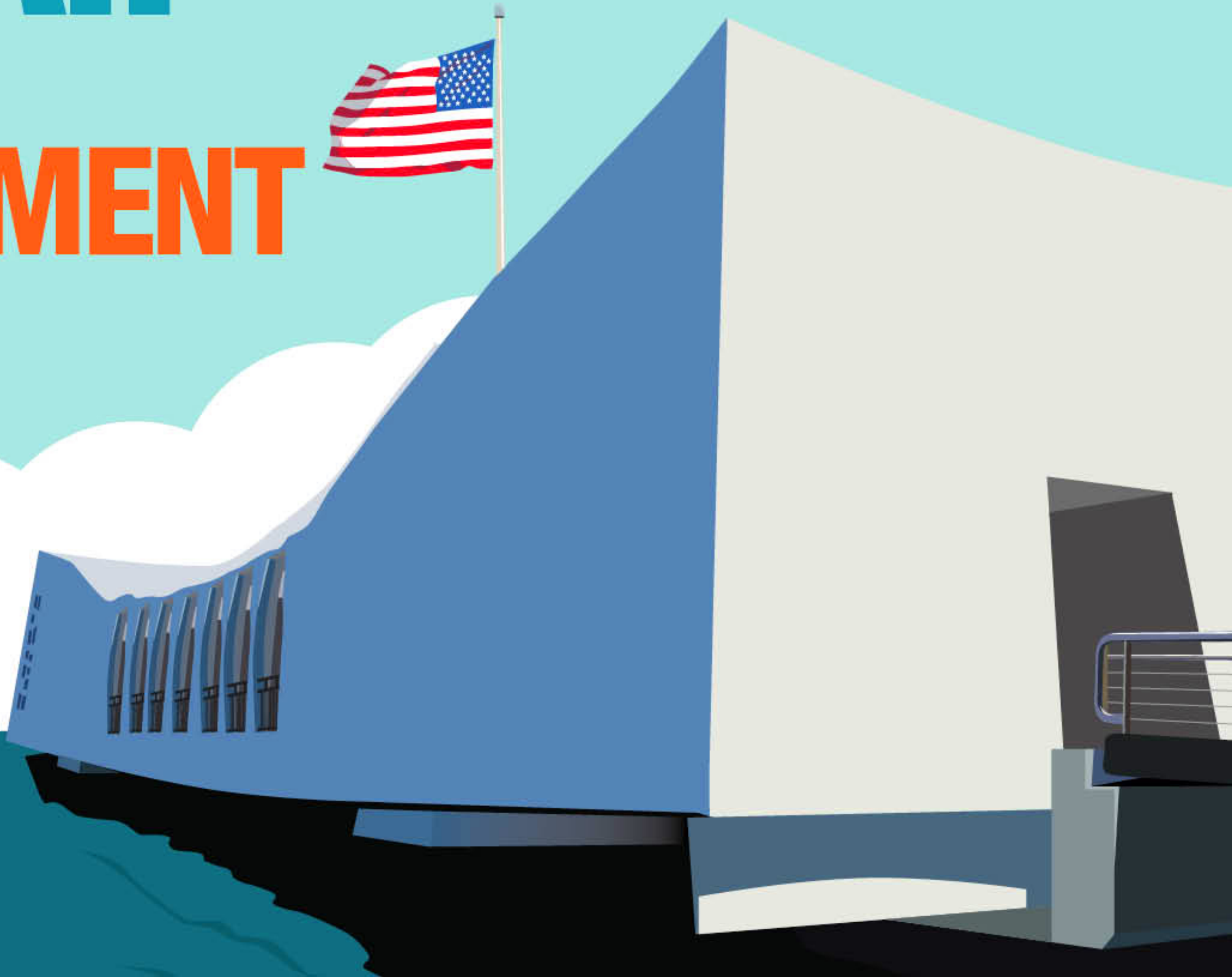
GOVERNMENT TECHNOLOGY®

HAWAII DIGITAL GOVERNMENT SUMMIT

HONOLULU
HAWAII
NOVEMBER
TWENTY-FIRST
2013



Session T7: Improving State Security and Privacy

Hawaii, like most states, has specific laws, regulations and executive orders that govern the protection of personal information. Compliance is much more than just a technology issue - it is also a matter of organization-wide policies and processes necessary to safeguard private information. This session will clarify requirements, standards, strategies and the varying legal drivers for security that apply to state agencies, municipalities and their private sector contractors.

Panel Members

Jodi Ito – Information Security Officer, University of Hawaii

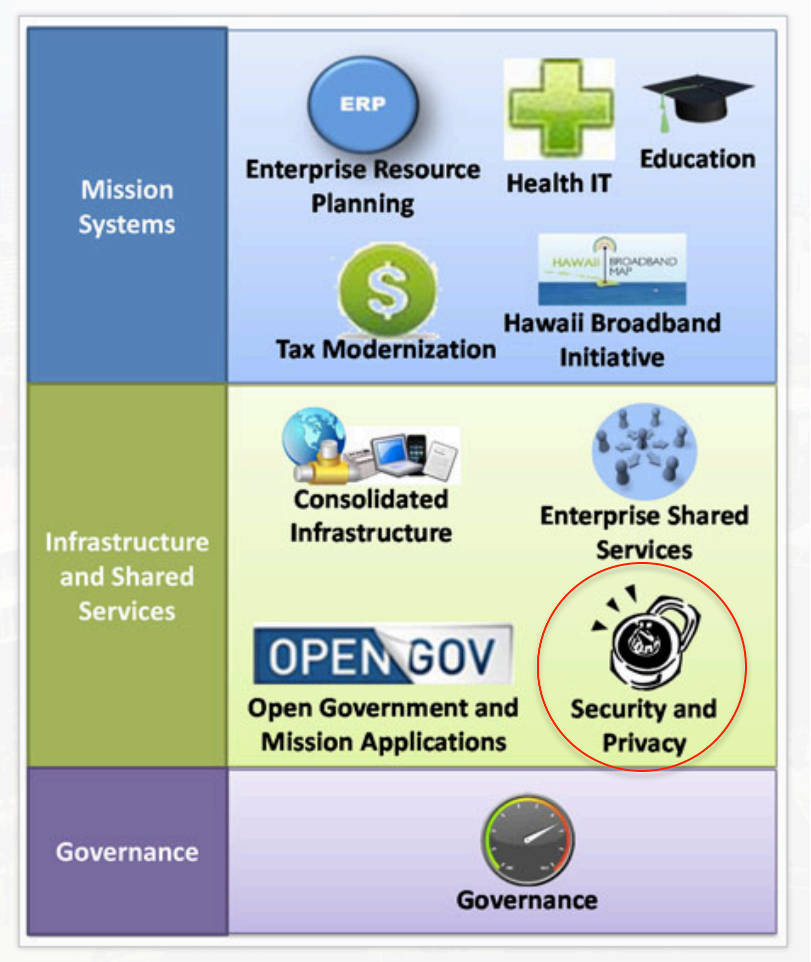
Lieutenant Colonel Antonio Querubin – Department of Defense

Bob Smock – Senior Director, Security & Risk Management, Gartner

Christina Tydeman – Director of Data Governance Office, Department of Education, State of Hawaii

State of Hawaii's Transformation Programs

- Infrastructure and Shared Services
  - Security and Privacy


Mission Systems
ERP
Enterprise Resource Planning
Health IT
Education
Tax Modernization
HAWAII BROADBAND MAP
Hawaii Broadband Initiative
Infrastructure and Shared Services
Consolidated Infrastructure
Enterprise Shared Services
OPEN GOV
Open Government and Mission Applications
Security and Privacy
Governance
Governance

Unfortunate Realities (*Source: Gartner Research)

California - Estimated $5M+ in Agency Remediation

- December 2012 – Department of Health Services
- 14,000 Social Security Numbers Posted Online

South Carolina - $340M (Breach and Remediation)

- November 2012 – Department of Revenue
- 3.8 Million SSNs, 650K Business Tax Filings;400K credit/debit card numbers hacked

