Protecting UH Research
Fall 2022 Briefing

November 29, 2022 (recorded)

Sean Cleveland, Sr. Project Manager, ITS Cyberinfrastructure

Sandra Furuto, Data Governance Director

Valerie Iinuma, COI Specialist, Office of Research Compliance

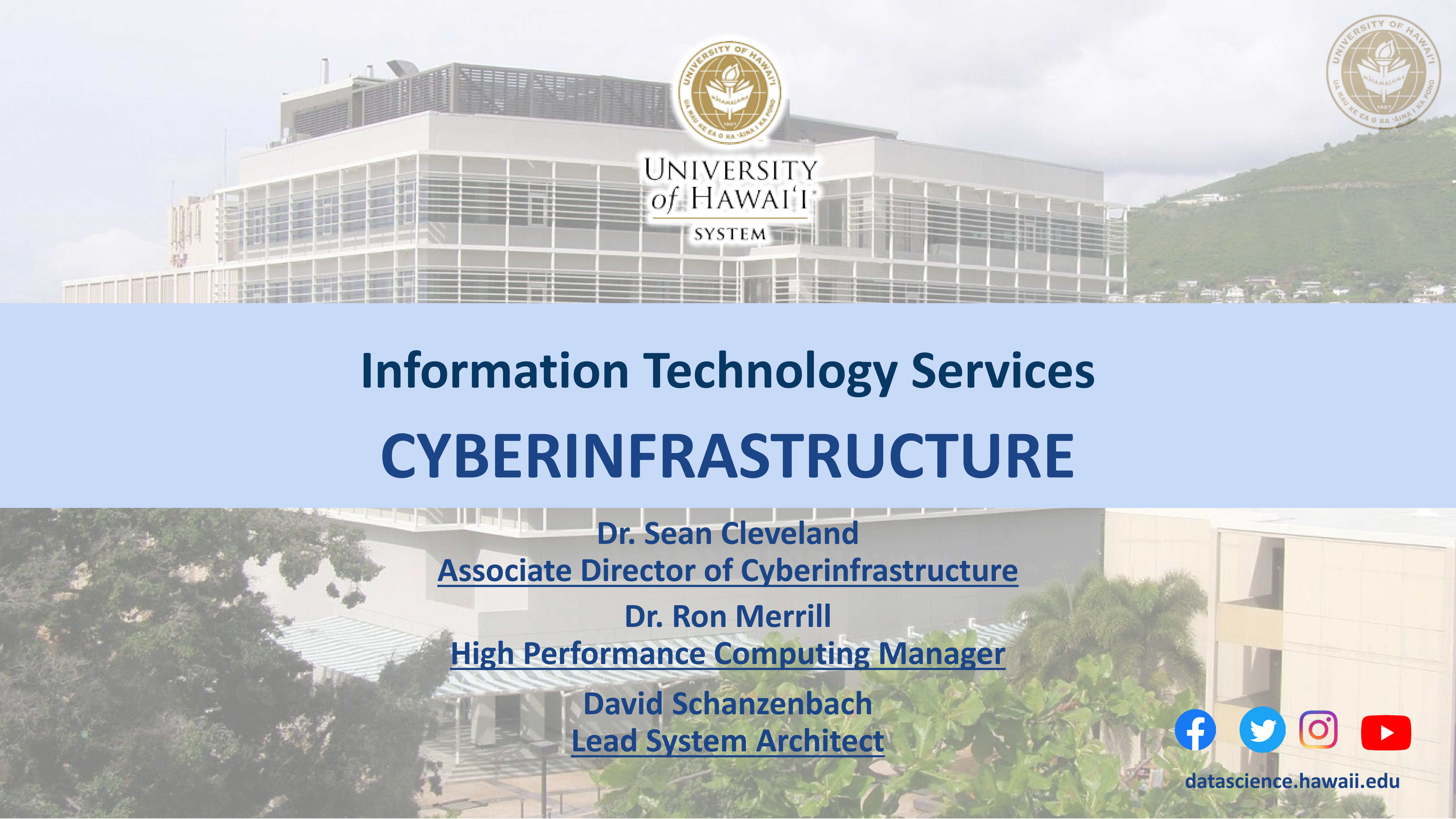
Jodi Ito, Chief Information Security Officer

Victoria Rivera, Director, Office of Research Compliance & FSO

Last updated: 11/29/2022

Today’s Agenda

- Sean Cleveland, High Performance Computing (HPC) Services
- Jodi Ito, Threats, Vulnerabilities & Compliance
- Sandra Furuto, Data Governance
- Victoria Rivera, Research Security Briefing
- Valerie Iinuma, Conflict of Interest



UNIVERSITY of HAWAIʻI SYSTEM

Information Technology Services

CYBERINFRASTRUCTURE

Dr. Sean Cleveland
Associate Director of Cyberinfrastructure

Dr. Ron Merrill
High Performance Computing Manager

David Schanzenbach
Lead System Architect

datascience.hawaii.edu

Mission

Support data intensive research and scholarship at UH with state of the art resources, services and expertise.

Our focus is:

- Advanced Computing (above the desktop)
- Data
- Science as a Service
- Collaborative research

We Serve The Entire UH System

HAWAIʻI DATA SCIENCE

ITS Cyberinfrastructure Team

Gwen A Jacobs, PhD - Director of Cyberinfrastructure

Sean Cleveland, PhD – Assoc. Director – Cyberinfrastructure Research Scientist

Advanced Computing:

Ron Merrill, PhD - HPC Manager

David Schanzenbach - Lead System Architect

Software & Data Science:

Jennifer Geis - Research Software Engineer

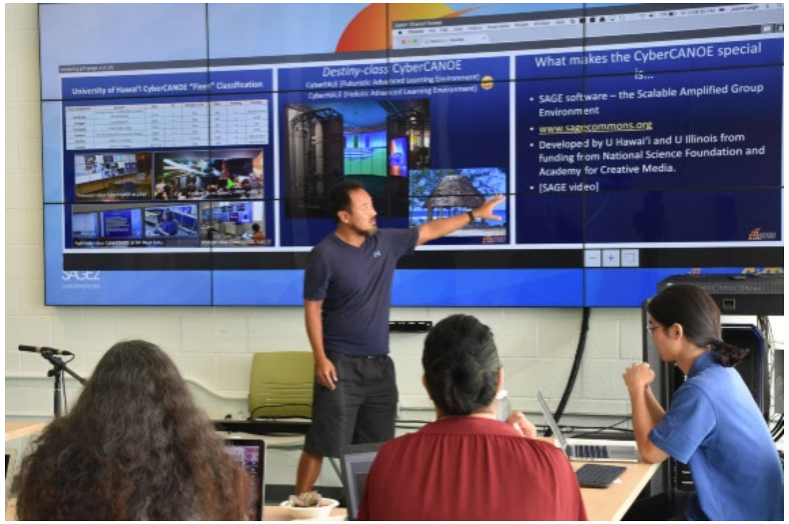
Jared McLean - Research Software Engineer

Jeff Wong – Research Software Engine

HAWAIʻI DATA SCIENCE

ADVANCED CYBERINFRASTRUCTURE

- Collaborative Workspace
- High resolution display walls for distance collaboration
- High Performance Computing & Cloud Resources with Training---**FREE**


Destiny-class CyberCANOE
What makes the CyberCANOE special is...
SAGE software – the Scalable Amplified Group Environment
www.sagecommons.org
Developed by U Hawai'i and U Illinois from funding from National Science Foundation and Academy for Creative Media.
[SAGE video]

