



Protecting UH Research Spring 2023 Briefing

Wednesday, March 8, 2023

10:30 – 12:00

(session will be recorded)



Today's Agenda

- Guest Speaker
Anthony Lang, Chief Division Counsel and SSA FBI HNL
- Jodi Ito, Vulnerabilities & Compliance
- Sandra Furuto, Data Governance
- Victoria Rivera, Disclosure Requirements & Conflict of Interest

PROTECTING UNIVERSITY OF HAWAII RESEARCH SPRING 2023

TONY LANG, FBI HONOLULU
DIVISION

UNCLASSIFIED//FOUO



HAWAII



WASHINGTON DC



FBI CYBER DIVISION: THREAT ANALYTICS COLLABORATION UNIT (FBI TACU)



- **Gryphon Citadel** is a unique set of integrated tools and processes developed by **FBI TACU** to detect and alert an organization to cyber threats.

GRYPHON CITADEL

Log Type Page Overview:

- Zeek/Bro; Apache; Cisco; Palo Alto;
- PFSense; Sophos; UTM; CSV;
- Netflow; CSV Weblog;
- Microsoft ISS; Microsoft ISS ALM;
- Microsoft O365; QoScient Argus; and Suricata



UNIVERSITIES/EDUCATION: RIPE TARGETS?

- TOP 5 INDUSTRIES MOST VULNERABLE TO CYBER ATTACKS IN 2022:
 - (1) FINANCIAL SERVICES;
 - (2) HEALTHCARE;
 - (3) **EDUCATION;**
 - (4) ENERGY & UTILITIES;
 - (5) GOVERNMENT AGENCIES

LOS ANGELES UNIFIED SCHOOL DISTRICT DATA BREACH – 10/2022

- Russian Speaking Hacking Group VICE SOCIETY unleashed RANSOMWARE with an October 4, 2022 DEADLINE --- leaked 500GB data containing:
 - (a) PII – SS#s;
 - (b) tax forms;
 - (c) passport information;
 - (d) contact and legal documents;
 - (e) bank account details;
 - (f) health information;
 - (g) conviction reports; and
 - (h) psychological assessments of students.



#1 – PII & PHI

- Financial Data of Students, applicants, faculty, staff, and alumni.
- Financial data of season ticket holders – sports and theaters.
- Campus parking permits have driver's license and vehicle data.
- Medical research facilities have patient data.



PII/PHI – UNIVERSITY CASE STUDY

- FACTS:
- FBI notifies a University that foreign actors hacked into two servers!
- One of the servers could have been used as a pivot point to access student and faculty PII.
- University uses this opportunity to engage a computer forensics company to remediate this incident.
- University uses this incident to re-evaluate their computer security posture and upgrades various network security infrastructure and controls.
- Foreign Actor Motivation – Dissidents – PII and financial data not exfiltrated.



#2 – INTELLECTUAL PROPERTY

- Engineering, computer science and other hard sciences
- Classified research – DOD contracts/other US Government agencies



#2- INTELLECTUAL PROPERTY: CASE STUDY – SPEAR PHISHING

- A prominent California University professor receives a spear-phish email.
- The Professor is an expert in a certain region's political landscape.
- FBI contacts the Professor on his cell phone and explains their e-mail and computer may be compromised.
- FBI meets with Professor, Chief Information Security Officer (CISO), Legal and IT Department where FBI discovers that large e-mail attachments not scanned by University due to performance reasons.
- FBI assists University with forensic analysis.



#3 - BANDWIDTH

- Looking at large data pipes or hop-points.
- The threat actors have typically accessed hop points, from various China-based internet protocol addresses that pointed to different Chinese internet service providers (ISPs).
- The servers allow them to access operational email accounts and host domains.
- Armed with those credentials, threat actors can reroute traffic to infrastructure they command.



#3 – BANDWIDTH – CASE STUDY

- FBI identified Russian cyber attackers were proxying through University networks since they have fast network links to target systems and their traffic appears more legitimate than a connection from Moscow.
- FBI installed the network equivalents of wire-taps at a number of the compromised universities that the attackers were moving through.
- Now they could watch the attackers as they typed out their commands. They discovered the attackers were using the standard tools to move through networks and steal documents without standing out.



#4 – IT INFRASTRUCTURE

- Use of open or low security networks for criminal purposes –
 - (a) innocent images;
 - (b) forums;
 - (c) botnets;
 - (d) DDoS.



#4 – IT INFRASTRUCTURE: CASE STUDIES.....

