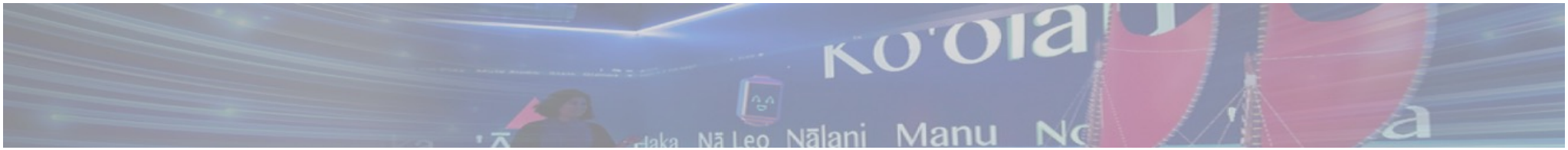
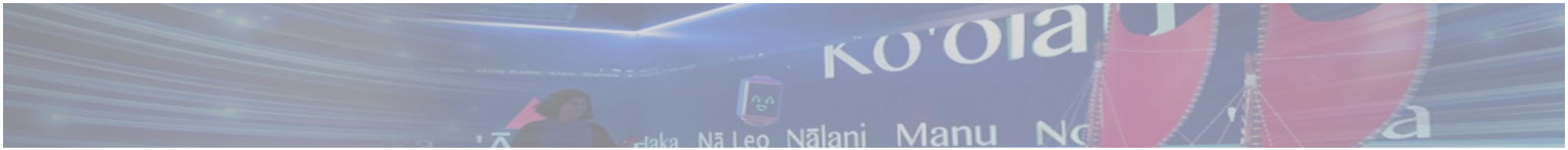


Protecting UH Research: Spring 2024 Briefing

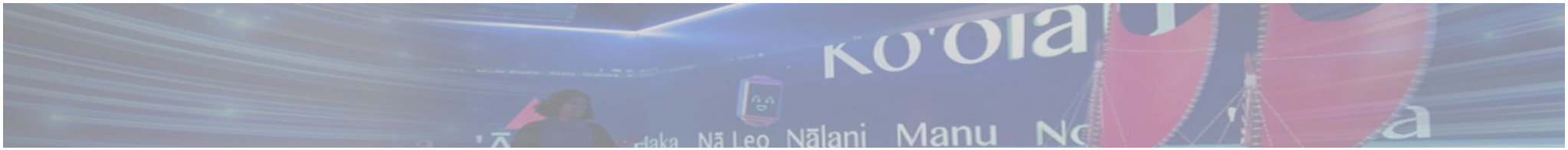
Monday, April 8, 2024
9:30-11:00am

Office of Research Compliance
Data Governance Office
Information Security Team



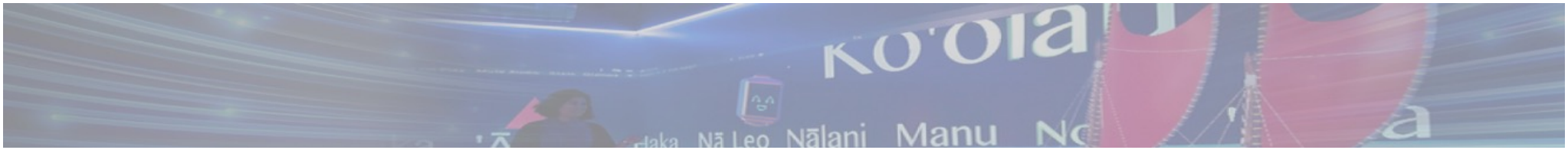
Housekeeping Items

- UH section of this session will be recorded
- Recording will be posted on the Office of Research Compliance website
- Please use the Q&A for questions



Agenda

- Office of Research Compliance: Victoria Rivera
- Cyberinfrastructure: Ron Merrill
- Regulation & Compliance: Jodi Ito



Research: Regulations & Compliance

Jodi Ito

UH CISO

jodi@hawaii.edu

The Register

Former CIO accuses Penn State of faking cybersecurity compliance

Now-NASA boffin not impressed

Thomas Claburn

Mon 18 Sep 2023 // 20:15 UTC

Last October, Pennsylvania State University (Penn State) was sued by a former chief information officer for allegedly falsifying government security compliance reports.