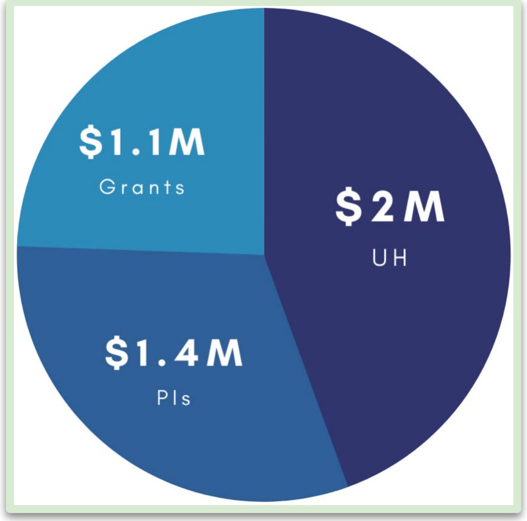
HAWAIʻI DATA SCIENCE

datascience.hawaii.edu

MANA HIGH PERFORMANCE COMPUTING

FREE!!! TO UH Faculty/Researchers/Students/Staff!!!!!

- 357 Compute Nodes
- 120 GPUs
- 8,964 cores
- 62.28 TB of memory
- 1 PB of long-term storage
- 61 TB of Flash scratch storage
- 50 TB of Standard scratch storage



$4.5M
Total Investment in HPC

MANA

$1.8 Million institutional investment 2014,

$700,000 NSF MRI 2019, $400K & $500K NSF CC* 2022

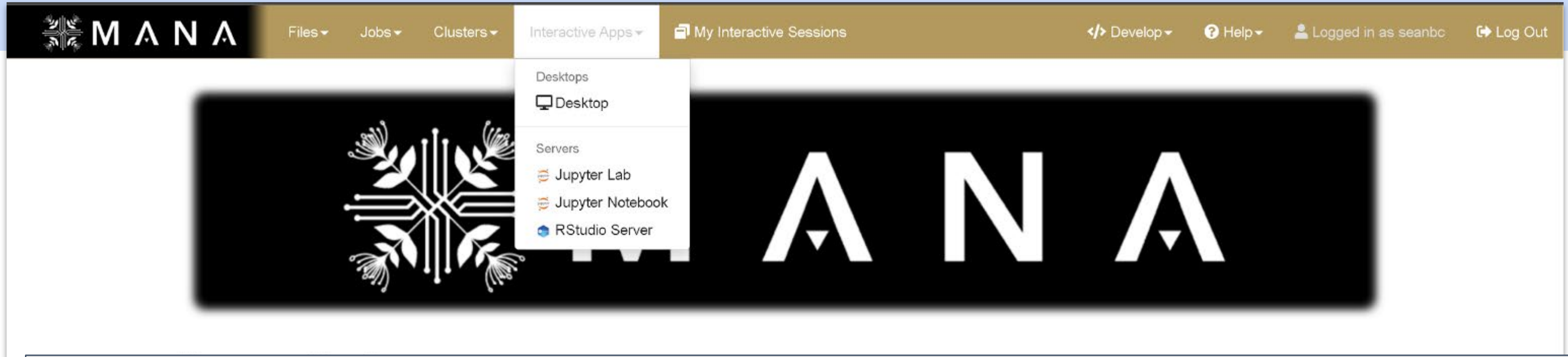
$1.4 Million - 140 Condo Nodes from Researchers

datascience.hawaii.edu

HAWAIʻI DATA SCIENCE

MANA -
Beyond Your Laptop/Workstation

HAWAI‘I DATA SCIENCE

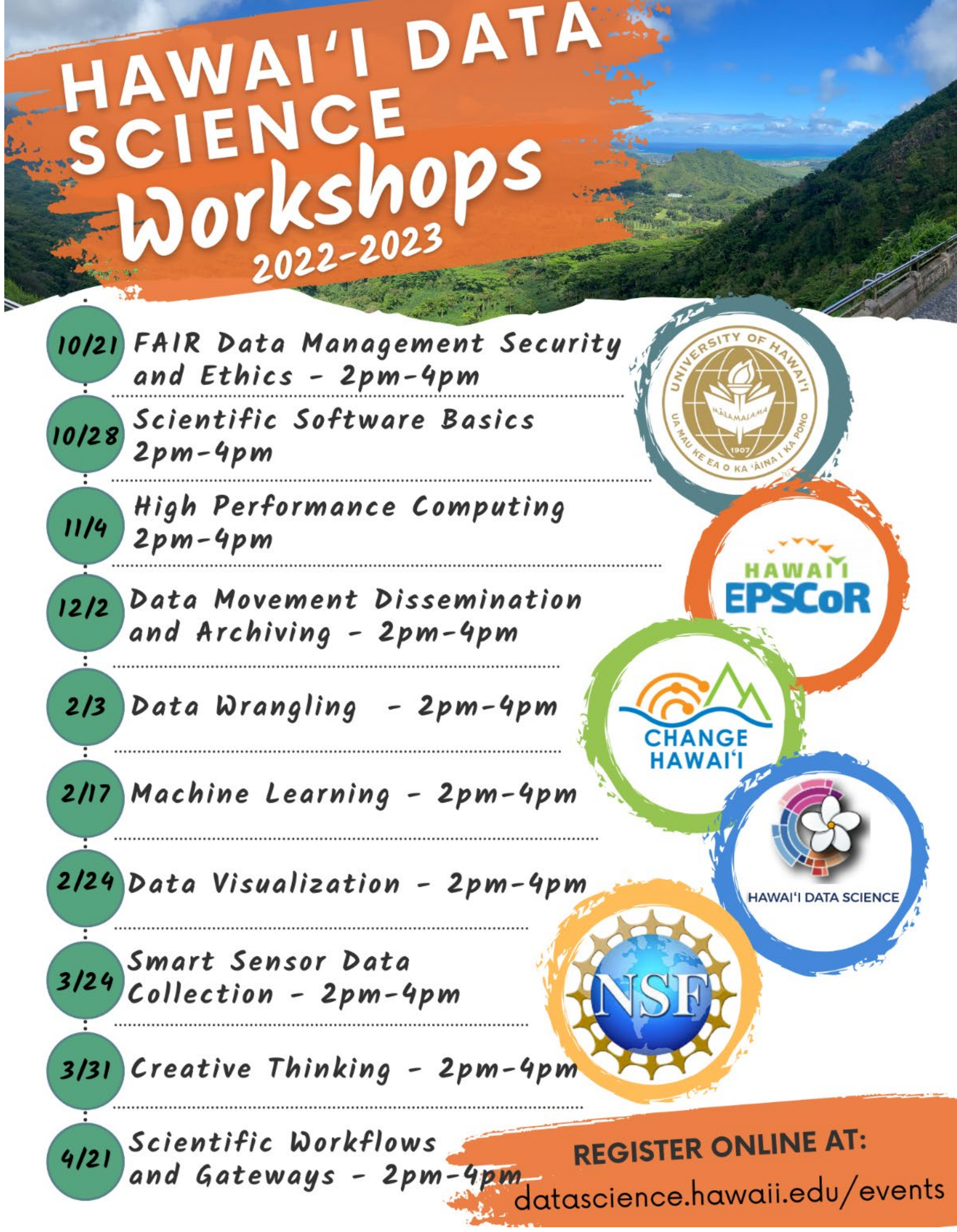


- Access via the Web Browser or Terminal
- Supports interactive computing for Jupyter/Rstudio/VNC and short compute jobs
- Batch computing for large or long running compute jobs
- High Speed data transfer- 100 Gbps Data Transfer Nodes
- Enabling access to multiple GPUs for Deep Learning and AI