- INNOCENT IMAGES –
 - (a) Open or weak security for campus Wi-Fi'
 - (b) Led to individuals uploading child pornography on University's network; and
 - © Could also be committed by university employees and/or students.
- CREDIT CARD HACKING FORUM-
 - (a) FBI and Secret Service notified
 - (b) DDoS attack



FINAL THOUGHTS...QUESTIONS?

- PARTNERSHIP WITH THE FBI & LAW ENFORCEMENT BENEFITS:
 - (a) Acts as a deterrence to potential hackers;
 - (b) Computer intrusion may have national security implications;
 - (c) Pre-established FBI Honolulu Division POC for computer intrusions, malware infections, FLASH, PINS, Joint Indicators Bulletins and vulnerability notification = **Gryphon Citadel**.
 - (d) FBI does not have “full” visibility into our adversaries and needs your assistance.
- QUESTIONS? aklang@fbi.gov OR (808) 479-7439





Vulnerabilities & Compliance

Jodi Ito

UH Chief Information Security Officer

jodi@hawaii.edu

JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA22-277A

October 4, 2022



Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization

SUMMARY

From November 2021 through January 2022, the Cybersecurity and Infrastructure Security Agency (CISA) responded to advanced persistent threat (APT) activity on a Defense Industrial Base (DIB) Sector organization's enterprise network. During incident response activities, CISA uncovered that likely multiple APT groups compromised the organization's network, and some APT actors had long-term access to the environment. APT actors used an open-source toolkit called Impacket to gain their foothold within the environment and further compromise the network, and also used a custom data exfiltration tool, CovalentStealer, to steal the victim's sensitive data.

This joint Cybersecurity Advisory (CSA) provides APT actors tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) identified during the incident response activities by CISA and a third-party incident response organization. The CSA includes detection and mitigation actions to help organizations detect and prevent related APT activity. CISA, the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) recommend DIB sector and other critical infrastructure organizations implement the mitigations in this CSA to ensure they are managing and reducing the impact of cyber threats to their networks.

Actions to Help Protect Against APT Cyber Activity.

- Enforce multifactor authentication (MFA) on all user accounts.
- Implement network segmentation to separate network segments based on role and functionality.
- Update software, including operating systems, applications, and firmware, on network assets.
- Audit account usage.



Table 1: Top CVEs most used by Chinese state-sponsored cyber actors since 2020

| Vendor | CVE | Vulnerability Type |
|--|----------------|--------------------------------------|
| Apache Log4j | CVE-2021-44228 | Remote Code Execution |
| Pulse Connect Secure | CVE-2019-11510 | Arbitrary File Read |
| GitLab CE/EE | CVE-2021-22205 | Remote Code Execution |
| Atlassian | CVE-2022-26134 | Remote Code Execution |
| Microsoft Exchange | CVE-2021-26855 | Remote Code Execution |
| F5 Big-IP | CVE-2020-5902 | Remote Code Execution |
| VMware vCenter Server | CVE-2021-22005 | Arbitrary File Upload |
| Citrix ADC | CVE-2019-19781 | Path Traversal |
| Cisco Hyperflex | CVE-2021-1497 | Command Line Execution |
| Buffalo WSR | CVE-2021-20090 | Relative Path Traversal |
| Atlassian Confluence Server and Data Center | CVE-2021-26084 | Remote Code Execution |
| Hikvision Webserver | CVE-2021-36260 | Command Injection |
| Sitecore XP | CVE-2021-42237 | Remote Code Execution |
| F5 Big-IP | CVE-2022-1388 | Remote Code Execution |
| Apache | CVE-2022-24112 | Authentication Bypass by Spoofing |
| ZOHO | CVE-2021-40539 | Remote Code Execution |
| Microsoft | CVE-2021-26857 | Remote Code Execution |
| Microsoft | CVE-2021-26858 | Remote Code Execution |
| Microsoft | CVE-2021-27065 | Remote Code Execution |
| Apache HTTP Server | CVE-2021-41773 | Path Traversal |

These state-sponsored actors continue to use virtual private networks (VPNs) to obfuscate their activities and target web-facing applications to establish initial access.

Many of the CVEs indicated in Table 1 allow the actors to surreptitiously gain unauthorized access into sensitive networks, after which they seek to establish persistence and move laterally to other internally connected networks.



VULNERABILITIES

CVE-2022-42475 Detail

Description

A heap-based buffer overflow vulnerability [CWE-122] in FortiOS SSL-VPN 7.2.0 through 7.2.2, 7.0.0 through 7.0.8, 6.4.0 through 6.4.10, 6.2.0 through 6.2.11, 6.0.15 and earlier and FortiProxy SSL-VPN 7.2.0 through 7.2.1, 7.0.7 and earlier may allow a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests.