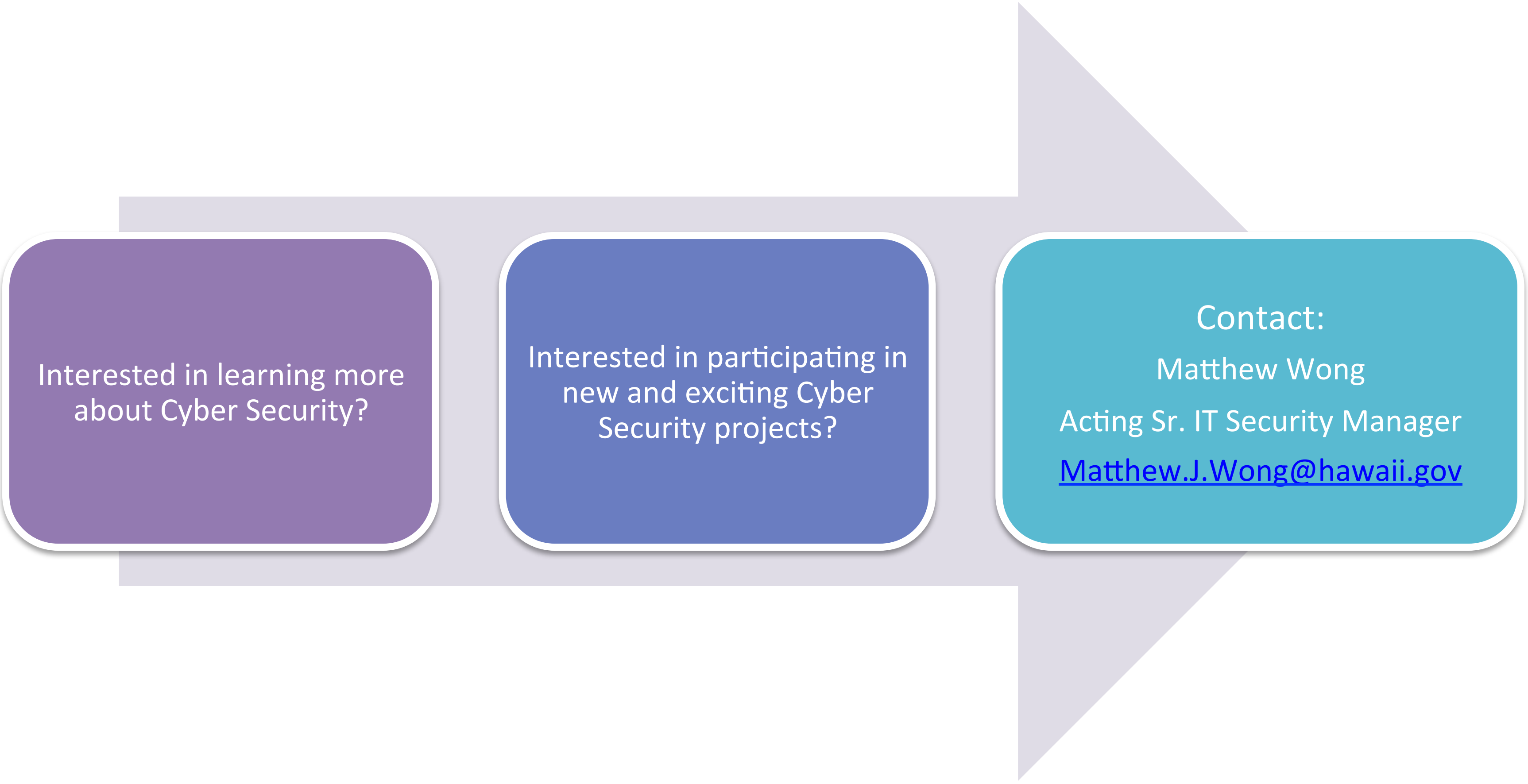
Texas - Estimated $5M+ in Agency Remediation

- April 2011- Texas Comptroller
- 3.5 Million Records (SSN, DOB, Name, Address) Posted Online

Utah - $9.48M (Initial Breach Only)

- April 2012 – Department of Health – 780K Medicaid Patient PII
- January 2013 – Contractor lost thumb drive of 6K Medicaid Recipients

Mahalo!



Interested in learning more about Cyber Security?

Interested in participating in new and exciting Cyber Security projects?

Contact:

Matthew Wong

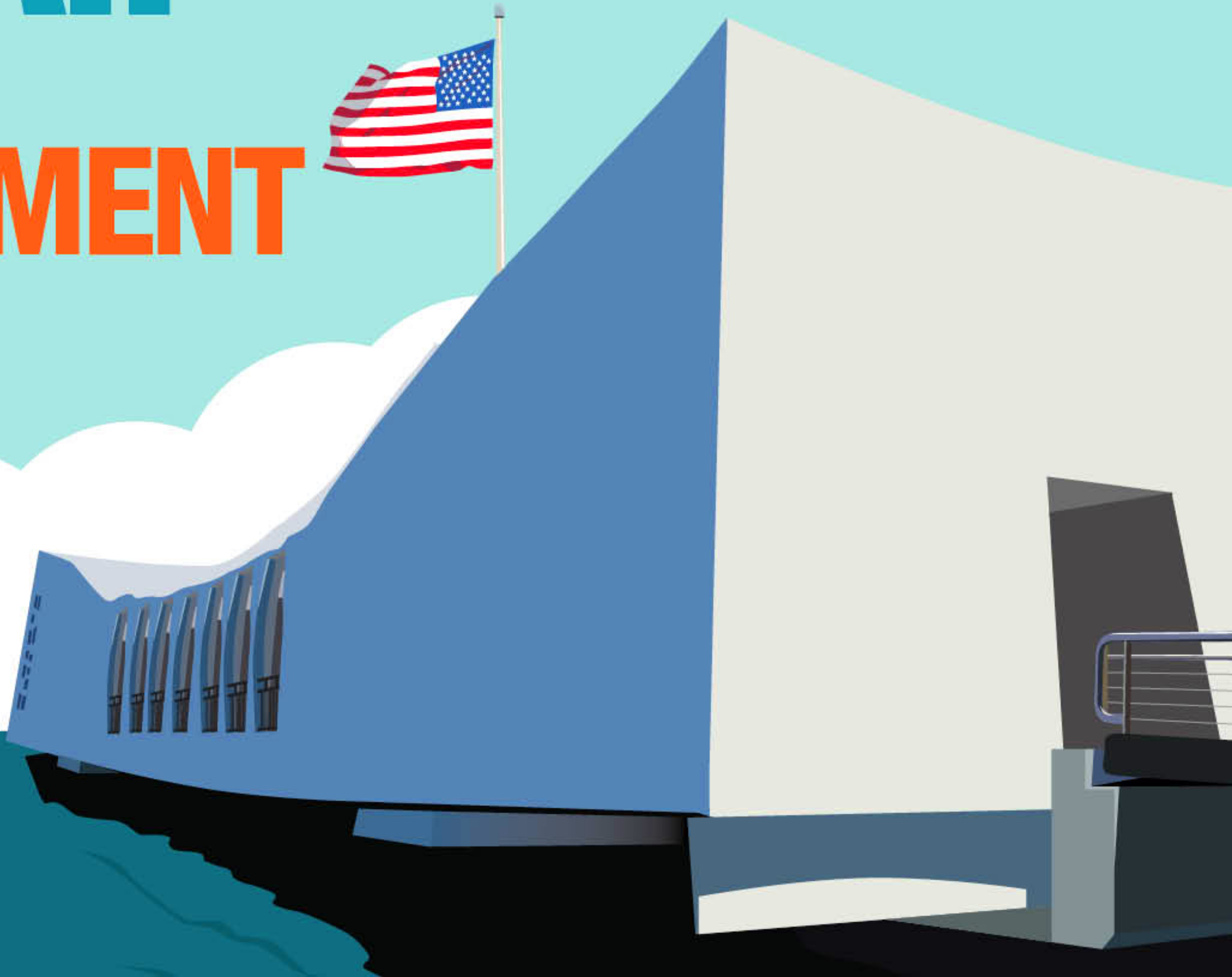
Acting Sr. IT Security Manager

Matthew.J.Wong@hawaii.gov

GOVERNMENT TECHNOLOGY®

STATE OF HAWAII
1959
UA MAU KE EA O KA AINA I KA PONO

HAWAII DIGITAL GOVERNMENT SUMMIT

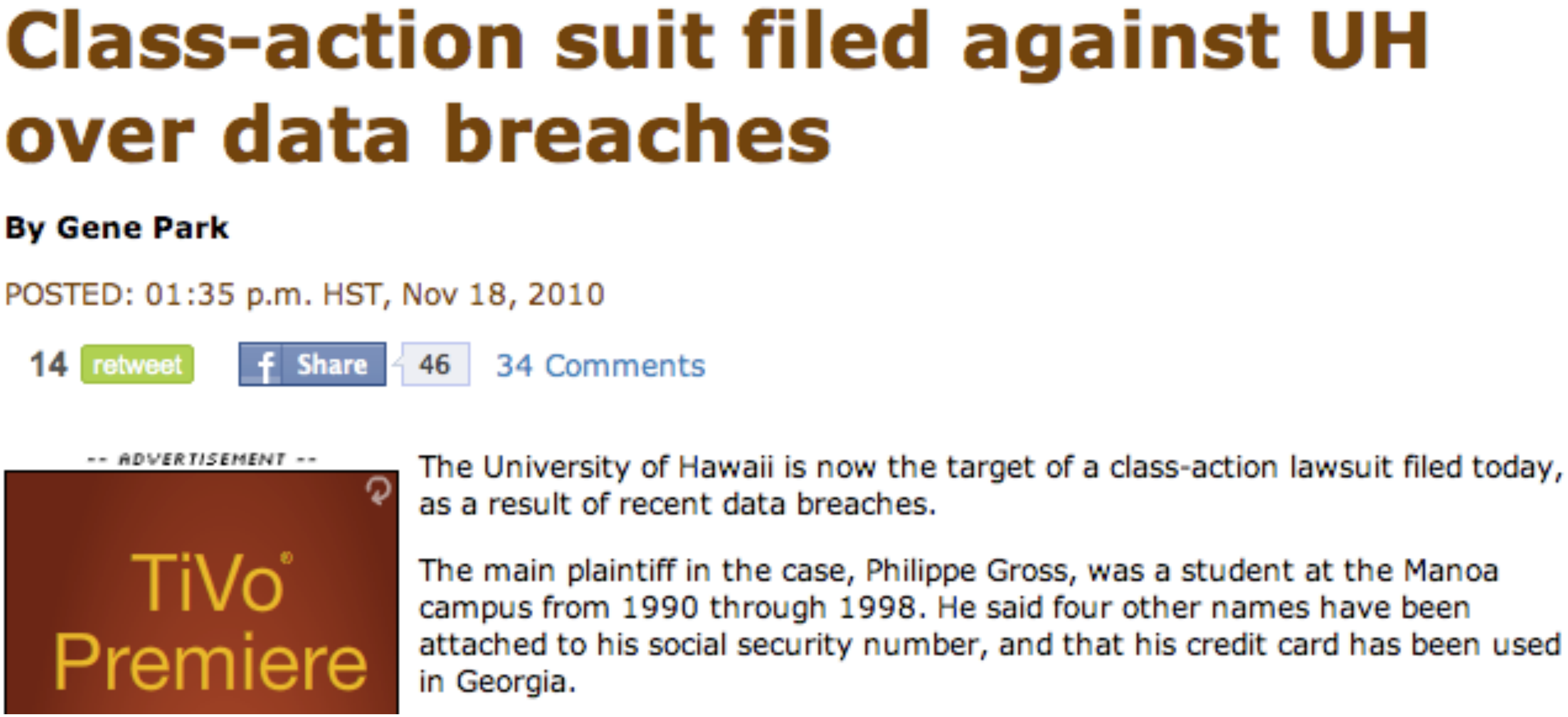


HONOLULU
HAWAII
NOVEMBER
TWENTY-FIRST
2013

Improving Security & Privacy @ UH

Overview of the UH Information Security Program

Jodi Ito
Information Security Officer
University of Hawaii
jodi@hawaii.edu



Class-action suit filed against UH over data breaches

By Gene Park

POSTED: 01:35 p.m. HST, Nov 18, 2010

-- ADVERTISEMENT --
TiVo® Premiere

The University of Hawaii is now the target of a class-action lawsuit filed today, as a result of recent data breaches.

The main plaintiff in the case, Philippe Gross, was a student at the Manoa campus from 1990 through 1998. He said four other names have been attached to his social security number, and that his credit card has been used in Georgia.

2010 External Information Security Assessment

- Summary of Findings:
  - A significant under-investment in information security resources
  - Trying to operationally manage information security as a fully de-centralized activity

Overarching Recommendation

“Develop a properly funded, strategically oriented, university-wide information security program that is centrally managed and operates in collaboration with the many de-centralized units throughout the university.”

Information Security Program

http://www.hawaii.edu/infosec/infosecprogram.html

- Five focus areas
  - Data Governance & Oversight
  - Information Security Audits & Risk Assessments
  - Information Security Policies & Procedures
  - Identity Management & Access Controls
  - Information Security Training & Awareness

Data Security Governance

- Data Security Leadership Council
  - – Comprised of senior leaders from each campus designated by Chancellor
  - – Responsible for compliance with Information Security Program
- UH IT Security Leads
  - – Comprised of technical support staff from departments designated by Dean/Director
  - – Responsible for carrying out technical security requirements

E2.215: Data Governance

http://www.hawaii.edu/uhdatagov/

- *"Data governance is the exercise of authority and control (planning, monitoring, and enforcement) over the management of data assets."*
- Designed to provide better understanding of our data assets and better protection for our sensitive data
- Complements E2.214: Security and Protection of Sensitive Information

E2.215: Overview

- Defines “institutional data” and governing principles across the UH System
- Establishes roles & responsibilities and clear lines of accountability
- Outlines best practices for effective data management & risk mitigation

Designed to:

- Provide accountability for use of data
- Reduce unnecessary duplication of data
- Reduce unnecessary risk of exposure of data when retained longer than REQUIRED
- Improve quality of data by identifying the primary source/owner of data

Data Governance Summary

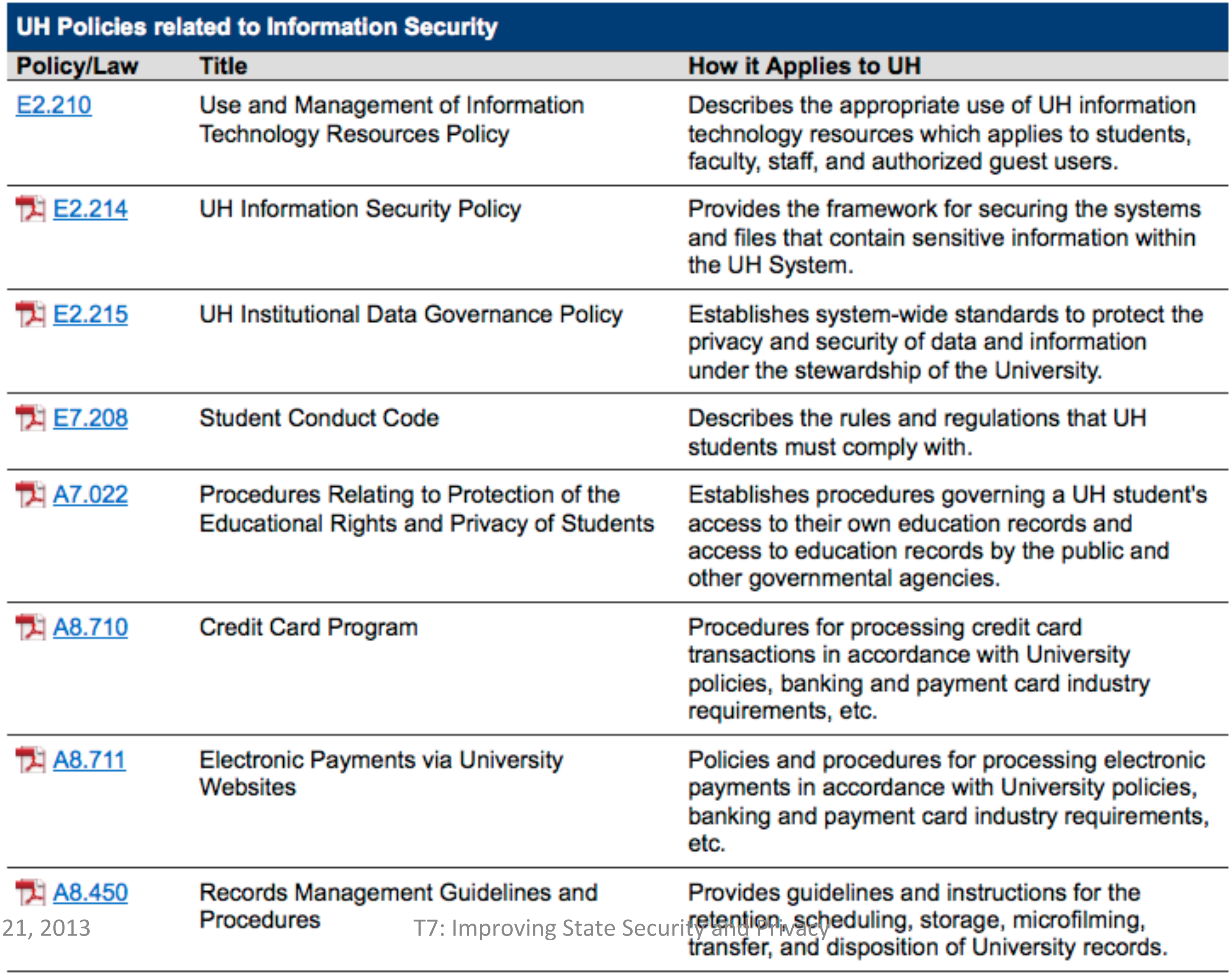
- Establishes a process that:
  - determines who needs to approve use of data
  - defines specifically what the data can be used for
  - which data can be used
  - what entities can use the data
  - how long the data can be used
  - what happens to the data after usage is over
- UH Data Sharing Request Procedure – needs to be completed when using “other campuses” institutional data or sharing outside of UH

