Protecting UH Research
Spring 2021

March 23, 2021 (recorded)

Sandra Furuto, Data Governance Director
Jodi Ito, Chief Information Security Officer
Victoria Rivera, Office of Research Compliance Director
Allie Zust, Export Controls & FSO Manager
And Special Guest:
Shawn Case, Counterintelligence Special Agent, Defense Counterintelligence and Security Agency (DCSA)
Today’s Agenda

• Welcome
• Research-Related Threats and Regulations
• Data Governance & Compliance
• Export Controls
• Foreign Influence
• Conflict of Commitment / Interest
Research-Related Threats and Regulations

Jodi Ito, Chief Information Security Officer
Increased Threats to UH

• Large increase of scans and RDP/SSH/VNC/DB bruteforcing attacks from non-attributable cloud providers such as Google, Microsoft, Amazon, DigitalOcean, and others since this summer.

• Ransomware operators forming a cartel to buy access to compromised networks from other criminal groups, affiliates, and contractors who are offered a commission on the payout.

• In 2020, criminal gangs have been demanding ransom payments of over $1 million. One of the largest demands was 136,000 BTC or $1.5 billion for a global corporation.

• Ransomware attacks against higher ed up 100% compared to 2019

• Recent alerts: ransomware targeting healthcare & public health sectors: https://us-cert.cisa.gov/ncas/alerts/aa20-302a
A leading medical-research institution working on a cure for Covid-19 has admitted it paid hackers a $1.14m (£910,000) ransom after a covert negotiation witnessed by BBC News.

The Netwalker criminal gang attacked University of California San Francisco (UCSF) on 1 June.

IT staff unplugged computers in a race to stop the malware spreading.

And an anonymous tip-off enabled BBC News to follow the ransom negotiations in a live chat on the dark web.
Higher Ed Ransomware Attack: University Pays $457K Despite Having Backups

Fri | Aug 21, 2020 | 4:30 AM PDT

The University of Utah is starting its fall semester with a great deal of disruption.

There is COVID-19 testing and tracing, new human traffic flow patterns to avoid student bottlenecks getting into buildings, and mandatory limits on how many students can be in a single facility like the library.

Now, you can add a ransomware attack to the list of disruptions the university is juggling.

And this disruption was enough, the university says, to justify paying hackers nearly half a million dollars in digital ransom.

Details of the University of Utah ransomware attack

The university just shared what happened, and when, regarding the cyberattack.

We know the attack started on July 19, 2020, after hackers accessed a sliver of the university’s network:

"...computing servers in the University of Utah’s College of Social and Behavioral Science (CSBS) experienced a criminal ransomware attack, which rendered its servers temporarily inaccessible.

https://www.secureworldexpo.com/industry-news/university-of-utah-ransomware-attack
<table>
<thead>
<tr>
<th>Ransomware Gangs who Exfiltrate/Leak Stolen Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaddon</td>
</tr>
<tr>
<td>Cl0p</td>
</tr>
<tr>
<td>Conti/Ryuk</td>
</tr>
<tr>
<td>CryLock</td>
</tr>
<tr>
<td>Crysis/Dharma</td>
</tr>
<tr>
<td>DarkSide</td>
</tr>
<tr>
<td>DoppelPaymer</td>
</tr>
<tr>
<td>Egregor</td>
</tr>
<tr>
<td>Fonix</td>
</tr>
<tr>
<td>Light</td>
</tr>
<tr>
<td>LockBit</td>
</tr>
<tr>
<td>Maze</td>
</tr>
<tr>
<td>MountLocker</td>
</tr>
<tr>
<td>Nemty</td>
</tr>
<tr>
<td>Nefilim/Nephilim</td>
</tr>
<tr>
<td>Netwalker</td>
</tr>
<tr>
<td>OldGremlin</td>
</tr>
<tr>
<td>Pysa/Mespinoza</td>
</tr>
<tr>
<td>ProLock</td>
</tr>
<tr>
<td>RagnarLocker</td>
</tr>
<tr>
<td>RansomExx</td>
</tr>
<tr>
<td>Ranzy/Ako</td>
</tr>
<tr>
<td>Revil/Sodinokibi</td>
</tr>
<tr>
<td>Sekhmet</td>
</tr>
<tr>
<td>Snake</td>
</tr>
<tr>
<td>Snatch</td>
</tr>
<tr>
<td>SunCrypt</td>
</tr>
</tbody>
</table>
As ransomware attacks have quickly morphed over the past few years into a billion-dollar business, the groups behind them are increasingly adopting the practices and tactics of the corporate businesses they target.