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:

**CNA:** Fortinet, Inc.**Base Score:** 9.8 CRITICAL**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: The NVD and the CNA have provided the same score. When this occurs only the CNA information is displayed, but the Acceptance Level icon for the CNA is given a checkmark to signify NVD concurrence.

QUICK INFO

CVE Dictionary Entry:[CVE-2022-42475](#)**NVD Published Date:**

01/02/2023

NVD Last Modified:

01/09/2023

Source:

Fortinet, Inc.



David Merian

Jan 11 · 2 min read · ✨ Member-only · [Listen](#)



ChatGPT hacking tools for bug bounty, pentesting, blue teams, and more

Hackers aren't shy in exploiting brilliant tools like ChatGPT. They have used ChatGPT's capabilities to speed up script writing, automation, bug bounty reporting, nmap scans, and more.

<https://systemweakness.com/chatgpt-hacking-tools-for-bug-bounty-pentesting-blue-teams-and-more-c445698d23f>



Using ChatGPT to Write a Phishing Email



You are an HR representative with the University of Hawaii named Alice V. Write an email in english with some local hawaiian influences to Bob notifying them of changes to their tax records and request that they review the attached documents. The language should be somewhat casual.



Aloha Bob,

Howzit? I hope you're doing well.

I'm reaching out to you because there have been some updates to your tax records that I wanted to make you aware of. I've attached the necessary documents for your review.

Please take a look and let me know if you have any questions or concerns. I'm happy to help in any way I can.

Mahalo for your time and attention to this matter.

Warmest regards,

Alice V.





ChatGPT and other AI / LLM* issues

Subscribe

Latest Issues

SCIENTIFIC
AMERICAN®

Cart

0

Sign In | Newsletters

COVID

Health

Mind & Brain

Environment

Technology

Space & Physics

Video

Podcasts

Opinion

Store



nature

ARTIFICIAL INTELLIGENCE

Research Summaries Written by AI Fool Scientists

Scientists cannot always differentiate between research abstracts generated by the AI ChatGPT and those written by humans

By Holly Else, Nature magazine on January 13, 2023

*LLM: Large Language Model

<https://www.scientificamerican.com/article/research-summaries-written-by-ai-fool-scientists/#>

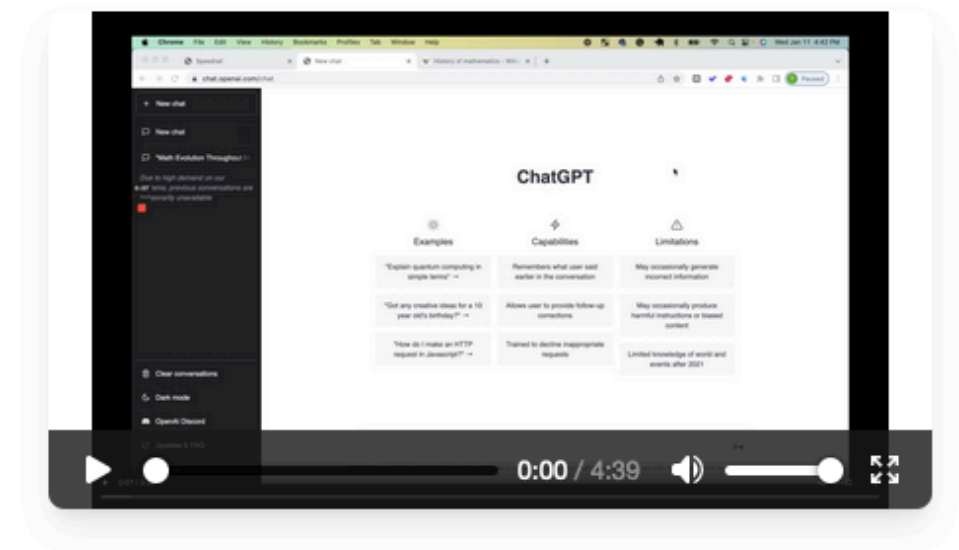
<https://www.chatgptplagiarism.com/>

Introducing ChatGPT Plagiarism

Find out if your students are using ChatGPT or other AI for their assignments.

Are you interested in institutional licensing? Get in touch with us today to schedule a demo!

Book Demo





UH Incidents & Initiatives



IoT, MFD, Unsecure Devices on UH Network

- Please remember that when connecting to any UH network your device will receive a public IP address that allows for actors to actively exploit or brute force access unless behind a department firewall
- Most devices are never meant to be public facing without enabling security controls, minimum security standards should be applied before connecting to UH network
<https://www.hawaii.edu/infosec/assets/minimum-standards/implementation-guides/>
- Check with your department IT staff or appliance vendor if you are unsure about connecting your devices with sensitive information.