Audits & Risk Assessments

- Partnering with UH Internal Audit to conduct information security assessments in “high risk” areas
- Combination of a survey and onsite inspections
- Resulting in revision or establishment of policies
- External assessment of critical assets every 2-3 years

Policies

http://www.hawaii.edu/infosec/policies.html



UH Policies related to Information Security

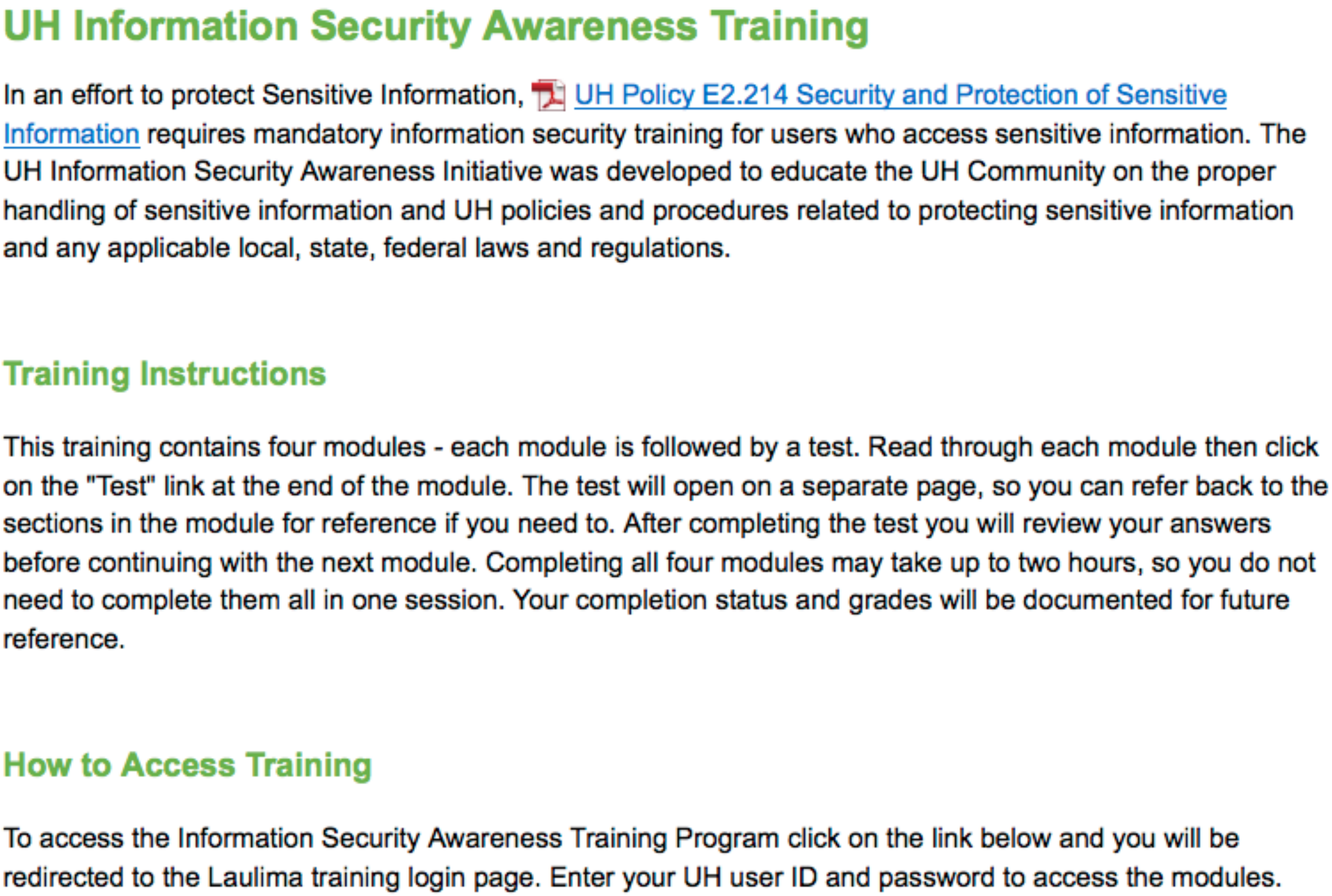
Policy/Law	Title	How it Applies to UH
E2.210	Use and Management of Information Technology Resources Policy	Describes the appropriate use of UH information technology resources which applies to students, faculty, staff, and authorized guest users.
E2.214	UH Information Security Policy	Provides the framework for securing the systems and files that contain sensitive information within the UH System.
E2.215	UH Institutional Data Governance Policy	Establishes system-wide standards to protect the privacy and security of data and information under the stewardship of the University.
E7.208	Student Conduct Code	Describes the rules and regulations that UH students must comply with.
A7.022	Procedures Relating to Protection of the Educational Rights and Privacy of Students	Establishes procedures governing a UH student's access to their own education records and access to education records by the public and other governmental agencies.
A8.710	Credit Card Program	Procedures for processing credit card transactions in accordance with University policies, banking and payment card industry requirements, etc.
A8.711	Electronic Payments via University Websites	Policies and procedures for processing electronic payments in accordance with University policies, banking and payment card industry requirements, etc.
A8.450	Records Management Guidelines and Procedures	Provides guidelines and instructions for the retention, scheduling, storage, microfilming, transfer, and disposition of University records.

Developing New Policies

- HIPAA
- PCI-DSS
- Updating data classification categories
- Developing technical requirements for new data categories

Information Security Training & Awareness

- Developed in-house in UH learning management system (Sakai)
- Consists of 4 modules with quiz after each module
- Must pass with 70% score
- Required for users of UH information systems (personnel, student information, & operational data warehouse systems)
- Starting to require consultants to take training



UH Information Security Awareness Training

In an effort to protect Sensitive Information, UH Policy E2.214 Security and Protection of Sensitive Information requires mandatory information security training for users who access sensitive information. The UH Information Security Awareness Initiative was developed to educate the UH Community on the proper handling of sensitive information and UH policies and procedures related to protecting sensitive information and any applicable local, state, federal laws and regulations.

Training Instructions

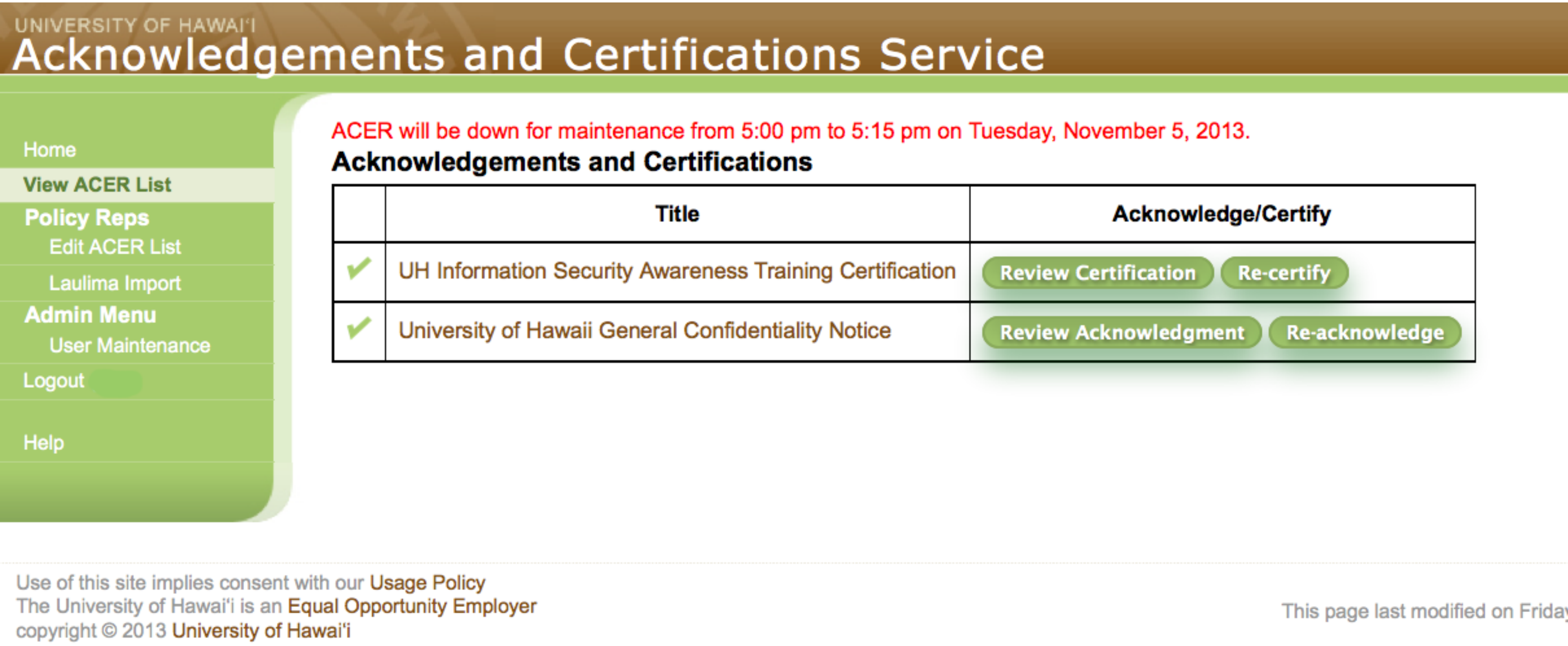
This training contains four modules - each module is followed by a test. Read through each module then click on the "Test" link at the end of the module. The test will open on a separate page, so you can refer back to the sections in the module for reference if you need to. After completing the test you will review your answers before continuing with the next module. Completing all four modules may take up to two hours, so you do not need to complete them all in one session. Your completion status and grades will be documented for future reference.