More and more, ransomware groups (and some argue the larger cybercrime ecosystem) are gravitating towards joint partnerships and profit sharing arrangements with other hacking groups, introducing tools to measure the efficiency of their work, creating playbooks and scripts during the negotiation phase, and adopting customer service and PR tactics from the corporate world.
Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets

University of Hawaii, University of Washington and MIT are among schools hit by cyberattacks

By Dustin Volz
March 5, 2019 5:30 a.m. ET

Woods Hole is the largest independent oceanographic research institution in the U.S. Here, a mechanical engineer at Wood Hole looks on as a crane lifts a specially designed system of sonars and cameras. PHOTO: DAVID L. RYAN/THE BOSTON GLOBE VIA GETTY IMAGES

Data was exfiltrated (data encrypted – don’t know what was taken)

Multiple UHM subnets were compromised (behind a firewall)

Servers that were compromised contained Personally Identifiable Information (PII)
  • UH is required by Hawaiʻi Revised Statute (§487N-4) to inform the Legislature and notify individuals affected by the potential exposure
  • Unsure whether the PII was accessed, thus proceeded out of an abundance of caution and sent out notifications

Federal Law Enforcement Agencies assisted in the investigation
Malicious Activity Targeting COVID-19 Research, Vaccine Development

Original release date: July 16, 2020

In response to malicious activity targeting COVID-19 research and vaccine development in the United States, United Kingdom (UK), and Canada, the Cybersecurity and Infrastructure Security Agency (CISA), UK’s National Cyber Security Centre (NCSC), Canada’s Communications Security Establishment (CSE), and the National Security Agency (NSA) released a Joint Cybersecurity Advisory to expose the threat. A malicious cyber actor is using a variety of tools and techniques to target organizations involved in COVID-19 research and vaccine development. Tools include SOREFANG, WELLMESS, and WELLMAIL malware.

CISA encourages users and administrators to review the Joint Cybersecurity Advisory and the following Malware Analysis Reports for more information and to apply the mitigations provided.

- SOREFANG
- WELLMESS
- WELLMAIL
Two Threats to Watch Out For...

• Credential Stuffing
  • Attacker uses credentials stolen from other websites in order to gain access into the target organization

• Malware infected email (SpearPhishing) or website
  • Attacker infects victim machines with malware in order to gain access into the target organization
Credential Stuffing

Collection of Public Data Dumps
12,755 files totaling 708GB
4.6 billion credentials

Matches on "@hawaii.edu"
146,774 credentials
4,402 credentials (complexity match)
1,649 passwords reset since 2019

Chegg breach accounted for 82% of password resets at UH

https://haveibeenpwned.com/
This screenshot was taken when malware executed on a victim's PC. This user has **McAfee**, **SUPERAntiSpyware**, **MalwareBytes**, and **Kaspersky**.
This malware will **steal data** from the computer and **send** it off to its Command and Control, then **delete itself** so the user will find no evidence of an infection and take no action (e.g. don't change passwords).

- **Browser cookies used to bypass passwords and 2FA**
- **RDP credentials**
- **Credit card numbers, home address, phone number, passwords stored in browser's autofill**
- **Access tokens and cached credentials**

Text, Word, Excel, and other files taken from the desktop and "My Documents" folder.
Research-Related Regulations & Compliance
HIPAA
(Health Insurance Portability and Accountability Act)

• UH HIPAA Policy: EP 2.217
• UH is a Covered Entity
  • Healthcare providers
  • Research
• https://www.hawaii.edu/infosec/hipaa/
Other Federal Regulations

• NDAA 889 / HHS 889
• DoD published the interim DFARS rule 2019-D041, “Assessing Contractor Implementation of Cybersecurity Requirements”, on September 29, 2020, with an effective date of November 30, 2020
• https://www.govinfo.gov/content/pkg/FR-2020-09-29/pdf/2020-21123.pdf
• DFARS 252.204-7012: requires implementation of NIST 800-171: Controlled Unclassified Information (CUI) by Dec. 2017
• DFARS 252.204-7019: Notice of NIST SP 800–171 DoD Assessment Requirements
• DFARS 252.204-7020: NIST SP 800–171 DoD Assessment Requirements
• DFARS 252.204-7021: Cybersecurity Maturity Model Certification (CMMC) Requirements
NDAA 889 / HHS 889 Summary