OneScreen Vulnerability

- OneScreen is a smart display with touchscreen capabilities
- Android OS with “userdebug” mode on by default
- Attacker gains root access by connecting to TCP port 5555 via the ADB protocol
- Compromised when connected to a network
- Used as a proxy and used to attack other networks



Multi-function Devices/Printers on UH Network

- MFD's on public network can be a security risk if not configured properly. Recent scans identified SMB shares on printers that contained sensitive/regulated data.
- Ability to save scans to local drive should be disabled unless the following at minimum is enabled
 - Full-disk encryption to comply with regulatory requirements for PHI, PII
 - Proper access control so scans are saved to folders restricted to the intended users. (Saving files to 1 accessible location is not acceptable as others with access to the folder would allow for unauthorized access.)
 - Administrator passwords should be changed to a strong and unique password.
 - HTTPS should be enabled on the web interface to avoid credentials being intercepted.



GLBA MFA Requirement

- Basic information about GLBA and how it applies to UH:
 - <https://www.hawaii.edu/infosec/glba/>
- From: <https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know>
 - **“Implement multi-factor authentication for anyone accessing customer information on your system.”**
- It is already implemented at UH login but is NOT mandatory yet
- ITS is still working on details of implementation
- Expecting to distribute USB tokens for those that do not have cell phones
- More information will be forthcoming this semester



Implementation of Proofpoint

- Recognized industry leader in email protection, threat detection, and response solutions to help secure against phishing attacks, malware, and other advanced threats
- Implementation will be done slowly over this calendar year
- Additional webinars about Proofpoint will be offered



Research Regulations & Compliance Update



CMMC Update

- Cybersecurity Maturity Model Certification (CMMC)
- Requires 3rd party certification (essentially for NIST 800-171)
- Will NOT be released as an Interim Rule in March
- Not included in the current Unified Agenda as a Proposed Rule
 - <https://www.reginfo.gov/public/do/eAgendaMain>
- DOD is still reviewing it
 - Will require 60 day public comment period
 - DOD needs to respond to every comment received
- Guesstimate: Rule may be finalized in 2024
- <https://dodcio.defense.gov/CMMC/About/>
- <https://www.projectspectrum.io/#/>



NSPM-33 & Guidance

- NSPM-33 established national security policy for US Government-supported R&D (issued Jan. 14, 2021)
- “Guidance For Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development” (Jan. 2022)
- PDF: <https://go.hawaii.edu/25C>
- Issued by National Science and Technology Council Subcommittee on Research Security, Joint Committee on the Research Environment



The purpose of this document is to provide guidance to Federal departments and agencies regarding their implementation of NSPM-33. The guidance does not create or confer any rights for or on any person or entity and does not operate to bind any department or agency of the U.S. Government or the public. It includes general guidance that agencies should apply across their implementation efforts, followed by more detailed guidance in five key areas addressed in NSPM-33:

1. Disclosure Requirements and Standardization
2. Digital Persistent Identifiers
3. Consequences for Violation of Disclosure Requirements
4. Information Sharing
5. Research Security Programs



Standardized Disclosure & Conflict of Interest

- Update in August 2022: <https://www.whitehouse.gov/ostp/news-updates/2022/08/31/an-update-on-research-securitystreamlining-disclosure-standards-to-enhance-clarity-transparency-and-equity/>
- Standardized data fields and instructions for disclosure of information
- <https://www.federalregister.gov/documents/2022/08/31/2022-18746/agency-information-collection-activities-request-for-comment-regarding-common-disclosure-forms-for>
- National Science Foundation assigned the lead

US FCC bans sales, import of Chinese tech from Huawei, ZTE

an hour ago

November 25, 2022



Click to copy

RELATED TOPICS

[Joe Biden](#)

[Technology](#)

[Trending News](#)

[Business](#)

[China](#)

[Donald Trump](#)

[National security](#)

“Our unanimous decision represents the first time in FCC history that we have voted to prohibit the authorization of new equipment based on national security concerns,” tweeted Brendan Carr, a Republican FCC commissioner.

Carr added that as “a result of our order, no new Huawei or ZTE equipment can be approved. And no new Dahua, Hikvision, or Hytera gear can be approved unless they assure the FCC that their gear won’t be used for public safety, security of government facilities, & other national security purposes.”

Hikvision said in a statement that its video products “present no security threat” to the U.S. but the FCC’s decision “will do a great deal to make it more harmful and more expensive for US small businesses, local authorities, school districts, and individual consumers to protect themselves, their homes, businesses and property.”

