Protecting UH Research
Fall 2020

December 3, 2020 (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
Today’s Agenda

• Welcome
• Issues & Threats Against Research
• Data Governance & Compliance
• Export Controls
• Foreign Influence
• Conflict of Interest Disclosure
Issues & Threats Against Research

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.

• Recent alerts: ransomware targeting healthcare & public health sectors: https://us-cert.cisa.gov/ncas/alerts/aa20-302a
Notable HE Ransomware Attacks

• University of California San Francisco paid out $1.14 million this June following an attack by Netwalker.

# Ransomware Gangs who Exfiltrate/Leak Stolen Data

<table>
<thead>
<tr>
<th>Avaddon</th>
<th>Light</th>
<th>ProLock</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cl0p</td>
<td>LockBit</td>
<td>RagnarLocker</td>
</tr>
<tr>
<td>Conti/Ryuk</td>
<td>Maze</td>
<td>RansomExx</td>
</tr>
<tr>
<td>CryLock</td>
<td>MountLocker</td>
<td>Ranzy/Ako</td>
</tr>
<tr>
<td>Crysis/Dharma</td>
<td>Nemty</td>
<td>Revil/Sodinokibi</td>
</tr>
<tr>
<td>DarkSide</td>
<td>Nefilim/Nephilim</td>
<td>Sekhmet</td>
</tr>
<tr>
<td>DoppelPaymer</td>
<td>Netwalker</td>
<td>Snake</td>
</tr>
<tr>
<td>Egregor</td>
<td>OldGremlin</td>
<td>Snatch</td>
</tr>
<tr>
<td>Fonix</td>
<td>Pysa/Mespinoza</td>
<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

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

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


HAWAII NEWS

2,400 were exposed to phishing scheme, UH tells lawmakers

By Tyne Phillips tphillips@staradvertiser.com
Posted January 25, 2018
|
January 25, 2018

Updated January 25, 2018 1:03am
• 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 Hawai‘i 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
Incident Summary

• UH was notified on 9/15/2017 that a UH researcher’s email account was used to send a malware-infected attachment to a targeted group of individuals (spear phishing)

• Analysis of the malware identified an external server that was used to download additional malware

• The external server was found to be communicating with 7 other UH computers (staff computers and servers) on a research department’s network; including the department’s Active Directory (AD) Domain Controller administrator accounts (keys to the kingdom)

• Attackers captured all of the department’s Active Directory user accounts and passwords

• INCLUDING the researcher’s email account and password that was used to send the malware-infected attachment

• Servers that were compromised contained Personally Identifiable Information (PII)
  • UH is required by Hawai‘i 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
• Very sophisticated attack; the malware imbedded in the email exploited a vulnerability that was announced just 3 days earlier on Sept. 12.

• **Attack started on Aug. 29, 2017** and was exposed on Sept. 15, 2017 when the infected email was sent to other institutions

• **Suspected reconnaissance appears to have started June 29, 2017 through Sept. 26, 2017**

• Reconnaissance emails were resumes from Chinese individuals with a web object that was downloaded from a Beijing mail server

• The web object was a 1x1 pixel, white graphic object and when the image was loaded, it was virtually undetectable

• The connection to download the object could provide additional information for the attackers such as IP addresses, usernames, operating system, web browser information, and email client information
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
More Federal Regulations

- 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](https://www.govinfo.gov/content/pkg/FR-2020-09-29/pdf/2020-21123.pdf)
- DFARS 252.204-7012: NIST 800-171 (Controlled Unclassified Information – CUI)
- Cybersecurity Maturity Model Certification
- 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 Requirements
- NDAA 889
Cyber Hygiene Best Practices

Cyber Hygiene is a set of best practices users should follow to improve the safety and security of their devices.