TRAINING/Workshops

REGISTER HERE – all are welcome!

https://datascience.hawaii.edu/data-science-workshops/

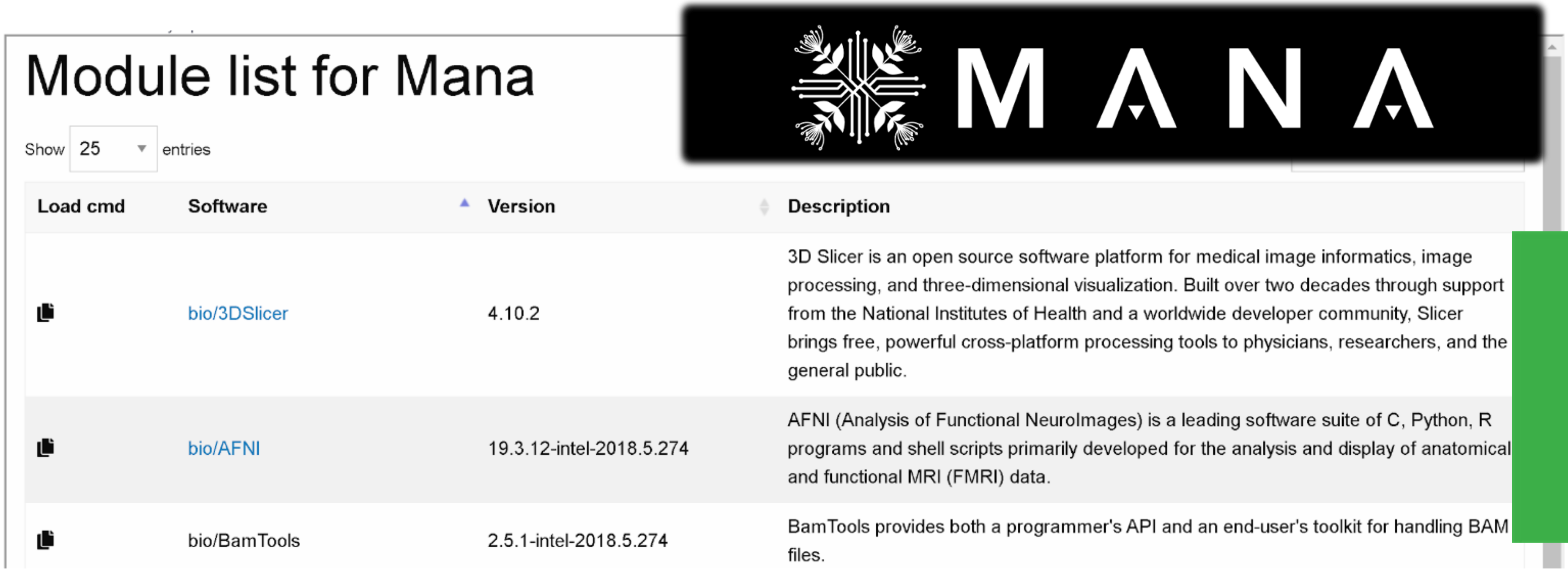


HAWAI'I DATA SCIENCE Workshops 2022-2023

10/21	FAIR Data Management Security and Ethics - 2pm-4pm
10/28	Scientific Software Basics 2pm-4pm
11/4	High Performance Computing 2pm-4pm
12/2	Data Movement Dissemination and Archiving - 2pm-4pm
2/3	Data Wrangling - 2pm-4pm
2/17	Machine Learning - 2pm-4pm
2/24	Data Visualization - 2pm-4pm
3/24	Smart Sensor Data Collection - 2pm-4pm
3/31	Creative Thinking - 2pm-4pm
4/21	Scientific Workflows and Gateways - 2pm-4pm