DOJ's Civil Cyber-Fraud Initiative Secures More Than \$9 Million in Two False Claims Act Settlements for Alleged Cybersecurity Violations



By **Ryan P. Blaney** and **Matthew J. Westbrook** on July 21, 2022

Posted in **Cybersecurity, Data Privacy Laws, Invasion of Privacy, Legislation, Privacy Law, Privacy Litigation**

Last fall, the United States Department of Justice ("DOJ") launched its **Civil Cyber-Fraud Initiative** ("CCFI") as part of its effort to "combat new and emerging cyber threats to the security of sensitive information and critical systems." Led by the Civil Fraud Section of DOJ's Commercial Litigation Branch, the CCFI leverages the False Claims Act ("FCA") to prosecute, in part, government contractors and federal grant recipients for cybersecurity-related fraud.

<https://privacylaw.proskauer.com/2022/07/articles/cybersecurity/dojs-civil-cyber-fraud-initiative-secures-more-than-9-million-in-two-false-claims-act-settlements-for-alleged-cybersecurity-violations/>



Civil Cyber-Fraud Initiative Settlements

The CCFI secured its **first settlement** in March 2022 in the Eastern District of New York. Comprehensive Health Services ("CHS") of Cape Canaveral, Florida, agreed to pay \$930,000 to resolve allegations that it violated the FCA by falsely representing compliance with contract requirements relating to the provision of medical services at State Department and Air Force facilities in Iraq and Afghanistan. In the settlement agreement, DOJ specifically alleged that CHS failed to store medical records on a secure electronic medical record system. According to DOJ some of the medical records were saved to an unsecured internal network drive and improperly made accessible to non-clinical staff. According to DOJ, this constituted a direct violation of government contractual requirements and raised numerous privacy concerns. In **announcing the settlement**, DOJ reiterated its priority to curb cybersecurity violations that place "confidential medical records risk."

About four months after its resolution with CHS, **DOJ announced** that a defense contractor agreed to pay \$9 million to resolve allegations that it violated the FCA by allegedly misrepresenting its compliance with cybersecurity requirements in certain federal government contracts, including contracts with the Department of Defense and NASA.



NSF Research Security: <https://beta.nsf.gov/research-security>

The National Science Foundation (NSF) is committed to safeguarding the integrity and security of science while also keeping fundamental research open and collaborative. NSF seeks to address an age of new threats and challenges through close work with our partners in academia, law enforcement, intelligence and other federal agencies. By fostering transparency, disclosure and other practices that reflect the values of research integrity, NSF is helping to lead the way in ensuring taxpayer-funded research remains secure.

NSF's research security initiatives seek to:

- Continue to increase the clarity and comprehensiveness of the Foundation's disclosure requirements;
- Coordinate with U.S. government interagency partners to harmonize disclosure information to the extent practicable;
- Communicate and build awareness with the scientific community;
- Share knowledge and best practices;
- Improve transparency and clarification for disclosure; and
- Mitigate risk through assessment and analysis to better understand the scale and scope.

NSF's Actions in Research Security



Credit: National Science Foundation

[View the high resolution PDF image here](#)



Foreign Interference in the NSF Funding and Grant Making Processes: A summary of findings from 2019 to 2021

For decades, open and collaborative fundamental research has served as a scientific and economic boon to the U.S. and the world. The science and engineering enterprise, however, is put at risk when other governments endeavor to benefit from it without upholding the values of openness, transparency and reciprocal collaboration. Some governments are actively sponsoring activities that pose risks to this system, such as foreign-government-sponsored talent recruitment programs that incentivize behavior that is inconsistent with these values.

NSF recognizes this threat and has taken action to mitigate threats while also reinforcing that collaboration, including international collaboration, is integral to our continued scientific advancement. In 2019, NSF commissioned the JASON advisory group, outside experts who specialize in both science and security, to conduct a study and recommend ways for NSF to protect research integrity and maintain balance between openness and security of scientific research. The report, [Fundamental Research Security](#), was published in December 2019 and serves as the underpinning for NSF's actions to mitigate these risks in concert with other agencies and stakeholders.

RESEARCH SECURITY



Photo Credit: Sarah Kachoo



ADMINISTRATIVE ACTIONS

Figures as of March 23, 2022

NSF has taken a range of actions against individuals and entities associated with foreign talent programs or organizations receiving foreign funding, based on recommendations by the OIG. In many cases, actions were taken based on grant fraud or other wrongful conduct (or allegations thereof) before any foreign affiliation was surfaced to NSF.