For detailed information on minimum security standards for Servers, Endpoint, and Multi-Function Devices based on UH Institutional Data Category type (Public, Restricted, Sensitive, and Regulated), please visit the following page: https://www.hawaii.edu/infosec/minimum-standards/

When working with Regulated Data, please refer to the applicable Standard, Act, or Policy (e.g., CMMC, PCI DSS, HIPAA, FERPA, NIST SP800-171, etc.) for specific details on any additional controls needed.

<table>
<thead>
<tr>
<th>Best Practice</th>
<th>Description</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Anti-Malware Software and Host Based Firewalls</td>
<td>Install Anti-Malware software and ensure its signatures are regularly updated. Anti-Malware software is a key protective measure to detect, quarantine, and remove various types of malware. McAfee anti-virus software is licensed by the University of Hawaii (UH), Information Technology Services (ITS) site license for use by active UH faculty, staff, and students: <a href="https://www.hawaii.edu/itskust1254">https://www.hawaii.edu/itskust1254</a> In addition to installing Anti-Malware software, most modern Operating Systems include built-in firewalls, which are commonly referred to as Host Based Firewalls. Host Based Firewalls run on your device and provide an additional layer of protection from network cyberattacks.</td>
<td>US-CERT Security Tip (ST18004) Protecting Against Malicious Code: <a href="https://us-cert.cisa.gov/naca/tips/ST18-271">https://us-cert.cisa.gov/naca/tips/ST18-271</a> ITS M5 S.8.1 — Ensure Anti-Malware Software and Signatures are Updated US-CERT Security Tip (ST04004) Understanding Firewalls for Home and Small Office Use: <a href="https://us-cert.cisa.gov/naca/tips/ST04-004">https://us-cert.cisa.gov/naca/tips/ST04-004</a> ITS M5 S.9.1 — Apply Host-Based Firewalls or Port Filtering</td>
</tr>
</tbody>
</table>

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/
UH Enterprise Dropbox

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><strong>Public (No Risk)</strong></td>
<td><strong>Restricted (Low Risk)</strong></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>
<tr>
<td><strong>Definition:</strong> Institutional Data where access is not restricted and is subject to open records requests</td>
<td><strong>Definition:</strong> Institutional Data used for UH business only. Restricted data will not be distributed to external parties except under the terms of a written memorandum of agreement or contract. Data is maintained in a physically secured location.</td>
</tr>
</tbody>
</table>

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

[Google@UH Drive](https://www.hawaii.edu/sitelic/dropbox/index.php)  
[UH Enterprise Dropbox](https://www.hawaii.edu/sitelic/dropbox/index.php)
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
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, demographic information (e.g., gender, ethnicity) or highly personal responses (e.g., drug, alcohol, sex)</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>Data Type</td>
<td>Public</td>
<td>Restricted</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------</td>
<td>------------</td>
</tr>
<tr>
<td>Student Data</td>
<td>No risk</td>
<td>Low risk</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</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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</td>
<td></td>
<td></td>
</tr>
<tr>
<td>employment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Position #, type of</td>
<td></td>
<td></td>
</tr>
<tr>
<td>appointment, service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>computation date,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>occupational group or</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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 /</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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>Student Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Gender</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Ethnicity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Grades</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Courses taken</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• GPA</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>(names, transcripts, etc.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Salary &amp; payroll information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-UH PII Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Contact info, gender,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ethnicity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Responses on sensitive</td>
<td></td>
<td></td>
</tr>
<tr>
<td>topics (drug, alcohol, sex)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Financial Aid (FAFSA) Data

Examples of Data / Information by Category from EP2.214:

- **Protected Data**
  - No risk
  - Low risk
  - Medium risk
  - High risk

- **Public**
  - Restricted
  - Sensitive
  - Regulated

- **Student Data**
  - UH email address / username
  - Address (street name, #)
  - Personal phone #
  - Banner PIDM
  - ODS PIDM

- **Employee Data**
  - Name
  - Job title, description
  - Business address, phone
  - Education & training background
  - Previous work experience
  - Dates of first and last employment
  - Position #, type of appointment, service computation date, occupational group or class code, BU unit code

- **Student & Employee Data**
  - UH ID#
  - Banner PIDM
  - ODS PIDM

- **Student Data**
  - Gender
  - Ethnicity
  - Grades
  - Courses taken
  - GPA

- **Employee Data**
  - Address (street name, #)
  - Personal phone #

- **Student & Employee Data**
  - Date of birth
  - Non-UH email address
  - Job applicant records (names, transcripts, etc.)