- Part B: Effective **August 13, 2020**, the Government may not contract with an entity that **uses** certain telecommunications equipment or services, as a substantial or essential component of any system, or as critical technology as part of any system, produced by any of the same five named Chinese companies or their subsidiaries and affiliates

- Huawei, ZTE, Hytera, Hangzhou Hikvision, Dahua (or any subsidiary or affiliate)
Interim DFARS Rules Summary

- **DFARS Clause 252.204-7020**: NIST SP 800-171 DoD Assessment Methodology
  - Effective November 1, 2020
  - Must have a self assessment of 800-171 compliance submitted on the SPRS website *before award can be made*

- **DFARS Clause 252.204-7021**: Cybersecurity Maturity Model Certification (CMMC)
  - Five levels (CMMC Level 1 – Level 5)
    - Level 1 – Basic Safeguarding (FAR 52.204-21)
    - Level 3 – DFARS 252.204-7012 (NIST 800-171 + 20 additional controls)
  - Requires PASSING an audit by a 3rd party certified assessor BEFORE proposal submission
  - Phased rollout
    - FY 21: 15 contractors will be selected (includes flow down to subcontractors)
    - By Oct. 2025, CMMC certification will be required for ALL DoD contracts
Cyber Hygiene Best Practices – FOR EVERYONE

1. Anti-Malware Software and Host Based Firewalls
2. Regularly Update Software
3. Multi-Factor Authentication
4. Set Strong Passwords
5. Use Encryption
6. Back Up Your Data
7. Lock Your Devices
8. Limit the use of Administrative Accounts
9. Recognize Phishing
10. Mobile Device Security

Source: https://www.hawaii.edu/infosec/minimum-standards/cyber-hygiene/
The UH Enterprise Dropbox environment is intended for those working with Data categorized as Sensitive or Regulated.

Users working with Public and Restricted data should use Google@UH Drive.

<table>
<thead>
<tr>
<th>Public Data</th>
<th>Protected Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public (No Risk)</td>
<td>Restricted (Low Risk)</td>
</tr>
<tr>
<td>No privacy considerations.</td>
<td>Data used internally within the UH community but not released to external parties without a contract or memorandum of agreement.</td>
</tr>
</tbody>
</table>

**Definition:**
Institutional Data where access is not restricted and is subject to open records requests.

<table>
<thead>
<tr>
<th>Sensitive (Medium Risk)</th>
<th>Regulated (High Risk)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data subject to privacy considerations.</td>
<td>Highly sensitive data that is subject to state breach notification requirements, financial fines, or other penalties.</td>
</tr>
</tbody>
</table>

**Definition:**
Institutional Data subject to privacy or security considerations or any Institutional Data not designated as public, restricted, or regulated. Data is maintained in a physically secured location.

**Definition:**
Institutional Data where inadvertent disclosure or inappropriate access requires a breach notification in accordance with HRS §487N or is subject to financial fines. Social Security Number (SSN) and personal financial information fall within this category. Data is maintained in a physically secured location.

[Google@UH Drive](https://www.hawaii.edu/sitelic/dropbox)  
[UH Enterprise Dropbox](https://www.hawaii.edu/sitelic/dropbox)
Data Governance & Compliance

Sandra Furuto, Director, Data Governance
What is Data Governance

“...a framework that enables us to effectively manage data”

- Defines how data are collected, stored, and used
- Defines who can access data, when, and under what conditions
- Establishes decision rights
- Establishes clear lines of accountability
- Gives a voice to all appropriate parties
- Provides a mechanism for conflict resolutions involving data
UH Data Governance Goals

Protect the privacy and security of “Protected Data” (all non-public data)

• Produce higher quality data for informed decision making
• Promote efficient use of resources
• Increase transparency and accountability
Types of Protected Data

Institutional data
Supports administrative, academic operations (student, HR, finance)

Research data
Data created, collected, or analyzed for research
**EP2.214, Data Classification Categories**