REGISTER ONLINE AT:
datascience.hawaii.edu/events

Help With Software/Tools on Mana



Module list for Mana

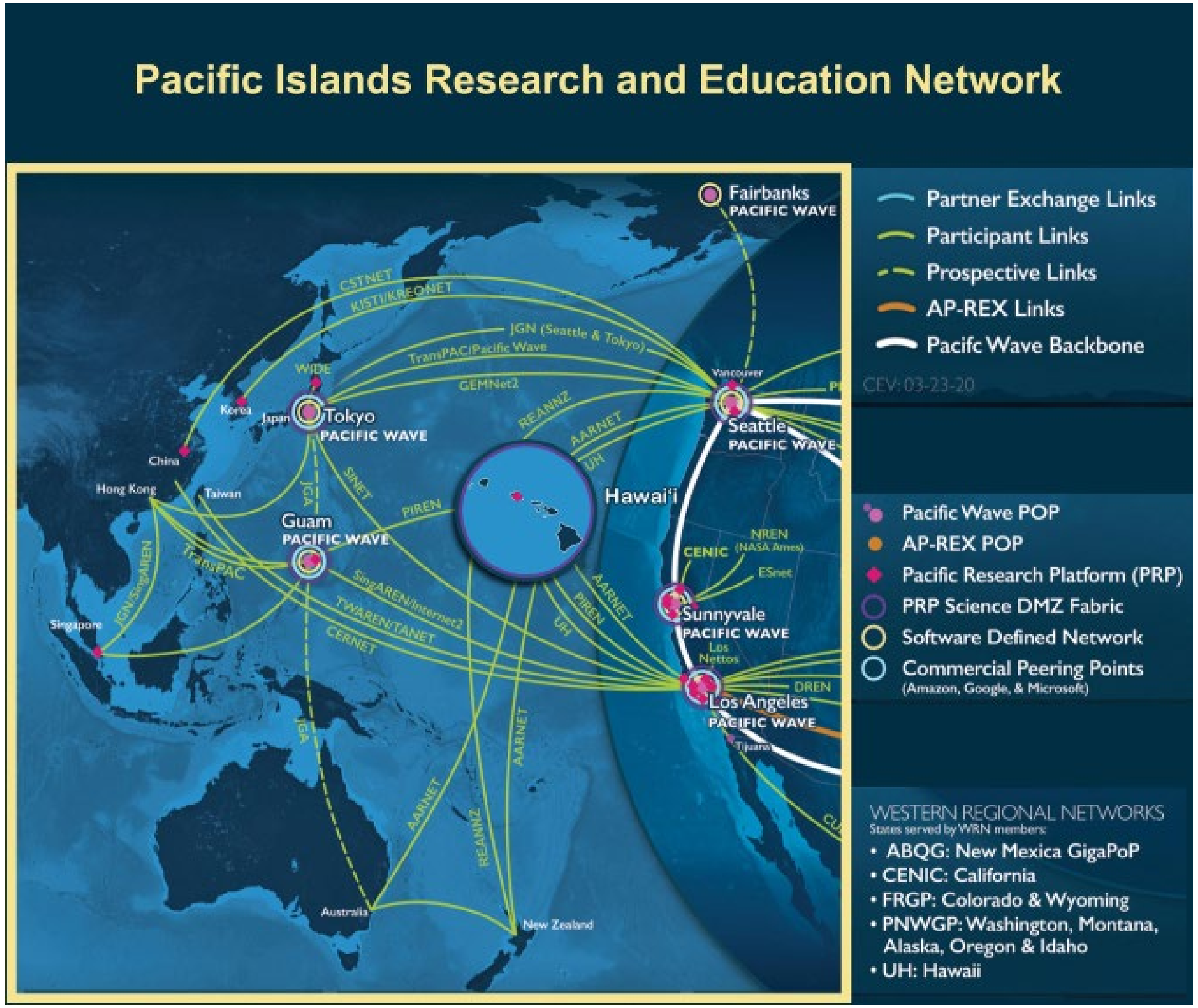
Show 25 entries

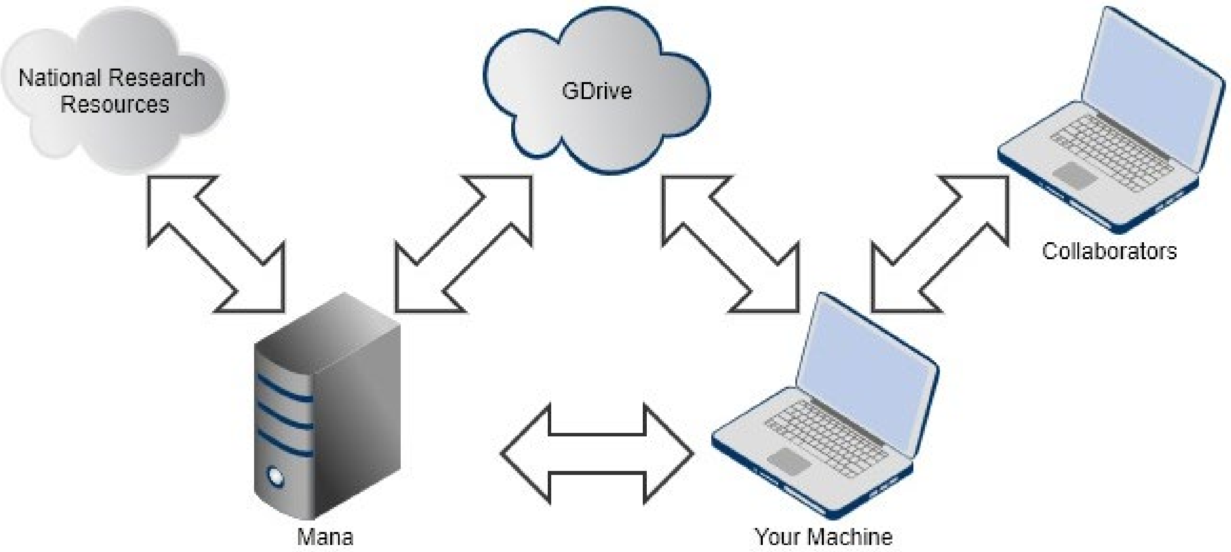
Load cmd	Software	Version	Description
	bio/3DSlicer	4.10.2	3D Slicer is an open source software platform for medical image informatics, image processing, and three-dimensional visualization. Built over two decades through support from the National Institutes of Health and a worldwide developer community, Slicer brings free, powerful cross-platform processing tools to physicians, researchers, and the general public.
	bio/AFNI	19.3.12-intel-2018.5.274	AFNI (Analysis of Functional NeuroImages) is a leading software suite of C, Python, R programs and shell scripts primarily developed for the analysis and display of anatomical and functional MRI (FMRI) data.
	bio/BamTools	2.5.1-intel-2018.5.274	BamTools provides both a programmer's API and an end-user's toolkit for handling BAM files.

- Central Software Repository - modules - installed for everyone
- Custom computing software/environments with Anaconda
- Compiling software - we have intel and open source compilers and knowledge/expertise in helping compile most software

HAWAIʻI DATA SCIENCE

Help With Research Data Movement





- Trouble Moving Data?
- Data Transfers Slow?
- Need to move a lot of Data?

HAWAI'I DATA SCIENCE

High Speed Data Transfer/Sharing

- UH System has a subscription - so free to researchers
- Very Fast and Robust data transfer - can resume large transfers
- Can transfer from laptop/workstation to Mana, or other major resources NCAR/ACCESS etc
- Can securely share files/folder on your laptop with other Globus users
- Encrypted transfers

globus

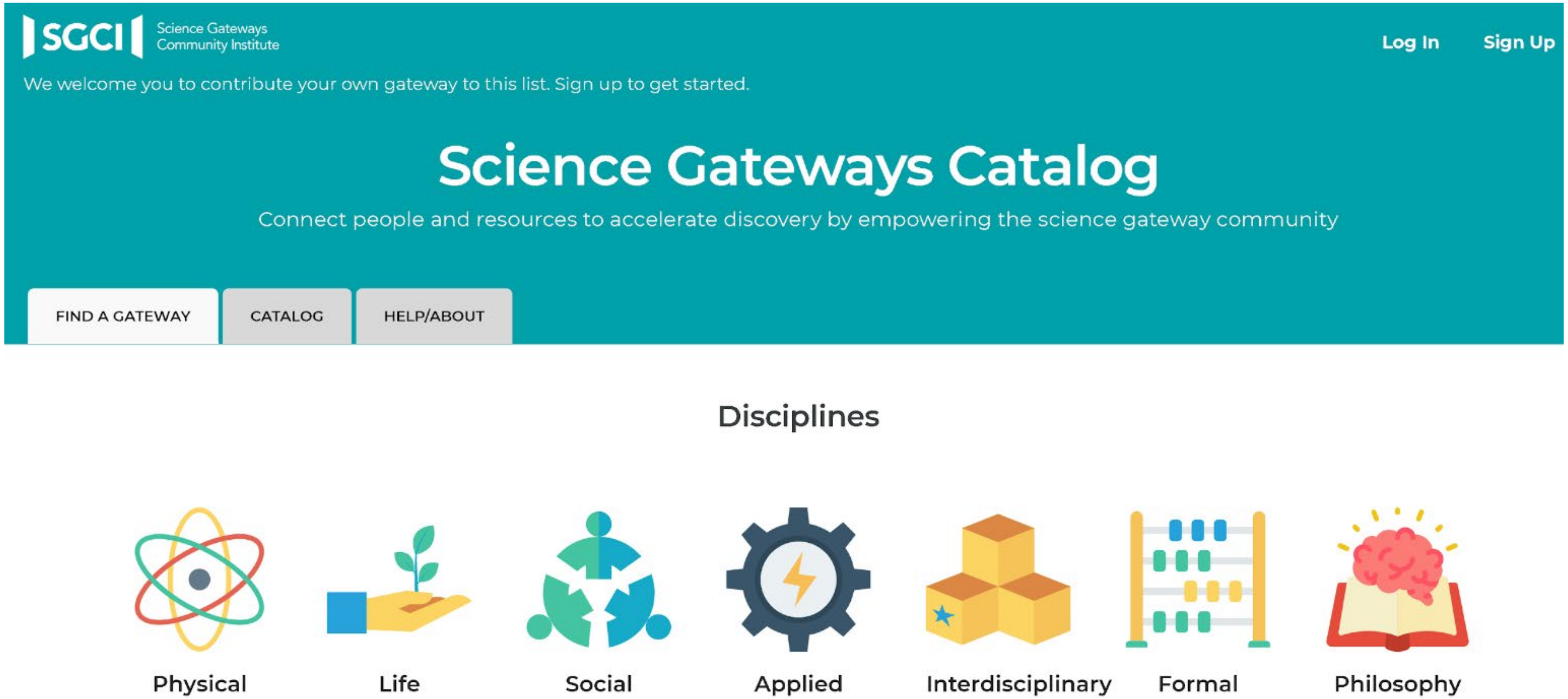
Help Accessing National Resources

- National NSF cloud computing - Jetstream2
  - UH has a regional portion of the Jetstream2 Cloud
  - https://jetstream-cloud.org/

- National HPC resources - ACCESS
  - We help with initial access and getting allocations to these resources and helping researcher get their codes running
  - https://access-ci.org/

HAWAIʻI DATA SCIENCE

Help Finding Resources & Tools



We welcome you to contribute your own gateway to this list. Sign up to get started.