AWARD SUSPENSION

31 awards
suspended*



AWARD TERMINATION

20 awards
terminated



FINAL PAYMENT CANCELED

Final payment cancelled to

1 organization on
1 award



GOVERNMENT-WIDE SUSPENSION

15 government-wide suspensions issued for
9 researchers and **4** entities.

One researcher and one entity were suspended twice.



DEBARMENT

4 researchers and
2 entities debarred



VOLUNTARY EXCLUSIONS

5 researchers and
1 entity agreed to voluntary
exclusions following notices
of proposed debarments
by NSF



BAR ON SERVING AS A REVIEWER, PANELIST OR CONSULTANT

16 individuals barred from serving
as reviewers
15 of these bars arose from government-wide
debarments, government-wide suspensions,
or voluntary exclusion agreements.

Collectively, collaborations with the OIG to date have resulted in:



Grant funds recovered by NSF



Other entities
involved



Organizations of
higher education/
small businesses
involved*

*Note: These numbers are
approximate due to pending cases.



Researchers
involved

*Note: Suspensions were lifted for a small subset of these awards based on OIG recommendations or responsive actions taken by the organization (e.g., removal of PI under OIG investigation).

**Note: This total includes funds that may have eventually been paid out under the awards; however, when there was risk to NSF of misuse or fraud, they were protected.



The LOS ALAMOS CLUB

<https://go.hawaii.edu/25T>

How the People's Republic of China Recruited Leading
Scientists from Los Alamos National Laboratory to
Advance Its Military Programs





 [View image credit & caption](#)

NSF News

NSF 2022 Research Security Training for the United States Research Community awardees announced

December 9, 2022

<https://beta.nsf.gov/news/nsf-2022-research-security-training-united-states>

Share



Related stories





- [Research Security Training: The Importance of Research Security](#), The University of Alabama in Huntsville.
The team will develop research security training that provides information and insights about best practices in designing, developing and evaluating educational tools for the adult learner. The training module will focus on the importance of research security, enhance awareness and provide online training about existing and emerging risks and threats to the global research ecosystem. This project is funded with a contribution from NSF's [EPSCoR](#) program.
- [Research Security Training: The Importance of Disclosure](#), Texas A&M University System.
The team will design and develop a training module about research security that will focus on the importance of properly disclosing information when proposing for and conducting federally funded research, increase awareness and understanding of the current disclosure process, and clarify the importance of transparency and risks associated with non-disclosure. The Texas A&M team is part of a consortium that includes the Texas A&M Engineering Experiment Station, the Texas A&M University System Administrative and General Offices and Redcliff Enterprises.
- [Research Security Training: Risk Management and Mitigation](#), University of Pennsylvania.
The team will develop a research security training module based on an assessment of current research security understanding and knowledge gaps among researchers. The module will examine actions researchers and their institutions can take to assess, reduce and manage security risks to ongoing, planned and unpublished research data. Institutions will be able to modify the training module to incorporate local practices. The University of Pennsylvania team is part of a consortium that includes the University of Madison at Wisconsin, the University of Chicago, Regents University of Michigan and the University of Pittsburgh.
- [Research Security Training: International Collaboration](#), Associated Universities, Inc., and AUI Labs
The team will create an online research security training module focused on the importance of principled international collaboration and ongoing threats posed to scientific research security by improper foreign government influence. The training module will be customized for specific stakeholder groups in the U.S. research ecosystem and use hypothetical scenarios and real-world case studies to propel learners through advanced levels of knowledge and skills.



Key Regulations and Penalties – Research-related (1)

| Regulation | Description | Penalty |
|---|---|--|
| National Institute of Standards and Technology Special Programs (NIST SP) 800-171 | <p>Federal Department of Defense (DoD) standards aimed at safeguarding Controlled Unclassified Information (CUI)</p> <ul style="list-style-type: none">• 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<ul style="list-style-type: none">• 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) | <p>A tiered approach to audit contractor compliance with NIST SP 800-171, based on five different levels of maturity expectations</p> <ul style="list-style-type: none">• DFARS Clause 252.204-7021• By Oct. 2025, CMMC certification will be required for ALL DoD contracts• Phased rollout | |



Key Regulations and Penalties – Research-related (2)

| Regulation | Description | Penalty |
|---|---|---------|
| Federal Acquisition Regulation (FAR) 52.204-25; Section 889(a)(1)(B) of the National Defense Authorization Act (NDAA) | <ul style="list-style-type: none">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 systemProhibition applies regardless of <u>whether or not</u> that usage is in performance of work under a Federal contractUH cannot purchase/use any telecom or video surveillance equipment or services from:<ul style="list-style-type: none">Huawei Technologies CompanyZTE CorporationHytera Communications CorporationHangzhou Hikvision Digital Technology CompanyDahua Technology Companyor any subsidiary or affiliate of these entitieshttps://www.federalregister.gov/documents/2020/07/14/2020-15293/federal-acquisition-regulation-prohibition-on-contracting-with-entities-using-certain | |