How to Access Training

To access the Information Security Awareness Training Program click on the link below and you will be redirected to the Laulima training login page. Enter your UH user ID and password to access the modules.

Identity Management & Access Controls

- Developing ACER system (**A**cknowledgements & **CER**tifications)
- Track electronic signing of confidentiality agreement or other agreements
- Track completion of training
- Eventually will automatically disable accounts if training requirements not fulfilled
- Ongoing password strengthening
- Working towards multi-factor authentication



UNIVERSITY OF HAWAI'I

Acknowledgements and Certifications Service

ACER will be down for maintenance from 5:00 pm to 5:15 pm on Tuesday, November 5, 2013.

Acknowledgements and Certifications

	Title	Acknowledge/Certify
✓	UH Information Security Awareness Training Certification	Review Certification Re-certify
✓	University of Hawaii General Confidentiality Notice	Review Acknowledgment Re-acknowledge

Use of this site implies consent with our Usage Policy
The University of Hawai'i is an Equal Opportunity Employer
copyright © 2013 University of Hawai'i

This page last modified on Frida

Additional Program Elements

- Protecting Sensitive Information at UH:
  - http://www.hawaii.edu/askus/1266
- Registration & scanning of servers (file, web, ftp)
  - http://www.hawaii.edu/its/server/registration/

Summary

- Continuous review and refinement
- 2013 Information Security Assessment shows significant improvement
- Increased awareness among staff

Questions?

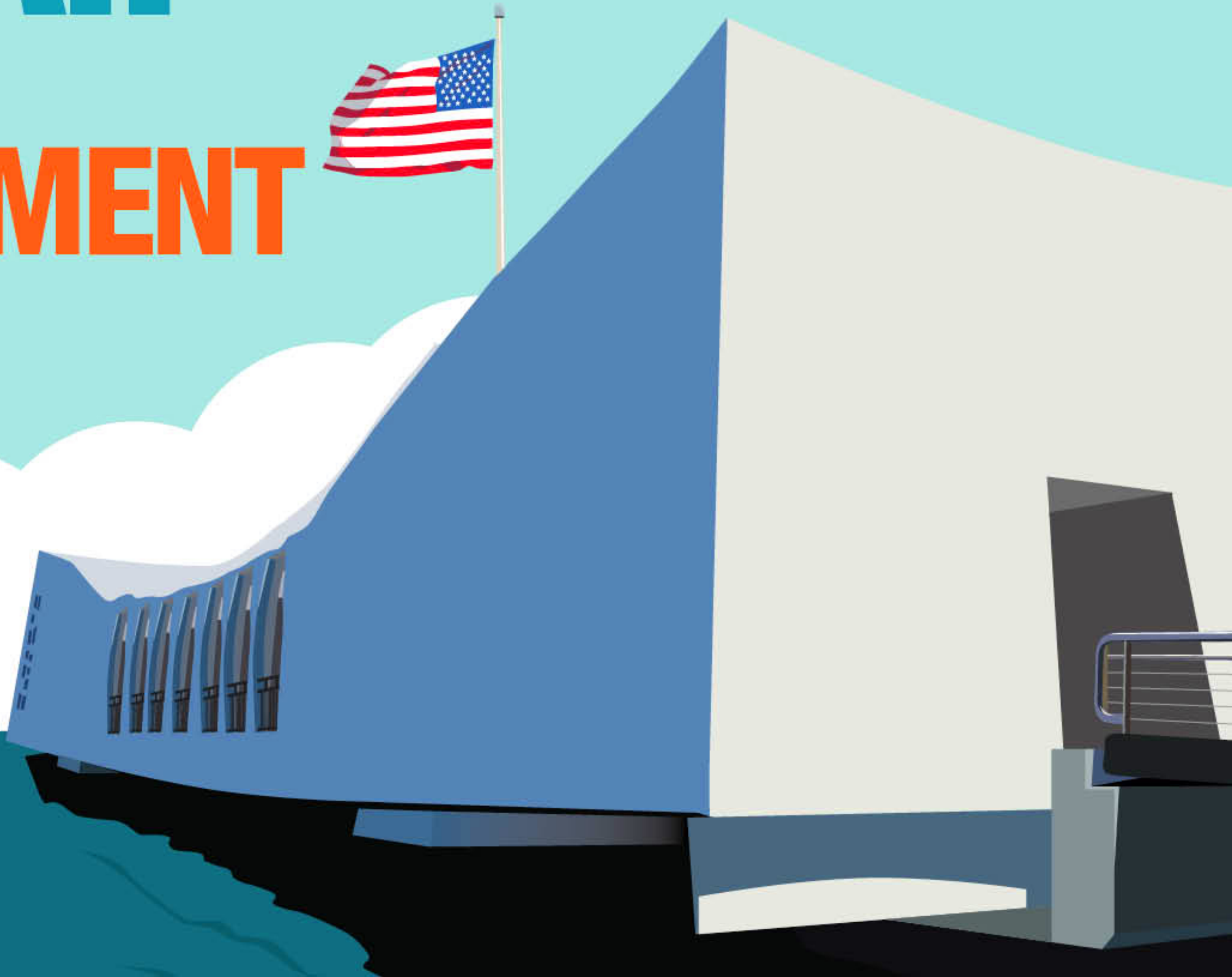
jodi@hawaii.edu

GOVERNMENT TECHNOLOGY®

STATE OF HAWAII 1959
UA MAU KE EA O KA AINA I KA PONO

HAWAII DIGITAL GOVERNMENT SUMMIT

HONOLULU
HAWAII
NOVEMBER
TWENTY-FIRST
2013



T7: Improving State Security and Privacy

- Cyber Protection Team
- Cyber Security Center of Excellence
- PKI

Cyber Protection Teams

- **ARNG CND team of 10**
- **US Cyber Command**
  - active duty Title 10 authorization limits
  - NG troops can operate under both Title 10 and Title 32
- **10 Army NG CPTs proposed, one in each FEMA region**
  - Hawaii is in FEMA region 9 (AZ, CA, HI, NV, Pacific Islands)
  - 39 personnel
  - SCIF
  - presence of multiple agencies makes Hawaii target rich

Cyber Security Center of Excellence

- **Pooihe exercise**
- **Collaboration among diverse levels of government, academia, and other organizations (fusion centers, SOC, FBI, NSA, etc)**
- **Cyber security skills training**
- **Skilled STEM workforce**
- **Sustainable Cyber Range**
  - community resource
  - conduct exercises, simulations, forensic analysis
  - research best practices and strategies for response and mitigation

PKI

- **Why?**
  - – encrypt/sign email with other government agencies
  - – inter-agency forms processing
  - – identity management
- **Cross-certification with the Federal Bridge CA**

PKI

- **Establishing a Federally recognized CA**
  - Illinois first state to cross-certify with FBCA
  - established state law recognizing digital signatures
  - 300000 certificates issued
  - various security levels
  - identity distinct from authorization
  - decade long effort
  - staff of 5
- **Audit Requirements**