Science Gateways Catalog

Connect people and resources to accelerate discovery by empowering the science gateway community

Disciplines

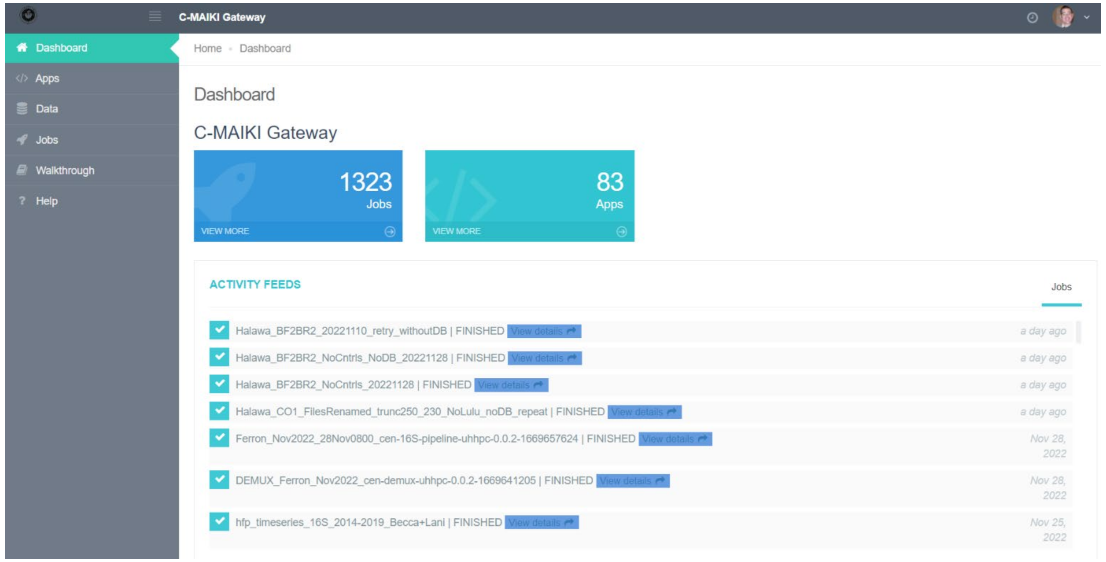
- Science Gateways - bringing together data, software and resources related to domains or communities

Help With Workflows & Pipelines

- Science-As-A-Service Platform
  - Advanced Computing end-to-end workflows
  - Functions-As-A-Service (serverless/lambda)
  - Streaming Data
  - Collaboration, Data Management and Sharing

Example - C-MAIKI Gateway for Microbiome data analysis

> 1300 workflows run
>900K parallel jobs on Mana
Simple Browser Access



Dashboard

C-MAIKI Gateway

ACTIVITY FEEDS

☑ Halawa_BF2BR2_20221110_retry_withoutDB | FINISHED — a day ago
☑ Halawa_BF2BR2_NoCntrls_NoDB_20221128 | FINISHED — a day ago
☑ Halawa_BF2BR2_NoCntrls_20221128 | FINISHED — a day ago
☑ Halawa_CO1_FilesRenamed_trunc250_230_NoLulu_noDB_repeat | FINISHED — a day ago
☑ Ferron_Nov2022_28Nov0800_cen-16S-pipeline-uhhpc-0.0.2-1669657624 | FINISHED — Nov 28, 2022
☑ DEMUX_Ferron_Nov2022_cen-demux-uhhpc-0.0.2-1669641205 | FINISHED — Nov 28, 2022
☑ hfp_timeseries_16S_2014-2019_Becca+Lani | FINISHED — Nov 25, 2022

HAWAIʻI DATA SCIENCE

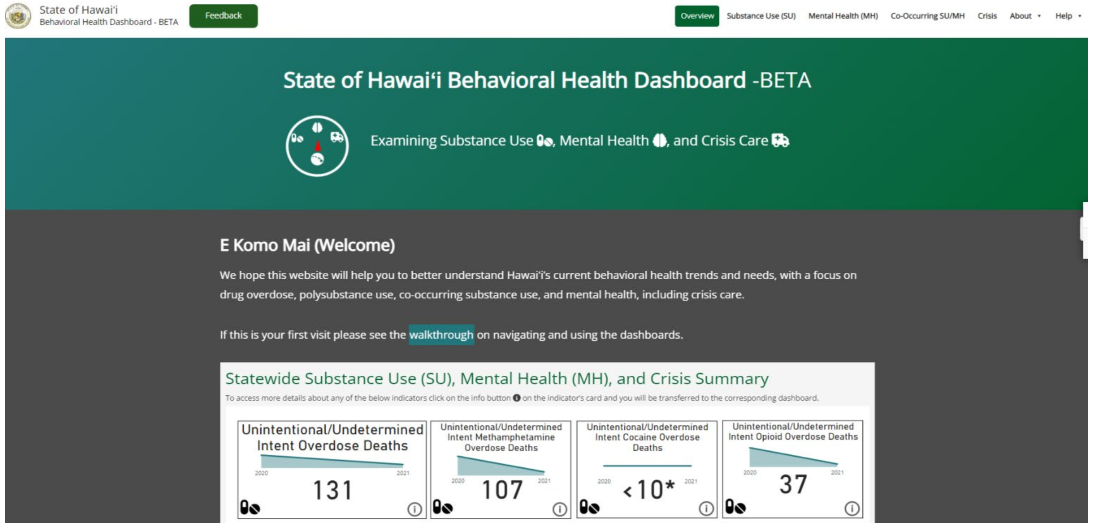
Help With Software & Data Science

- Software Engineering and Data Science Services To Accelerate Your Research
  - Access Professional Research Software Engineers
  - Access Data Fellow

Current Projects

State of Hawaii Behavioral Health Dashboard

https://bh808.hawaii.gov/



State of Hawaiʻi Behavioral Health Dashboard -BETA

Examining Substance Use, Mental Health, and Crisis Care

E Komo Mai (Welcome)

We hope this website will help you to better understand Hawai'i's current behavioral health trends and needs, with a focus on drug overdose, polysubstance use, co-occurring substance use, and mental health, including crisis care.

If this is your first visit please see the walkthrough on navigating and using the dashboards.