Key Regulations and Penalties – Research-related (3)

| Regulation | Description | Penalty |
|---|---|---------|
| National Industrial Security Program | <ul style="list-style-type: none">• DoD Directive 5220.22-M• National Industrial Security Program Operating Manual• Classified data subject to regulation | |
| Biological Safety Program | <ul style="list-style-type: none">• Governs all research, teaching, and testing activities involving infectious agents and recombinant materials | |
| Export Control & International Traffic in Arms Regulations (ITAR) | <ul style="list-style-type: none">• 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 | |



Data Governance

Sandra Furuto

UH Data Governance Goals



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

- Produce higher quality data for 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

Protected
Data

| Category | Definition | Examples |
|------------|---|--|
| Public | Access is not restricted and is subject to open records requests | Student directory information, employee's business contact info |
| Restricted | Used for UH business only; will not be distributed to external parties; released externally only under the terms of a written MOA or contract | Student contact information, UH ID number |
| Sensitive | Data subject to privacy considerations | 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.) |
| Regulated | Inadvertent disclosure or inappropriate access requires a breach notification by law or is subject to financial fines | FN or first initial/LN in combination with SSN , driver license number, or bank information; credit card, FAFSA information; health information |



Examples of Data / Information by Category from EP2.214

| | Protected Data | | |
|--|--|--|---|
| Public | Restricted | Sensitive | Regulated |
| No risk | Low risk | Medium risk | High risk |
| <p>Student Data</p> <ul style="list-style-type: none"> Name Major field of study Class (i.e., freshman, sophomore, etc.) <p>Employee Data</p> <ul style="list-style-type: none"> 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 | <p>Student Data</p> <ul style="list-style-type: none"> UH email address / username Address (street name, #) Personal phone # <p>Student & Employee Data</p> <ul style="list-style-type: none"> UH ID# Banner PIDM ODS PIDM | <p>Student Data</p> <ul style="list-style-type: none"> Gender, ethnicity, grades, courses taken, GPA <p>Employee Data</p> <ul style="list-style-type: none"> Address (street name, #) Personal phone # <p>Student & Employee Data</p> <ul style="list-style-type: none"> Date of birth Non-UH email address Job applicant records Salary & payroll info <p>Other Data</p> <ul style="list-style-type: none"> PII responses on sensitive topics (illegal activities, addiction, sexual behavior and orientation, housing/food insecurity, etc.) | <p>FN / first initial and LN with the following:</p> <ul style="list-style-type: none"> SSN Driver's license Hawai'i ID card # Financial account info, credit / debit card #s, etc. <p>Business / Financial Data</p> <ul style="list-style-type: none"> Payment Card Industry Data Security Standard (PCI-DSS) info <p>Health Information</p> <ul style="list-style-type: none"> Individually identifiable health info (IIHI), HIPAA data <p>Financial Aid (FAFSA) Data</p> |



Data Classification Category Considerations

- Know your data, know your UH data classification categories
- Data elements likely in more than one data classification category
- Protect records based on data elements with the highest sensitivity
- Consider all data involved in your project
 - E.g., Assessments plus surveys and interviews
- Data security risk may vary over your project lifecycle
 - E.g., Collection of PII (higher risk), later de-identified (lower risk)



Purpose of Data Governance Process (DGP)

DATA GOVERNANCE PROCESS (DGP) REQUEST

Instructions

Complete this form if your request involves Protected Data (i.e., Restricted, Sensitive, and/or Regulated Data). See [here](#) for examples of data types. See [here](#) for more detailed guidelines on when a DGP request is required.

RENEWALS AND REVISIONS

This Kuai Build DGP request must be submitted and approved before submitting a [Kuai Build DGP Revision request](#). A DGP request submitted in Cognito Forms, i.e., before March 1, 2022 (03/01/2022) is no longer valid to reference for renewals and revisions.

- RENEWALS/EXTENSIONS: Email datagov@hawaii.edu if there are no substantive changes* to the previously approved Kuai Build DGP request, and we will add a post-approval note to your approved Kuai Build DGP form. For example, an extension to the service period or project end date is considered a non-substantive change.
- REVISIONS/CHANGES: Submit a [Revision to a Previously Approved Data Governance Process \(DGP\) Request form](#) (i.e., Kuai Build DGP Revision request) if any conditions will substantively change* since the original Kuai Build DGP request was approved.
- COMPLEX REVISIONS/CHANGES: Submit a new [DGP Request form](#) if the changes are too complex to be captured by the Revision to a Previously Approved DGP Request form.