The lawsuit [PDF], recently unsealed, is a *qui tam* complaint (in Latin "who as well,") meaning it was filed on behalf of the US government by former CIO Matthew Decker, who claims his former employer defrauded the government under the False Claims Act.

In November 2015, Decker, presently chief data and information officer at NASA's Jet Propulsion Laboratory, was appointed CIO and director of Information Technology Services at the University's Applied Research Lab (ARL), which does work for the US Navy.

This was several months after an attack attributed to hackers in China breached Penn State's College of Engineering and College of Liberal Arts. Decker was brought in to ensure ARL complied with federal defense rules for IT security, specifically DFARS 252.204-7012 and DFARS 252.204-7019, and NIST 800-171.

https://www.theregister.com/2023/09/18/cio_penn_state_security/

https://www.justice.gov/opa/pr/false-claims-act-settlements-and-judgments-exceed-268-billion-fiscal-year-2023

CYBER-FRAUD INITIATIVE

The Department's effort to combat cybersecurity threats includes the Civil Cyber-Fraud Initiative, which was announced in October 2021. The Initiative is dedicated to using the False Claims Act to promote cybersecurity compliance by government contractors and grantees by holding them accountable when they knowingly violate applicable cybersecurity requirements.

Jelly Bean Communications Design LLC and its manager paid $293,771 to resolve allegations that they failed to secure personal information on a federally funded Florida children's health insurance website, which Jelly Bean created, hosted, and maintained. The settlement resolved allegations that, contrary to its representations and commitments, Jelly Bean did not provide secure hosting of applicants' personal information and instead knowingly failed to properly maintain, patch, and update the software systems. The site was attacked, potentially exposing the information of 500,000 applicants.

The Justice Department also settled for over $4 million with **Verizon Business Network Services LLC**, which disclosed and remediated cybersecurity failures on contracts to provide trusted internet connections to the General Services Administration. In connection with the settlement, the company took a number of significant steps entitling it to credit for cooperating with the government, including providing the government with a written self-disclosure, initiating an independent investigation and compliance review of the issues, and providing the government with multiple detailed supplemental written disclosures.

TOP

https://www.justice.gov/opa/pr/false-claims-act-settlements-and-judgments-exceed-268-billion-fiscal-year-2023

- While healthcare continues to lead most FCA activity, including DOJ's focus on fraud in pandemic relief programs as a key enforcement priority, FY 2023 saw remarkably expanded DOJ and whistleblower activity on contracts involving the Department of Defense (DoD).

https://www.jdsupra.com/legalnews/doj-releases-false-claims-act-4866378/

PRESS RELEASE

Georgia Tech and Georgia Tech Research Corporation pay $90,000 to resolve allegations of violations of the False Claims Act

Thursday, November 30, 2023

Share

For Immediate Release

U.S. Attorney's Office, Northern District of Georgia

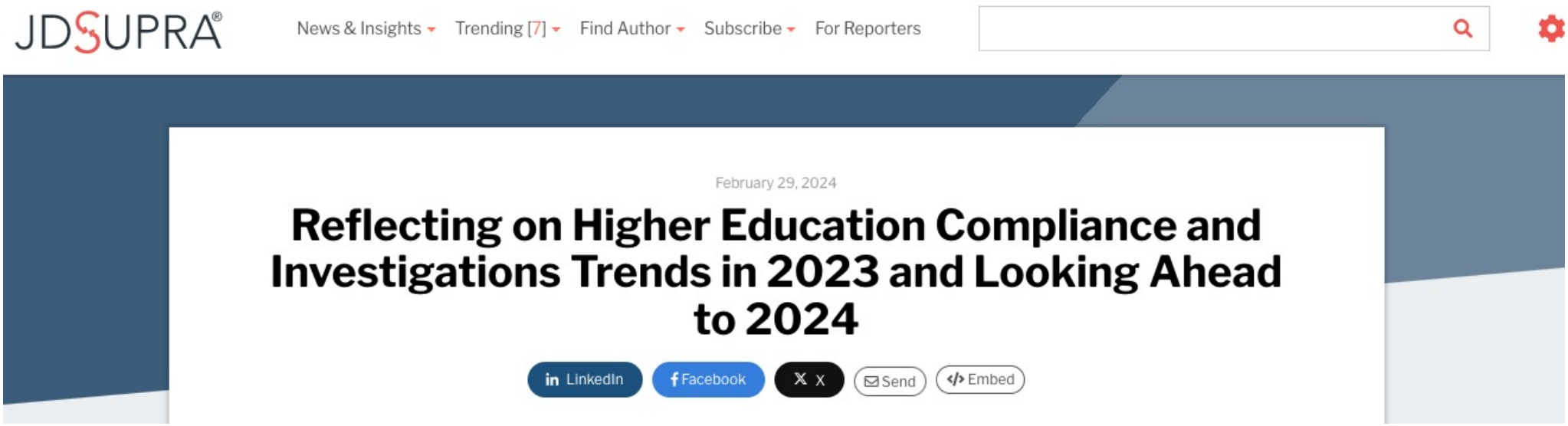
ATLANTA – The Georgia Institute of Technology ("Georgia Tech") and Georgia Tech Research Corporation ("GTRC") have agreed to pay $90,000 to resolve allegations that they violated the False Claims Act by failing to exercise proper oversight sufficient to allow them to detect the submission of false claims to the National Science Foundation ("NSF").