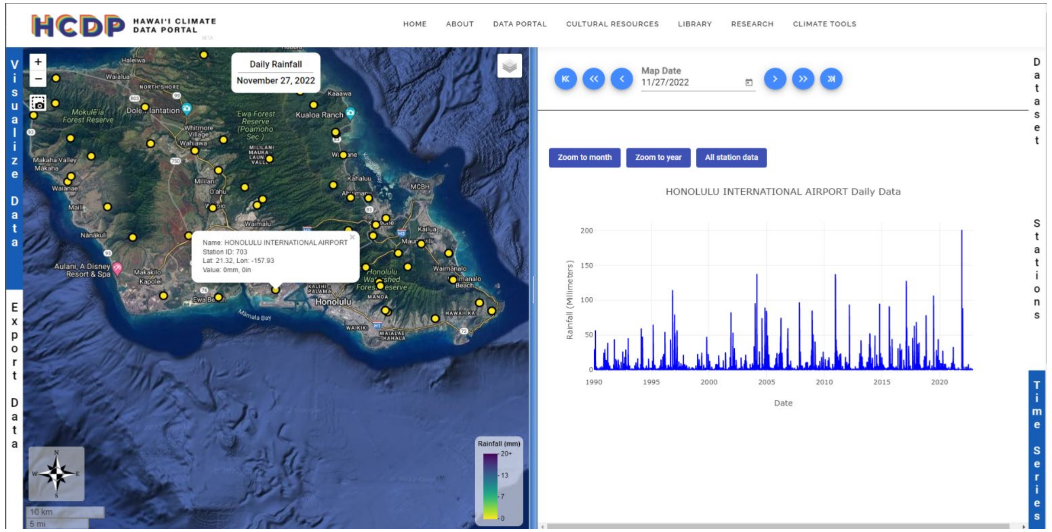
Statewide Substance Use (SU), Mental Health (MH), and Crisis Summary

To access more details about any of the below indicators click on the info button ⓘ on the indicator's card and you will be transferred to the corresponding dashboard.

Unintentional/Undetermined Intent Overdose Deaths	Unintentional/Undetermined Intent Methamphetamine Overdose Deaths	Unintentional/Undetermined Intent Cocaine Overdose Deaths	Unintentional/Undetermined Intent Opioid Overdose Deaths
131	107	<10*	37

Hawaii Climate Data Portal

https://hawaii.edu/hcdp



Daily Rainfall
November 27, 2022

Name: HONOLULU INTERNATIONAL AIRPORT
Station ID: 703
Lat: 21.32, Lon: -157.93
Value: 0mm, 0in

Map Date 11/27/2022

HONOLULU INTERNATIONAL AIRPORT Daily Data

HAWAIʻI DATA SCIENCE

Help With Reproducibility

- Looking at your results months/years later for publication or needing to re-run analysis or re-use methods is challenging - set yourself up for success
- Scientific container environments - combining dependencies, data, code and results aides in reproducibility and re-use - especially when combined with scientific computational notebook technologies (jupyter,rstudio)

Help With Data Management

- Funding Agencies and institutions spend $$$$ on research - the outputs (data) are valuable products
- Making data FAIR:
  - Findable
  - Accessible
  - Interoperable
  - Re-usable
- We can help with grant Data Management Plans

CURRENT FUNDING & COLLABORATIONS

Program	Project	Funding
NSF EPSCoR - RII T1	ChangeHI	$20M
NSF OAC	TAPIS	$5M
NSF OAC	PIREN	$3M
NSF OAC	Jetstream2	$12M
NSF OAC	CI-TRACS - Cyberinfrastructure Training to Advance Environmental Science	$3M
NSF CISE	SAGE3	$2.5M
NSF CC*	Koa	$400K
NSF CC*	KoaStore	$500K

Contact Us

itsci@hawaii.edu

https://datascience.hawaii.edu

Threats, Vulnerabilities & Compliance

Recap of Current Threats in the Cybersecurity Awareness Month Webinar Recording:
https://drive.google.com/file/d/1T9l1tHAJiyE80SUpa7KsH24n_RY-z4-h/view

Jodi Ito
UH Chief Information Security Officer
jodi@hawaii.edu

DBIR

Data Breach Investigations Report

Summary of findings

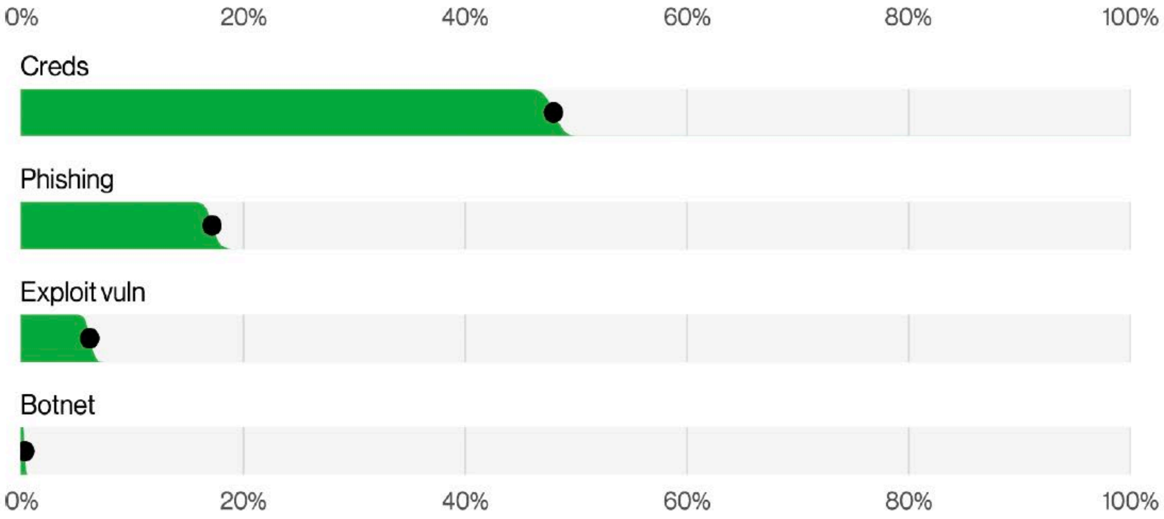


Figure 5. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

There are four key paths leading to your estate: Credentials, Phishing, Exploiting vulnerabilities and Botnets. These four pervade all areas of the DBIR, and no organization is safe without a plan to handle them all.