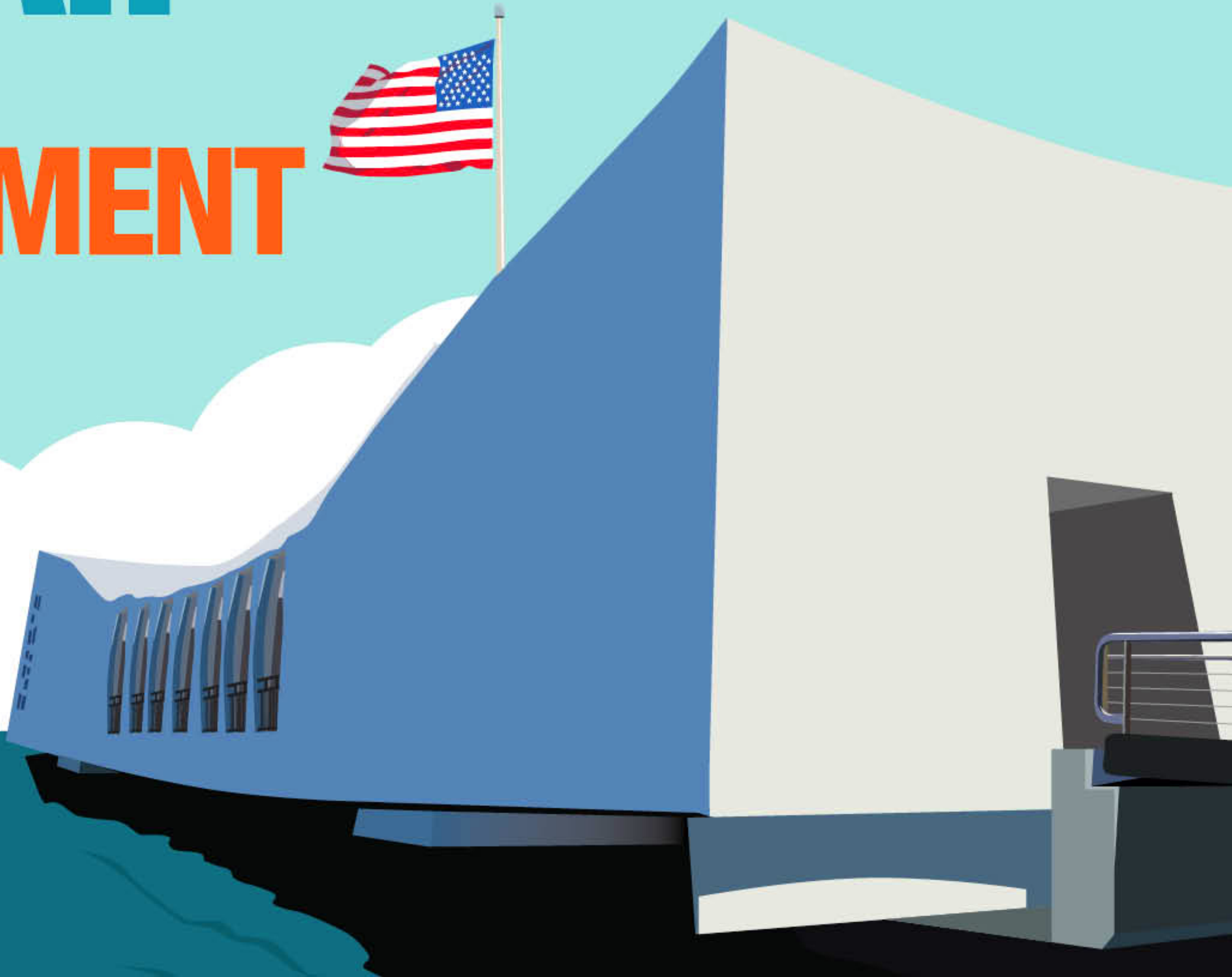
- **Summary**
  - Operational Needs Statement - CPT in Hawaii
  - Pooihe 2014 (state / county teams?)
  - PKI way forward