- **Non-UH PII Data**
  - Contact info, gender, ethnicity
  - Responses on sensitive topics (drug, alcohol, sex)
  - SSN
  - Driver's license
  - Hawai'i ID card #
  - Financial account info, credit / debit card #s, etc.

- **Business / Financial Data**
  - Payment Card Industry Data Security Standard (PCI-DSS) info

- **Health Information**
  - Individually identifiable health info (IIHI)
  - HIPAA data

- **Financial Aid (FAFSA) Data**

- **FN / first initial and LN with the following:**
  - SSN
  - Driver's license
  - Hawai'i ID card #
  - Financial account info, credit / debit card #s, etc.
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/
Summary: Data Classification Categories

• 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

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

• Personally identifiable data that is Sensitive and/or Regulated
  • E.g., Study that tracks symptoms of individuals with COVID-19

• Data originally collected for institutional purposes
  • E.g., Study on incentivizing students and seeing if it positively impacts their academic performance

• Data that involves UH community members as study participants
  • E.g., Survey on attitudes of UH Nursing students and (non-UH) professionals on COVID vaccinations

• De-identified health data, including Limited Data Sets
  • E.g., Participation in a consortium where multiple institutions are sharing de-identified health data

• Data that was originally PII or de-identified data that can be re-identified
  • E.g., Studies where data collected was personally identifiable then de-identified or identifiers are coded and retained indefinitely or when datasets can be combined and potentially identify individuals
Submit to DGO:
1. DGP form
2. Proposed agreements (proposed vendor contract, BAA, DUA)
3. IRB approval letter
4. Other supporting materials

Clarify, resolve issues; revise draft contract/agreement language

https://datagov.intranet.hawaii.edu/dgp/
Submit to DGO:
1. Shortened DGP form
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

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

https://datagov.intranet.hawaii.edu/dgp/
### Data Governance Process: What type of PII applies?

**Research vs Institutional Use**

<table>
<thead>
<tr>
<th>Protected Data</th>
<th>Public</th>
<th>Restricted</th>
<th>Sensitive</th>
<th>Regulated</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No risk</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Low risk</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Med risk</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>High risk</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Research</strong></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Institutional Use (e.g., student data)</strong></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Separate from the DGP process

Applies to subscription or shrink-wrap software purchases which are low cost (<$2500, purchased via Pcard), low risk

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

https://www.hawaii.edu/its/support-tools/

Tracks problematic language around indemnification and governing law only
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
# 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 assessment findings &amp; OMB compliance audits • <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.) |  |
| 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.) | Possible conviction |
### 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) |
New Interim DFARS Rules

• DFARS Clause 252.204-7020: NIST SP 800-171 DoD Assessment Methodology
  • Effective November 1, 2020
  • Must submit a self assessment of 800-171 compliance on SPRS website before award
    • https://www.sprs.csd.disa.mil/reference.htm

• DFARS Clause 252.204-7021: Cybersecurity Maturity Model Certification (CMMC)
  • By Oct. 2025, CMMC certification will be required for ALL DoD contracts
  • Phased rollout
  • FY 21: 15 contractors will be selected (including subcontractors)
OUSD(A&S) is working with Services and Agencies to identify candidate programs that will have the CMMC requirement during FY21-FY25 phased roll-out.