<table>
<thead>
<tr>
<th>Category</th>
<th>Definition</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Access is not restricted and is subject to open records requests</td>
<td>Student directory information, employee’s business contact info</td>
</tr>
<tr>
<td>Restricted</td>
<td>Used for UH business only; will not be distributed to external parties; released externally only under the terms of a written MOA or contract</td>
<td>Student contact information, UH ID number</td>
</tr>
<tr>
<td>Sensitive</td>
<td>Data subject to privacy considerations</td>
<td>Date of birth, job applicant records, salary/payroll information, most student information, PII responses on sensitive topics (e.g., illegal activities, addiction, sex, housing/food insecurity, etc.)</td>
</tr>
<tr>
<td>Regulated</td>
<td>Inadvertent disclosure or inappropriate access requires a breach notification by law or is subject to financial fines</td>
<td>FN or first initial/LN in combination with SSN, driver license number, or bank information; credit card, FAFSA information; health information</td>
</tr>
<tr>
<td>Category</td>
<td>Public</td>
<td>Restricted</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------</td>
<td>------------</td>
</tr>
<tr>
<td>No risk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Student Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Major field of study</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Class (i.e., freshman, sophomore, etc.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Job title, description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business address, phone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Education &amp; training background</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Previous work experience</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dates of first and last employment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Position #, type of appointment, service computation date, occupational group or class code, BU unit code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Student Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UH email address / username</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address (street name, #)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal phone #</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Student &amp; Employee Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UH ID#</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Banner PIDM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ODS PIDM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address (street name, #)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal phone #</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Student &amp; Employee Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date of birth</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-UH email address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Job applicant records</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Salary &amp; payroll info</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PII responses on sensitive topics (illegal activities, addiction, sexual behavior and orientation, housing/food insecurity, etc.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FN / first initial and LN with the following:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Driver’s license</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hawai’i ID card #</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial account info, credit / debit card #s, etc.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business / Financial Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payment Card Industry Data Security Standard (PCI-DSS) info</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Health Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Individually identifiable health info (IIHI), HIPAA data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Aid (FAFSA) Data</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Per Executive Policy 2.214 - Institutional Data Classification Categories and Information Security Guidelines:

D. DATA SECURITY MEASURES: 1. Technical guidelines for each data classification category shall be followed to prevent the inadvertent exposure and inappropriate disclosure of Institutional Data that are considered Protected Data.

Source: https://www.hawaii.edu/infosec/minimum-standards/
ITS has mapped the Minimum Security Standards (MSS) against:

- Cybersecurity Maturity Model Certification (CMMC) Levels 1 to 3
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)

Points to remember:

- When working with Regulated Data, please refer to the applicable Standard, Act, or Policy for specific details on any additional controls needed.
- When comparing Standards, Acts, or Policies to the ITS MSS, the more stringent standard takes precedence.
- Standard, Act, or Policy requirements still apply when there is no equivalent ITS MSS.

Source: [https://www.hawaii.edu/infosec/minimum-standards/](https://www.hawaii.edu/infosec/minimum-standards/)
Data Classification Category Considerations

• Know your data and what data classification categories they fall under (Public, Restricted, Sensitive, Regulated)

• Your project will likely contain data elements from more than one data classification category

• Protect your records based on the data element with the highest level of sensitivity

• Consider all data involved in your project, even those not part of your research
  • E.g., Collecting SSNs from gift card recipients for 1099 tax forms

• Look at your entire project lifecycle; data security risk may vary at different points in your project
  • E.g., Collection of identified data may require more security, but once the identifiers have been removed, there is less security concerns
Purpose of Data Governance Process (DGP)

- **Inventory** where Protected Data is coming/going
- **Protect**
  - Security – review how data will be collected, stored, and used
  - Legal – ensure agreements have appropriate language that protects UH
- **Communicate**
  - Share within and between campuses
  - Provide notice to our data and IT providers
- **Assess risk**

https://datagov.intranet.hawaii.edu/dgp/
When a DGP is Required for Research (newly revised)

Projects that involve the collection, management, sharing, exchange, use and/or release of any of the following:

• Individually Identifiable Health Information (IIHI) or de-identified health data originally collected as IIHI
  • E.g., A study on COVID symptoms of individuals within the first two weeks of testing positive

• SSN (even if it is the last 4 digits) or birthdate (month/day/year)

• Student data originally collected or issued by UH for institutional purposes (i.e., related to the student’s education). This includes student contact information to identify or contact prospective human subjects.
  • E.g., Request an email list of current students or to use the UH Announce feature to invite students to sign up for a listserv to participate in research studies

• Surveys, interviews, focus groups, or observations that collect personally identifiable information (PII) on highly sensitive topics (e.g., illegal activities, addiction, sexual behavior and orientation, housing and food insecurity, etc.)
Submit to DGO:
1. DGP form for research
2. Proposed agreements (proposed vendor contract, BAA, DUA)
3. IRB approval letter
4. Other supporting materials

DGO Reviews

Clarify, resolve issues; revise draft contract/agreement language

DGP Workflow – Revision in Progress

https://datagov.intranet.hawaii.edu/dgp/

DGP criteria question in IRB application

Subject Matter Experts Review

VPIT Reviews / Approves

Send FYI to UHM VCR or VCAA (9 campuses)

Researcher proceeds with signing any agreements or purchasing software/services
Why DGP When We Already Have IRB?