GOVERNMENT TECHNOLOGY®

STATE OF HAWAII 1959
UA MAU KE EA O KA AINA I KA PONO

HAWAII DIGITAL GOVERNMENT SUMMIT

HONOLULU
HAWAII
NOVEMBER
TWENTY-FIRST
2013

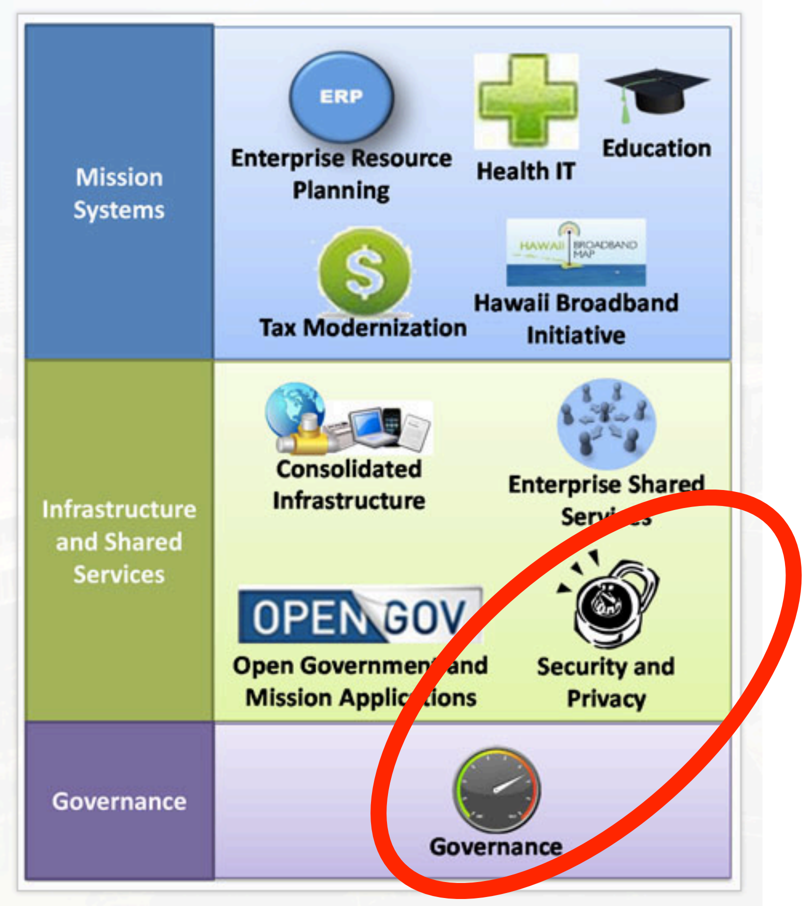


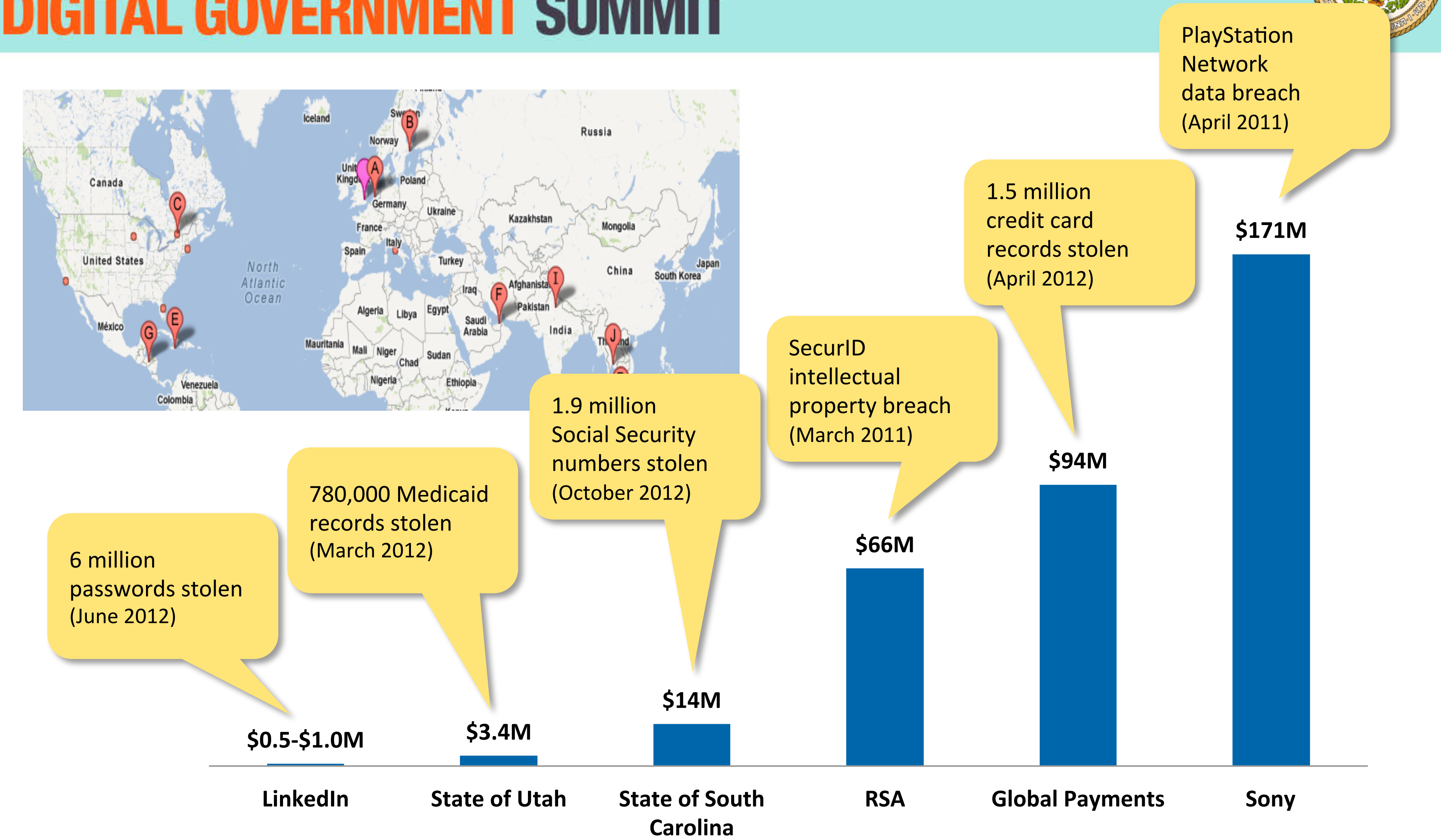
- **T7 – Improving State Security and Privacy**
- **Information Classification – The Most Essential Security Thing You're (Probably) Still Not Doing**
  - What is information classification/categorization?
  - Why classify – categorize – information?
  - Is data classification performed only for security purposes?
  - Can information classification be "transformational"?
  - How do you get started?
  - *Does your organization need to solve data classification?*

As the volume of electronic information created and maintained grows, it gets harder and harder for organizations to locate, catalog, SECURE, and manage information.

State of Hawaii's Transformation Programs

- Infrastructure and Shared Services
  - Security and Privacy
- Governance


Mission Systems
ERP
Enterprise Resource Planning
Health IT
Education
Tax Modernization
HAWAII BROADBAND MAP
Hawaii Broadband Initiative
Infrastructure and Shared Services
Consolidated Infrastructure
Enterprise Shared Services
OPEN GOV
Open Government and Mission Applications
Security and Privacy
Governance
Governance



6 million passwords stolen (June 2012)

780,000 Medicaid records stolen (March 2012)

1.9 million Social Security numbers stolen (October 2012)

SecurID intellectual property breach (March 2011)

1.5 million credit card records stolen (April 2012)

PlayStation Network data breach (April 2011)

It's no secret…our data is under assault!

- **Information Classification – What is it?**
  - The analysis of a data item or group of data items to determine into which of a predefined set of categories it belongs.
  - Information classification can be done at or before ("prospective") the time the information is rendered into usable (e.g., electronic) form or later ("retrospective").

Information classification is a branch of electronic content management (i.e., Information Governance).

- **Information Classification – Can you?**
  - Identify all duplicate copies of a document and replace them with links to the original ? (*data leakage*)
  - Find confidential content and prevent its disclosure to those without a need to know? (*data exposure*)
  - Identify every document to which the terms of a particular government regulation apply? (*compliance*)
  - Identify every document relevant to a particular transaction? (*e-discovery*)
  - Identify all infrequently used documents and move them to low-cost storage tiers? (*data leakage/storage management*)
  - Identify information subject to U.S. International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR) export restrictions and ensure that it is not communicated to non-U.S. persons? (*national security*)

Managing electronic data is not easy or inexpensive, but failing to manage it can be much more expensive.

Information classification is about more than just security.

Knowledge management: Information classification can be used to help identify the content of documents in a repository.

Storage management: Information classification can be used to identify seldom-used and duplicate documents to improve repository performance.

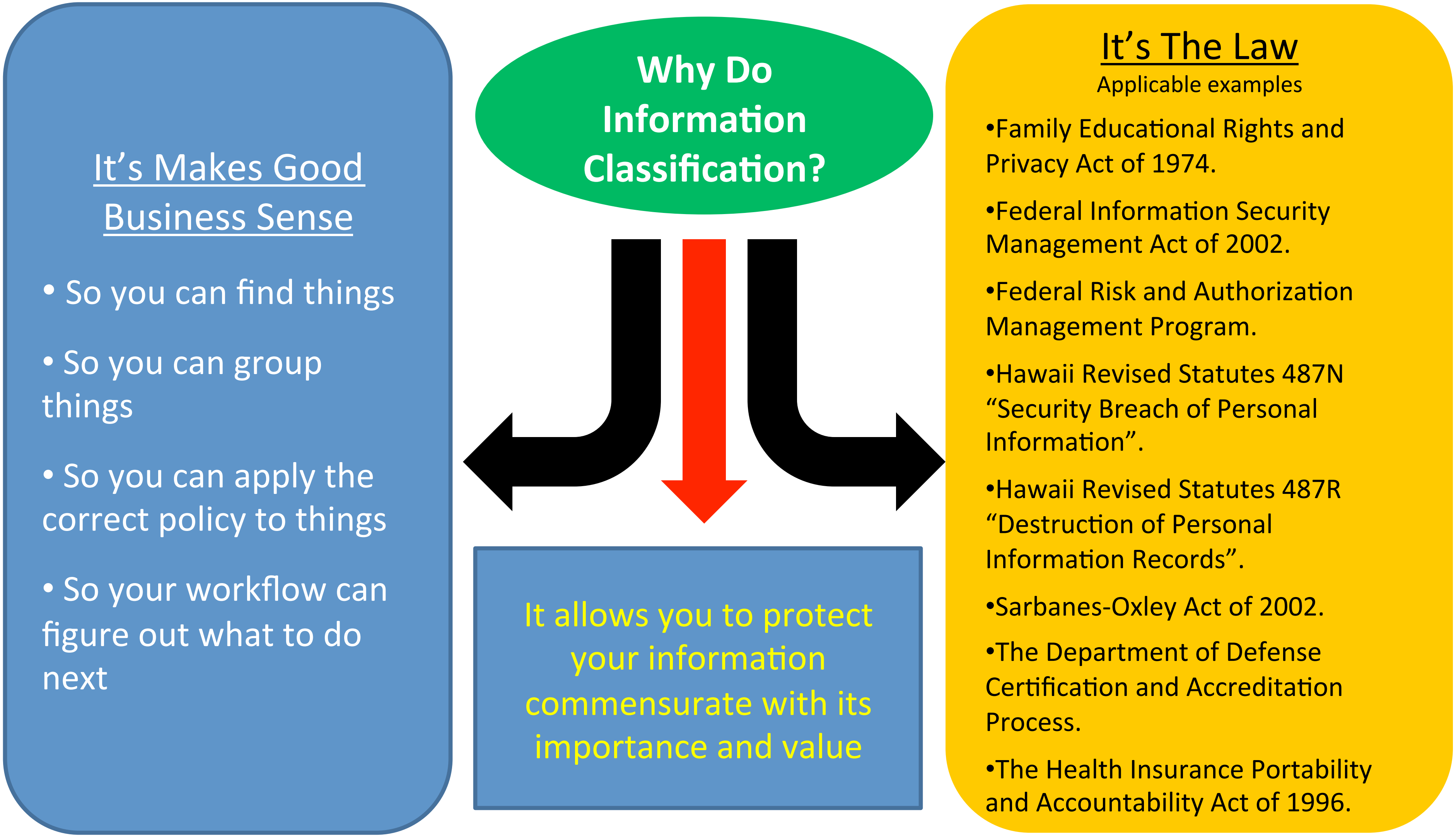
Electronic discovery: Information classification can be used to identify documents which are relevant to a business transaction that has given rise to legal action.

Compliance audit: Information classification can be used to find documents containing material that may be subject to the terms of a regulation.

Risk management: Information classification can be used to identify confidential documents requiring data-centric protection.

Compliance automation: Classification labels can be used as the basis for automating enforcement of policies that ensure compliance with the terms of regulations.

Access control: Classification labels can be used as the basis for automating enforcement of an access control policy that ensures the documents are viewed only by users with a demonstrated need to know their contents.



Why Do Information Classification?