*Substantive changes include a new contact person, change in UH users who have data access, change in scope of task/project, change to contract terms and conditions, adding more data elements, change in IP address, etc. Changes to the service period or project end date are NOT considered substantive changes.

I. GENERAL INFORMATION

A. REQUESTER'S INFORMATION

| | |
|--------------------------------------|--|
| Requester's Name * | Requester's Email Address |
| Sandra K. Furuto (yano@hawaii.edu) x | UH Email will auto-populate after completing Name field yano@hawaii.edu |
| Requester's UH Campus / System * | Requester's Department/Office * |
| ... | Enter your department/office |

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

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

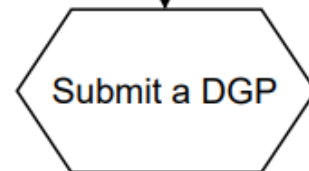


Research Data that Requires a DGP

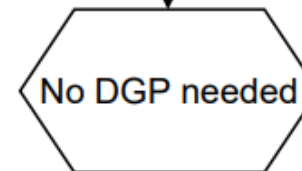
Does your project involve any of the following:

- 1. Health (medical record sourced/related) data (identified and de-identified)**
 - E.g., A study on COVID symptoms of individuals within the first two weeks of testing positive, setting up a telehealth service, or transferring de-identified datasets to partner institutions
- 2. Social Security Number (even if it is the last 4 digits) or full birthdate (month/day/year)**
- 3. 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 using the UH Announce feature to invite students to sign up for a listserv to participate in research studies
- 4. 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.)**

YES



NO





DGP Materials Required

- DGP request: <https://datagov.intranet.hawaii.edu/dgp/>
- Unsigned agreement (MOA/MOU, DUA/DSA/DTA, vendor contract, online terms)
- IRB approval letter
- Other supporting materials

DGP approvals typically take 1 week for research requests if we have all of the information we need.

Need help? DGO Open Hours: go.hawaii.edu/kkf



Non-compliant Terms (1)

Indemnification

- Look for language in vendor's online terms and conditions near the bottom

Ex: "UH agrees to indemnify, defend, or hold the other party harmless..."

By state statute, UH cannot agree to indemnify a third party (there are 4 rare exceptions). FYI, to agree means that UH will:

- Defend the third party, which includes paying for defense costs; and
 - Pay for any monetary judgment
- Ask vendor to remove language or accept alternate language available at EP8.200, Attachment 12 ("University responsibility" on page 2)



Non-compliant Terms (2)

Governing law

- Look for language in vendor's online terms and conditions near the bottom
Ex: "governed by...." or "subject to the jurisdiction of..." another state or country
To accept means that UH will be subject to that state or country's laws
 - May be more difficult or need to hire outside counsel
- Ask vendor to change to Hawaii or remove language
 - If vendor agrees, exclude from the waiver



Clarification on DGP and PI Responsibilities

- DGP approval allows the use of Protected Data for a specific purpose
 - Security and agreement terms were reviewed, modified as needed; risk was deemed acceptable
- PI responsibilities
 - Know your data and manage it according to the agreement terms
 - After DGP approval, route unsigned agreements for signature



Who Signs Agreements?

| Type of Agreements | Signature #1 | Signature #2 | Signature #3 |
|------------------------|----------------------------|------------------------|------------------------|
| HIPAA (System) | PI | Provost/ Chancellor | VPIT |
| HIPAA (Campus) | PI | VPIT | Provost/ Chancellor |
| No Cost DUA/DSA/DTA | PI | Dean/ Director | VPIT |
| Procurement Related | Check with FA for guidance | | |



Data Governance Principles and Guidelines

- Access based on need-to-know
- Grant minimal access to data
- Use de-identified data when possible
- No re-purposing or re-disclosure without permission
- Protect records based on data with the highest level of sensitivity
- Combinations of data elements, small cell sizes may become PII
- Remove duplicate data
- De-identify or destroy data when no longer needed



Questions?



Sandra Furuto, zano@hawaii.edu

Jodi Ito, jodi@hawaii.edu

Victoria Rivera, riveravg@hawaii.edu



Presentation slides and recording

<https://research.hawaii.edu/orc/export-controls/foreign-influence-in-university-research/webinar-protecting-uh-research/>

At the conclusion of this webinar, you will be asked to complete a short survey. Please share your feedback with us!

Office of Research Compliance
<https://research.hawaii.edu/orc/>

Information Security Team
infosec@hawaii.edu

Data Governance Office
datagov@hawaii.edu