<p>| Total Number of New Prime Contracts Awarded Each Year with CMMC Requirement |</p>
<table>
<thead>
<tr>
<th>FY21</th>
<th>FY22</th>
<th>FY23</th>
<th>FY24</th>
<th>FY25</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>75</td>
<td>250</td>
<td>479</td>
<td>479</td>
</tr>
</tbody>
</table>

<p>| Total Number of Prime Contractors and Sub-Contractors with CMMC Requirement |</p>
<table>
<thead>
<tr>
<th>FY21</th>
<th>FY22</th>
<th>FY23</th>
<th>FY24</th>
<th>FY25</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>899</td>
<td>4,490</td>
<td>14,981</td>
<td>28,714</td>
</tr>
<tr>
<td>Level 2</td>
<td>149</td>
<td>749</td>
<td>2,497</td>
<td>4,786</td>
</tr>
<tr>
<td>Level 3</td>
<td>452</td>
<td>2,245</td>
<td>7,490</td>
<td>14,357</td>
</tr>
<tr>
<td>Level 4</td>
<td>0</td>
<td>8</td>
<td>16</td>
<td>24</td>
</tr>
<tr>
<td>Level 5</td>
<td>0</td>
<td>8</td>
<td>16</td>
<td>24</td>
</tr>
<tr>
<td>Total</td>
<td>1,500</td>
<td>7,500</td>
<td>25,000</td>
<td>47,905</td>
</tr>
</tbody>
</table>

- All new DoD contracts will contain the CMMC requirement starting in FY26
- Assumes for every unique prime contractor, there are ~ 100 unique subcontractors

DISTRIBUTION A. Approved for public release
### 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  
Federal Acquisition Regulation: Prohibition on Contracting With Entities Using Certain Telecommunications and Video Surveillance Services or Equipment

A Rule by the Defense Department, the General Services Administration, and the National Aeronautics and Space Administration on 07/14/2020

Agency:
Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA).

Action:
Interim rule.

Summary:
Section 889’s Two Prohibitions


- Part A: Effective **August 13, 2019**, the Government may not **obtain** (through a contract or other instrument) certain telecommunications equipment or services produced by five named Chinese companies or their subsidiaries and affiliates.

- 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.
  - Use is “regardless of whether that use is in performance of a Federal contract”
What does this mean?

• As of August 13, 2020, 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>
<tbody>
<tr>
<td>National Industrial Security Program</td>
<td>• DoD Directive 5220.22-M&lt;br&gt;• National Industrial Security Program Operating Manual&lt;br&gt;• Classified data subject to regulation</td>
<td></td>
</tr>
<tr>
<td>Biological Safety Program</td>
<td>• Governs all research, teaching, and testing activities involving infectious agents and recombinant materials</td>
<td></td>
</tr>
<tr>
<td>Export Control &amp; International Traffic in Arms Regulations (ITAR)</td>
<td>• 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</td>
<td></td>
</tr>
</tbody>
</table>
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
- Additional legislative scrutiny
- Investigations by federal agencies or federal law enforcement
<table>
<thead>
<tr>
<th>Item</th>
<th>Current AP</th>
<th>Proposed changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name change</td>
<td>Mandatory Training and Continuing Education Requirements for Data Users</td>
<td>Mandatory Training on Data Privacy and Security</td>
</tr>
<tr>
<td>To whom does the training apply</td>
<td>Data users with access to Protected Data in bulk quantities</td>
<td>All employees (including student employees and graduate assistants) with some exceptions</td>
</tr>
<tr>
<td>Who is exempt from the training</td>
<td>N/A</td>
<td>Those who meet all three criteria:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- duties are not office- or classroom-based</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- duties do not involve working with Protected Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- limited access to technology at work</td>
</tr>
<tr>
<td>When to complete the GCN</td>
<td>Annually</td>
<td>During the onboarding process for new hires</td>
</tr>
<tr>
<td>When to complete the ISAT</td>
<td>Every two years</td>
<td>During onboarding, then annually, based on the anniversary date of last ISAT taken</td>
</tr>
</tbody>
</table>
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/

Information Security Team
infosec@hawaii.edu

Data Governance Office
datagov@hawaii.edu