It's Makes Good Business Sense

- So you can find things
- So you can group things
- So you can apply the correct policy to things
- So your workflow can figure out what to do next

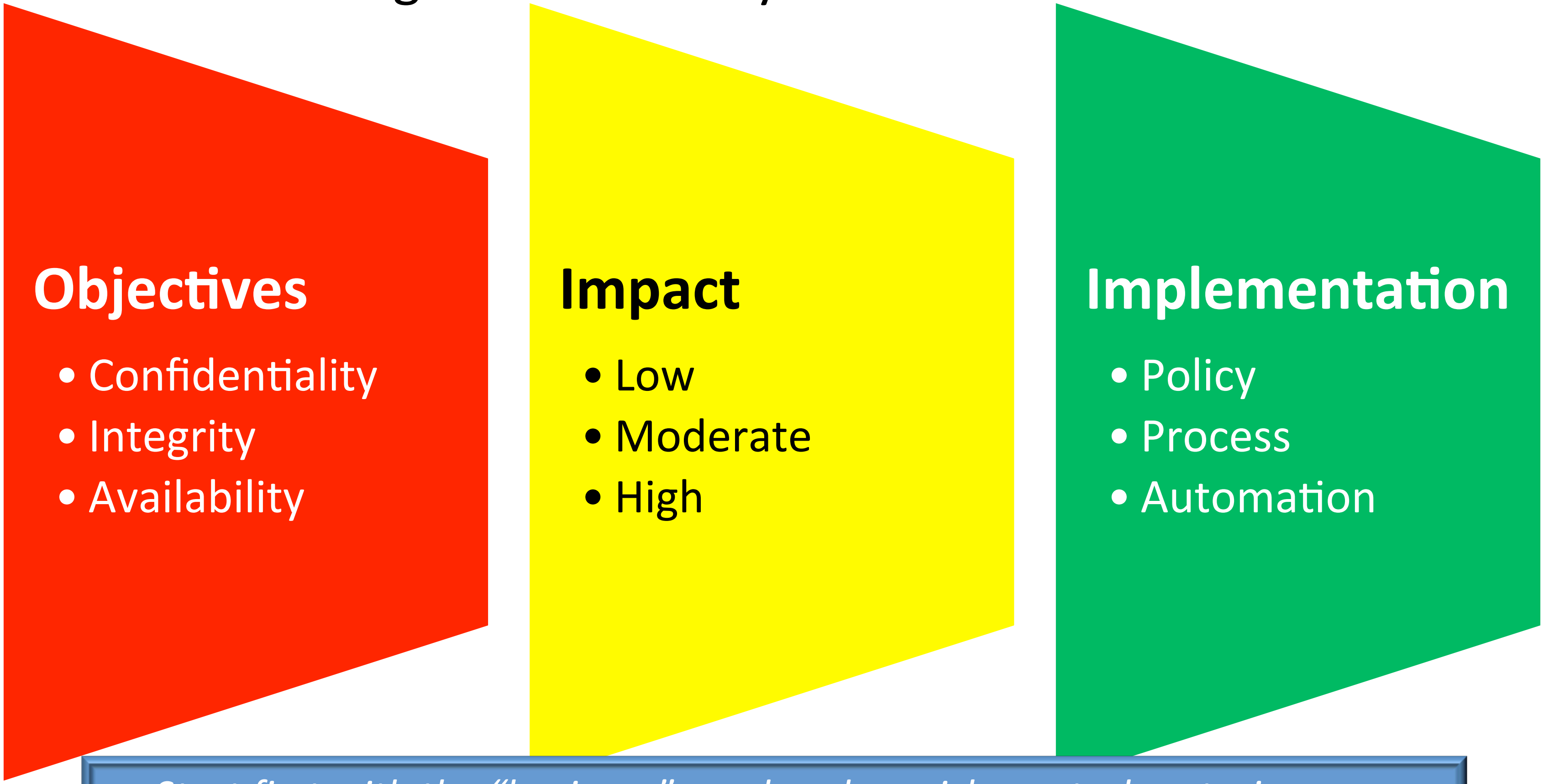
It allows you to protect your information commensurate with its importance and value

It's The Law

Applicable examples

- Family Educational Rights and Privacy Act of 1974.
- Federal Information Security Management Act of 2002.
- Federal Risk and Authorization Management Program.
- Hawaii Revised Statutes 487N "Security Breach of Personal Information".
- Hawaii Revised Statutes 487R "Destruction of Personal Information Records".
- Sarbanes-Oxley Act of 2002.
- The Department of Defense Certification and Accreditation Process.
- The Health Insurance Portability and Accountability Act of 1996.

Make Information Classification be ***transformational*** to your organization and your constituents



Objectives

- Confidentiality
- Integrity
- Availability

Impact

- Low
- Moderate
- High

Implementation

- Policy
- Process
- Automation

Start first with the "business" need: reduce risk, control costs, improve compliance, increase business value.

Practical Approaches

Referred to as …	Can Be Synopsized as …	Focuses on …	Is Exemplified by …
The Structuralist	Taking the most basic approach to classification; some practitioners may not officially consider it classification	Structured information that has specific regulatory requirements; locations of primary concern are databases and applications, but also include unstructured sources	•Payment Card Industry Data Security Standard (PCI DSS) cardholder data •Social Security numbers •Other PII data
The Realist	Acknowledging that the organization's information stewards think coarsely about information: Either it's sensitive, or it's not; suffers from over- and under-classification	Determining what is strictly public information and what needs to be protected by at least a baseline of security controls; often augments the two tiers with a structuralist approach	•Public or non-sensitive •Nonpublic, sensitive or confidential
The Broker	Trying to create better granularity of classification (generally in order to match controls with levels of sensitivity) while recognizing that a grandiose multitier scheme doesn't work	Information risk-based approach that differentiates low-, medium- and high-impact consequences for the organization; often struggles to articulate "middle-level" risk, although structuralist approach may be used to identify specific data risks	•Public or low business impact •Medium business impact •High business impact
The Striver	Striving to implement (some variation of) a traditional four-tier classification scheme whose middle levels distinguish internal-use information (broad employee access) from need-to-know (specifically defined employee access)	Three or more tiers of information risk above "public" or nonsensitive information; often challenging to define Levels 2 and 3 of the scheme in a meaningful way	•Public or non-sensitive •Internal or sensitive •Confidential or need-to-know •{Highly or strictly or registered} + {confidential or sensitive}, or secret

How To Get Started

- Establish a high-level classification policy, enumerating what information must be classified.
- Assign clear responsibility and authority for ensuring that procedures are implemented and followed.
- Formulate information classification criteria as rules to data users for the classification of information.
- Develop a process for classification review to ensure and demonstrate that the policy is being executed.
- Establish a process for reclassification of information when its content, significance, or ownership changes.
- Develop standards for labeling that alert users to the fact that those assets have been assigned a classification.
- Develop requirements & training to ensure users are aware of their responsibility to handle information appropriately.
- Ensure that classification is integrated into organizational processes including: Creation; Ownership change; modification; Publication; Workflow approval; Version control ; Copies; Backup/restore; reclassification request.

Automating poor process & policy only helps us do poor things faster.

Education Data - Rules and Regulations

FERPA = Family Educational Rights to Privacy Act
IDEA = Individuals with Disabilities Education Act
PPRA = Protection of Pupil Rights Amendment
COPPA = Children's Online Privacy Protection Act
COPA = Child Online Protection Act
CIPA = Children's Internet Protection Act

- ✓rules and guidelines
- ✓floor, not the ceiling
- ✓parental consent

Personally Identifiable Information (PII) includes, but is not limited to:

- Student’s name

  Name of parent or other family members

  Student’s / Family’s address

  Personal identifier (e.g. Social Security #, student ID, etc.)

  Student’s date/place of birth

- Any other personal information which could be linked to student

Frequent Requestors

School Community Councils

Media

Analysts and Researchers

Advocates

Outside Agencies/Companies

Transparency & Services vs. Privacy

"Big Brother and the National Databases"

Open Data & Big Data

Collaborative Assessment Databases

3rd Party Vendor Products

Statewide Longitudinal Data Systems

Technological Safeguards Guidelines and Resources

Suppression, Redaction, Limited Access

Confidentiality Agreements Data Sharing Agreements

Data Ethics Ongoing Training Monitoring and Audits

K-12 Education Resources

Data Governance Office

http://datagovernance.k12.hi.us/

DGO@notes.k12.hi.us

FERPA specialist

ferpa@notes.k12.hi.us

Research Application

DOEresearch@notes.k12.hi.us

US Department of Education

http://www.ed.gov/policy/gen/guid/fpco/ferpa