"Federal grants and awards come with known 'rules of the road,'" said U.S. Attorney Ryan K. Buchanan. "Organizations that receive federal funds — especially schools and universities that are pillars of our community — must take steps to ensure that their employees are following the rules. This settlement represents our office's commitment to ensuring accountability for institutions that fail to live up to these obligations."

The government's investigation concerned an NSF Industry-University Cooperative Research Center ("IUCRC") grant. The IUCRC program fosters pre-competitive research through multi-member collaborations among industry, academic, and government partners. The award at issue was made to a project entitled the "Center for Health Organization Transformation."

"The IUCRC program is a valuable tool in advancing NSF's mission to promote the progress of science by developing long-term partnerships among industry, academia, and government," said Allison Lerner, NSF's Inspector General. "The NSF Office of Inspector General is committed to vigorously pursuing oversight of taxpayer funds and protecting the integrity of this important program. We are pleased that Georgia Tech changed its practices to better safeguard IUCRC funds, and I commend the U.S. Attorney's Office for its strong support in this effort."

https://www.justice.gov/usao-ndga/pr/georgia-tech-and-georgia-tech-research-corporation-pay-90000-resolve-allegations



https://www.jdsupra.com/legalnews/reflecting-on-higher-education-5740395/

Research Misconduct Will Remain Under a Microscope

In 2023, allegations of data manipulation and plagiarism reverberated throughout academic communities across the country and, at times, made headlines that extended beyond research campuses and into broader society. We first highlight some cases regarding data manipulation, followed by a discussion of a growing trend in the use of AI to detect potential plagiarism.

Whistleblowers, activists and other interested parties continue to raise claims of data manipulation, plagiarism or other research misconduct. This past year saw a wide variety of cases alleging data manipulation. The allegations cut across a variety of research topics, ranging from an experimental drug for stroke patients to a behavioral-economics study on honesty. The parties raising the allegations also varied widely, and included not only peers within the same academic community, but also former lab members, so-called "watchdog" blog sites, and an undergraduate student journalist. Because such research is often inextricably intertwined with government grants or private funding that ties back to the potential commercialization of highly valuable products (e.g., cutting-edge drugs), bounties under the federal False Claims Act and stock market profiteering provide considerable financial incentives to surface allegations of misconduct.

Additional Terms (continued)

NIST SP 800-171 COMPLIANCE ACKNOWLEDGEMENT

As a recipient of a federally funded award from the Uniformed Services University of the Health Sciences, The Henry M. Jackson Foundation is required to flow down the Information Technology Compliance requirement, as stated in the attached prime award.

Please complete the following:

Subrecipient attest that we ☐ **are** ☐ **are not** in conformance with NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations at the appropriate information rating, as well conformance with any additional applicable qualifiers (e.g. HIPAA) prior to beginning work.