**IRB**
- Protects against harm to individuals

**DGP**
- Reduce risk of exposure of individuals’ data / reducing risk to UH

Research data
If you are purchasing a subscription or software purchase that is low cost ($0-$2500, often purchased via Pcard), low risk, this process may apply to you

Separate from the DGP process
Tracks problematic language around indemnification and governing law only; no data considerations and security reviews

Your fiscal administrator may ask you to complete the OVPIT Non-compliant Terms Waiver

https://www.hawaii.edu/its/support-tools/
OVPIT Non-compliant Terms (Shrinkwrap Terms) Waiver (2)

When to use: Subscriptions/shrink-wrap purchases that have non-compliant terms

Step 1: Review vendor’s online terms and conditions:

- Indemnification
  Ex: “UH agrees to indemnify, defend or hold VENDOR harmless from damages or injuries…”

  https://www.hawaii.edu/offices/legal/contractspolicy/appendices/

- Governing law
  Check if state (or country) is not Hawai’i

Step 2: Ask vendor to modify or remove indemnification and/or governing law language (i.e., remain silent)

Step 3: If vendor does not agree, fill out form

https://www.hawaii.edu/its/support-tools/
## Key Regulations and Penalties (1)

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Description</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Family Educational Rights and Privacy Act (FERPA)</td>
<td>Federal law that protects the privacy of student education records • Access based on legitimate need to know • All student data are FERPA protected EXCEPT directory info • UH’s FERPA policy: AP7.022</td>
<td>Potential loss of federal financial aid funding</td>
</tr>
<tr>
<td>Higher Education Act (HEA)</td>
<td>Federal law that focuses on college affordability and access • <strong>Title IV</strong>: Provides student assistance through scholarships, low-interest loans, and work-study programs • Draft Federal Student Aid Strategic Plan, FY2020-24, may result in HEA update that requires more data protection and cybersecurity safeguards: <a href="https://studentaid.gov/sites/default/files/fy2024-strategic-plan-draft.pdf">https://studentaid.gov/sites/default/files/fy2024-strategic-plan-draft.pdf</a> • Strategic Goal 4: Strengthen Data Protection and Cybersecurity Safeguards—“Performance metrics” mentions <strong>assessment findings &amp; OMB compliance audits</strong> • <a href="https://www.archives.gov/cui/registry/category-detail/student-records">https://www.archives.gov/cui/registry/category-detail/student-records</a> • <strong>Section 117</strong>: Requires reporting of contracts with and gifts from a foreign source that, alone or combined, are &gt;=$250,000 per calendar year</td>
<td>Potential loss of federal financial aid funding</td>
</tr>
</tbody>
</table>
## Key Regulations and Penalties (2)

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Description</th>
<th>Penalty</th>
</tr>
</thead>
</table>
| **Gramm-Leach-Bliley Act (GLBA)**               | Federal law that requires financial institutions to explain how they share/protect customers’ data  
• Applies to higher ed because of financial aid  
• Recent revision to the Safeguards Rule requires more IT security controls  
• External auditors review institutional data systems that house financial aid data | Financial fines, convictions |
| **General Data Protection Regulation (GDPR)**   | A European Union (EU) consumer protection law that applies to companies collecting PII as part of delivering goods and services  
• Regulation extends to colleges and universities  
• Applies ONLY when an individual is physically in the EU | Financial fines           |
<table>
<thead>
<tr>
<th>Regulation</th>
<th>Description</th>
<th>Penalty</th>
</tr>
</thead>
</table>
| Hawai’i Revised Statutes (HRS) §487N | State law that defines the breach notification to the legislature  
• Written report to the legislature within 20 days after the discovery of a data breach  
• Data subject to regulation:  
  • FN or First Initial/LN combined with:  
    • SSN  
    • Driver license or state ID #  
    • Person’s financial account info (account #, access codes, passwords, etc.) | Possible conviction |
| Hawai’i Revised Statute (HRS) Chapter 92F |  
• State law also known as the Uniform Information Practices Act (UIPA) which requires open access to government records  
• Governs open records requests  
• Data subject to 92F-12:  
  • Employee data (e.g., name, salary range, bargaining unit, job title, business address/phone, employing agency, etc.) |  |
## Key Regulations and Penalties (4)

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Description</th>
<th>Penalty</th>
</tr>
</thead>
</table>
| Health Insurance Portability and Accountability Act (HIPAA) | Federal law that protects the privacy of health information  
• UH’s HIPAA policy: EP2.217                                                      | Financial fines; breach notification to DHHS (and possibly state leg under HRS §487N) |
| Payment Card Industry Data Security Standard (PCI-DSS) information | A widely accepted set of policies / procedures that protects cardholders’ credit/debit/cash card transactions  
• Contact Treasury Office for credit card set ups                                | Financial fines; breach notification under HRS §487N                       |
### Key Regulations and Penalties (5)

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Description</th>
<th>Penalty</th>
</tr>
</thead>
</table>
| National Institute of Standards and Technology Special Programs (NIST SP) 800-171 | Federal Department of Defense (DoD) standards aimed at safeguarding Controlled Unclassified Information (CUI)  
- DFARS Clause 252.204-7012  
- 110 controls in 14 areas (e.g., access, awareness and training, audits, incident response, risk assessment, etc.)  
- Interim DFARS Clause 252.204-7020  
  - Effective November 1, 2020  
  - Must submit a self assessment of 800-171 compliance on SPRS website before award | Various criminal, civil, administrative, or contract penalties |
| Cybersecurity Maturity Model Certification (CMMC) | A tiered approach to audit contractor compliance with NIST SP 800-171, based on five different levels of maturity expectations  
- DFARS Clause 252.204-7021  
- By Oct. 2025, CMMC certification will be required for ALL DoD contracts  
- Phased rollout  
- FY 21: 15 contractors will be selected (including subcontractors) | |
## Key Regulations and Penalties (6)

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Description</th>
<th>Penalty</th>
</tr>
</thead>
</table>
| Federal Acquisition Regulation (FAR) 52.204-25; Section 889(a)(1)(B) of the National Defense Authorization Act (NDAA) | • As of 8/13/20, government agencies are prohibited from contracting with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system  
  • Prohibition applies regardless of whether or not that usage is in performance of work under a Federal contract  
  • UH cannot purchase/use any telecom or video surveillance equipment or services from:  
    • Huawei Technologies Company  
    • ZTE Corporation  
    • Hytera Communications Corporation  
    • Hangzhou Hikvision Digital Technology Company  
    • Dahua Technology Company  
    • or any subsidiary or affiliate of these entities  
|                                                                            |                                                                                                                                                                                                             |         |
# Key Regulations and Penalties (7)

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Description</th>
<th>Penalty</th>
</tr>
</thead>
</table>
| National Industrial Security Program | • DoD Directive 5220.22-M  
• National Industrial Security Program Operating Manual  
• Classified data subject to regulation | |
| Biological Safety Program | • Governs all research, teaching, and testing activities involving infectious agents and recombinant materials | |
| Export Control & International Traffic in Arms Regulations (ITAR) | • Federal regulations that impose access, dissemination or participation restrictions on the use and/or transfer of commodities, technical data, or the provision of services subject to United States (US) export controls for reasons of national security, foreign policy, anti-terrorism or non-proliferation | |
Impact of Data Breaches / Exposures (Electronic & Paper)

- Loss of federal financial aid funding
- Financial fines
- Class action lawsuits
- Expenses, financial and human capital
- Loss of reputation / unfavorable publicity
- Legislative scrutiny
- Investigations by federal agencies / law enforcement
Questions?

Sandra Furuto, Data Governance Director, yano@hawaii.edu
Jodi Ito, Chief Information Security Officer, jodi@hawaii.edu
At the conclusion of this webinar, you will be asked to complete a short survey. Please share your feedback with us!

Presentation slides and recording
https://researchcompliance.hawaii.edu/
https://www.hawaii.edu/research/foreign-influence/

Office of Research Compliance
https://researchcompliance.hawaii.edu/

Information Security Team
infosec@hawaii.edu

Data Governance Office
datagov@hawaii.edu