Federal Regulations

- NDAA section 889: https://www.acquisition.gov/Section-889-Policies
  - Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment
- Related to Controlled Unclassified Information (CUI):
  - DFARS 252.204-7012: Safeguarding Covered Defense Information & Cyber Incident Reporting
    - https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting
  - DFARS 252.204-7020: NIST SP 800-171 DoD Assessment Requirements
    - https://www.acquisition.gov/dfars/252.204-7020-nist-sp-800-171dod-assessment-requirements
  - DFARS 252.204-7021: Cybersecurity Maturity Model Certification Requirements*
    - https://www.acquisition.gov/dfars/252.204-7021-cybersecurity-maturity-model-certification-requirements

**Not in effect yet*

CMMC Update

- Dec. 26, 2023 Proposed Rule published
- 60 day public comment period closed end of Feb. 2024
- Spring 2024 – proposed 48 CFR expected to be published with 60 day comment period
- Final rule published after 60 day comment adjudication period
- May undergo a Congressional Review period
- Current expectation: Jan. 2025 begin phased implementation of CMMC level 1 – self assessment*

** Phased implementation starts **AFTER** 48 CFR CMMC DFARS Rule is final and effective*

Friday, April 12 • 8:00am-12:15pm

Kuykendall 201 (UHM Campus)

ONLY 4 seats left!

New: CIRCIA – Published April 4, 2024

- Proposed Rule
- The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), as amended, requires the Cybersecurity and Infrastructure Security Agency (CISA) to promulgate regulations implementing the statute's covered cyber incident and ransom payment reporting requirements for covered entities.
- 133 pages
- Applies to higher ed because of Federal Student Aid
- https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements

PRIVACY

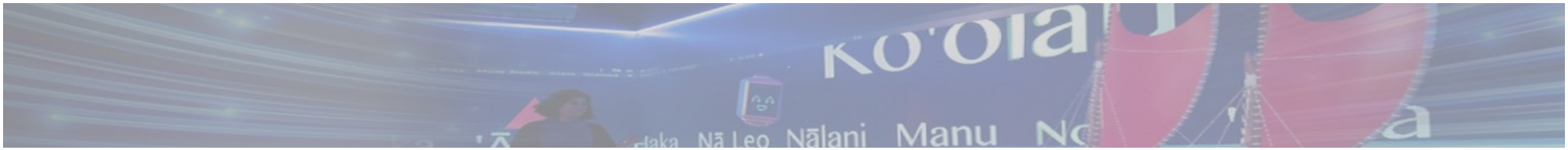
Legislators Release Draft Data Privacy Law

The measure would hand enforcement to the FTC, but would leave in place data breach rules the FCC adopted in December.

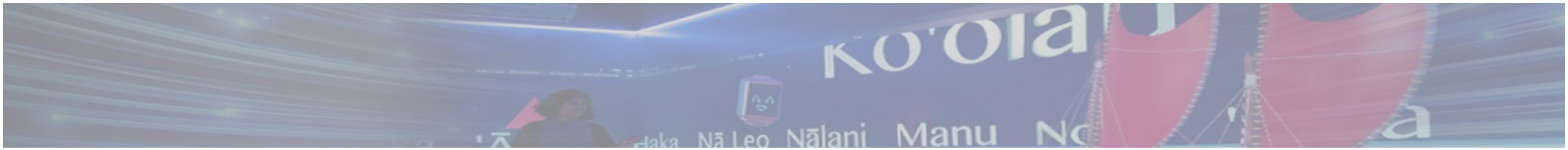
WASHINGTON, April 8, 2024 – The chairs of the House and Senate Commerce committees unveiled on Sunday a draft of federal data privacy legislation, which would give consumers broad control over how companies use their personal data and limit which kinds of data companies can hoover up.

Consumers would be able to opt out of targeted advertising and be able to access and delete the data tech companies have collected on them. Those companies would also be limited in the kinds of data they're allowed to collect depending on the services they offer.

https://broadbandbreakfast.com/legislators-release-draft-data-privacy-law/



Please complete the poll after this session ends!



Next DG & IS Webinar:
Monday, April 15, 2024
10:00-11:30am

https://hawaii.zoom.us/webinar/register/WN_SFhvyL_8RnWPZnF2Gm61Qg

Victoria Rivera: riveravg@hawaii.edu

Ron Merrill: merrill@hawaii.edu

Jodi Ito: jodi@hawaii.edu