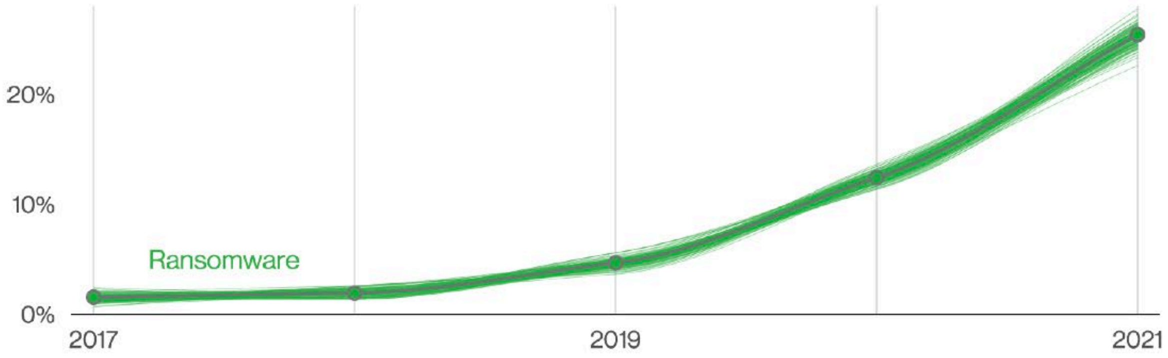
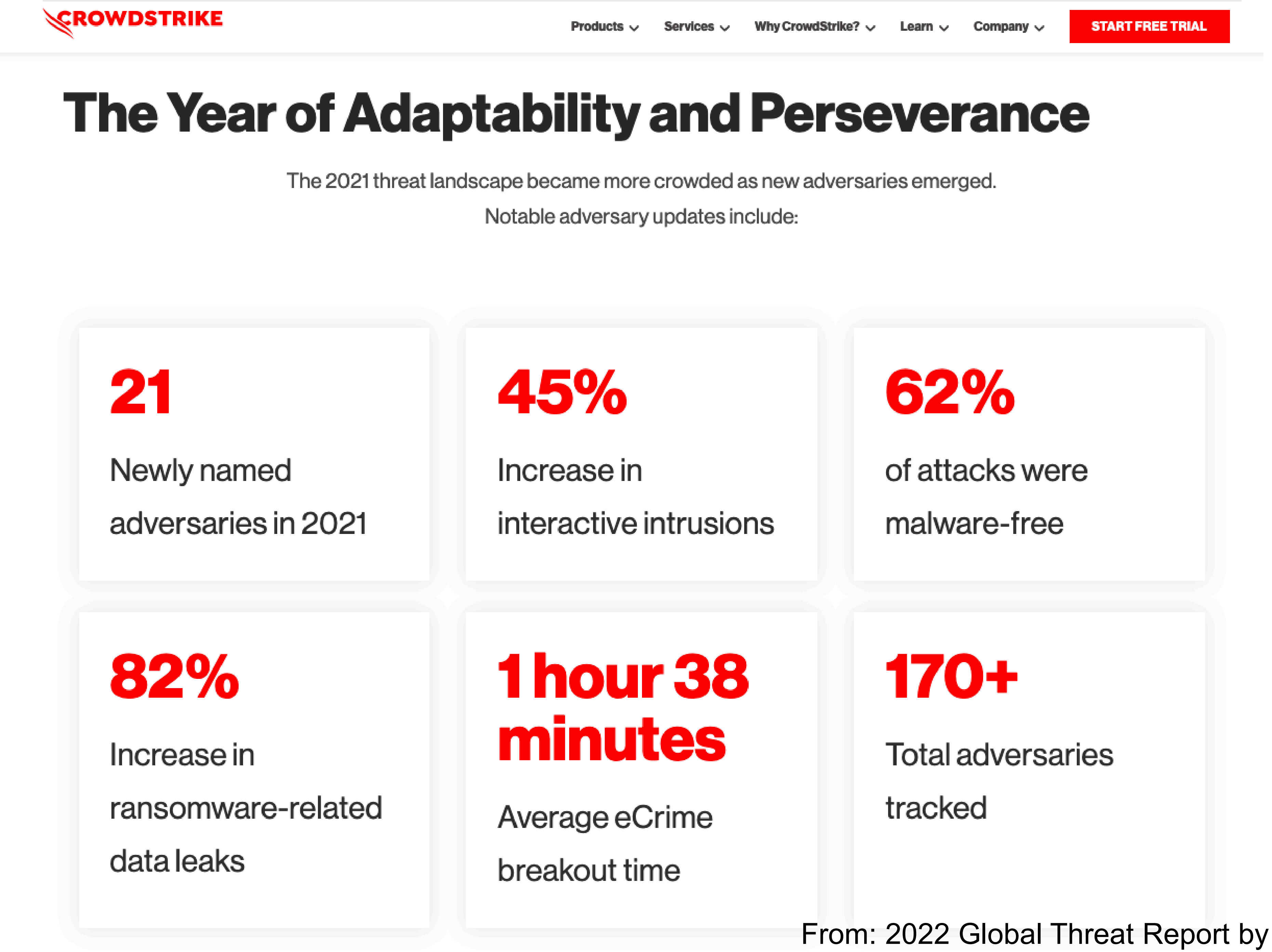


Figure 6. Ransomware over time in breaches

This year, Ransomware has continued its upward trend with an almost 13% increase–a rise as big as the last five years combined (for a total of 25% this year). It's important to remember, Ransomware by itself is really just a model of monetizing an organization's access. Blocking the four key paths mentioned above helps to block the most common routes Ransomware uses to invade your network.



The Year of Adaptability and Perseverance

The 2021 threat landscape became more crowded as new adversaries emerged.

Notable adversary updates include:

21

Newly named adversaries in 2021

45%

Increase in interactive intrusions

62%

of attacks were malware-free

82%

Increase in ransomware-related data leaks

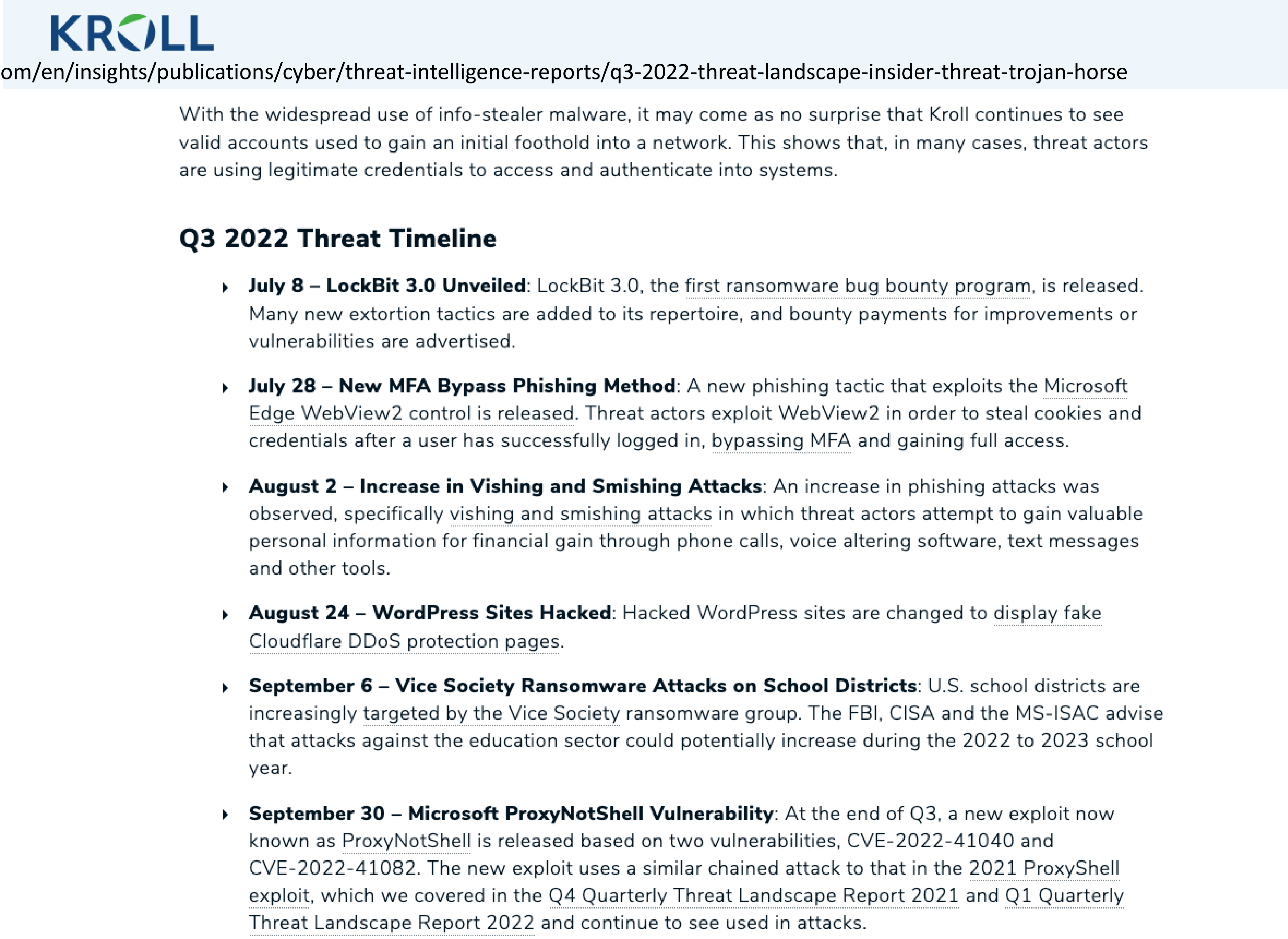
1 hour 38 minutes

Average eCrime breakout time

170+

Total adversaries tracked

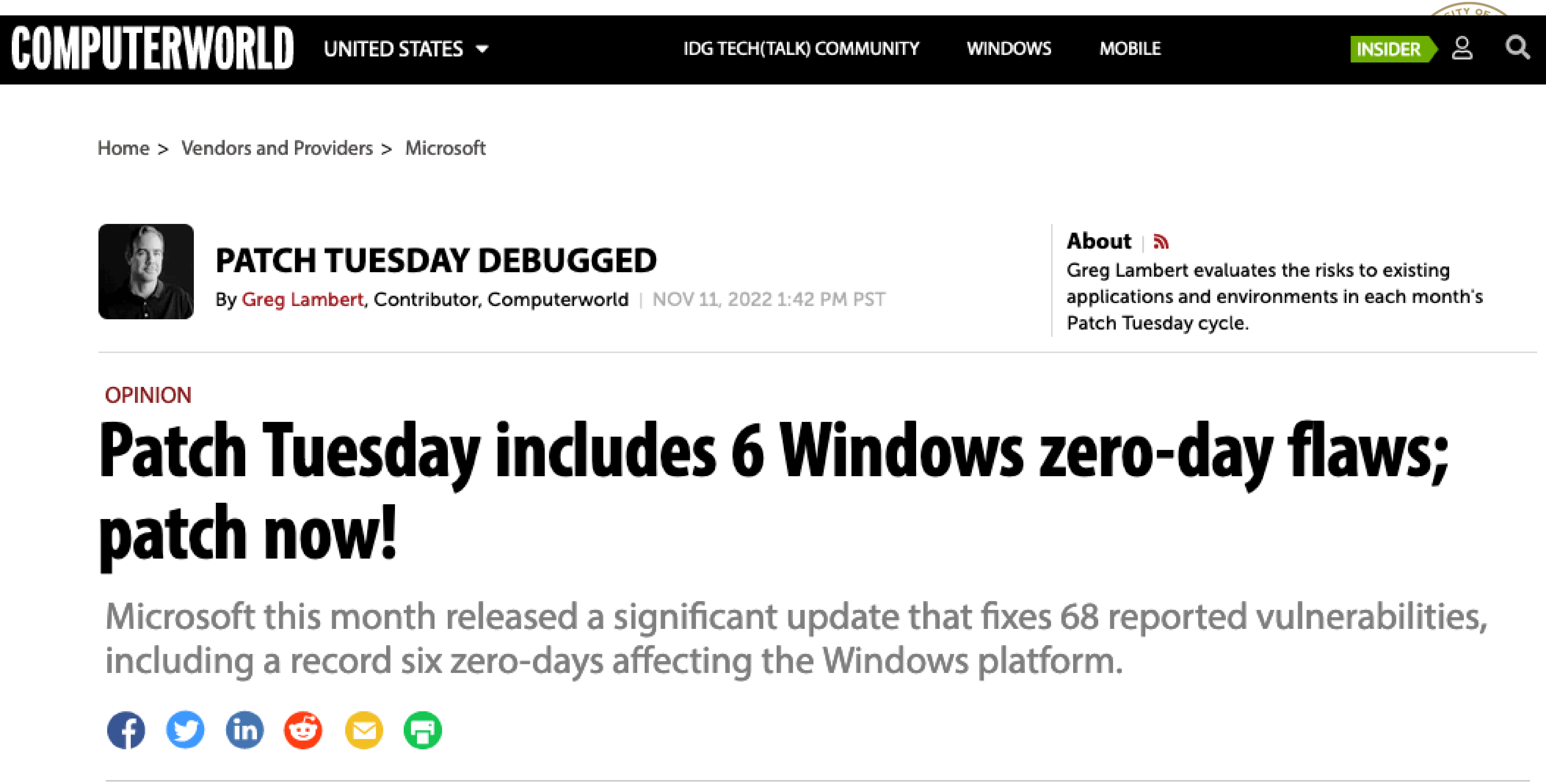
From: 2022 Global Threat Report by CrowdStrike https://www.kroll.com/en/insights/publications/cyber/threat-intelligence-reports/q3-2022-threat-landscape-insider-threat-trojan-horse


KROLL

With the widespread use of info-stealer malware, it may come as no surprise that Kroll continues to see valid accounts used to gain an initial foothold into a network. This shows that, in many cases, threat actors are using legitimate credentials to access and authenticate into systems.

Q3 2022 Threat Timeline

- **July 8 – LockBit 3.0 Unveiled**: LockBit 3.0, the first ransomware bug bounty program, is released. Many new extortion tactics are added to its repertoire, and bounty payments for improvements or vulnerabilities are advertised.
- **July 28 – New MFA Bypass Phishing Method**: A new phishing tactic that exploits the Microsoft Edge WebView2 control is released. Threat actors exploit WebView2 in order to steal cookies and credentials after a user has successfully logged in, bypassing MFA and gaining full access.
- **August 2 – Increase in Vishing and Smishing Attacks**: An increase in phishing attacks was observed, specifically vishing and smishing attacks in which threat actors attempt to gain valuable personal information for financial gain through phone calls, voice altering software, text messages and other tools.
- **August 24 – WordPress Sites Hacked**: Hacked WordPress sites are changed to display fake Cloudflare DDoS protection pages.
- **September 6 – Vice Society Ransomware Attacks on School Districts**: U.S. school districts are increasingly targeted by the Vice Society ransomware group. The FBI, CISA and the MS-ISAC advise that attacks against the education sector could potentially increase during the 2022 to 2023 school year.
- **September 30 – Microsoft ProxyNotShell Vulnerability**: At the end of Q3, a new exploit now known as ProxyNotShell is released based on two vulnerabilities, CVE-2022-41040 and CVE-2022-41082. The new exploit uses a similar chained attack to that in the 2021 ProxyShell exploit, which we covered in the Q4 Quarterly Threat Landscape Report 2021 and Q1 Quarterly Threat Landscape Report 2022 and continue to see used in attacks.



PATCH TUESDAY DEBUGGED

By Greg Lambert, Contributor, Computerworld | NOV 11, 2022 1:42 PM PST

About

Greg Lambert evaluates the risks to existing applications and environments in each month's Patch Tuesday cycle.

OPINION

Patch Tuesday includes 6 Windows zero-day flaws; patch now!

Microsoft this month released a significant update that fixes 68 reported vulnerabilities, including a record six zero-days affecting the Windows platform.

https://www.computerworld.com/article/3679631/patch-tuesday-includes-6-windows-zero-day-flaws-patch-now.html

JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

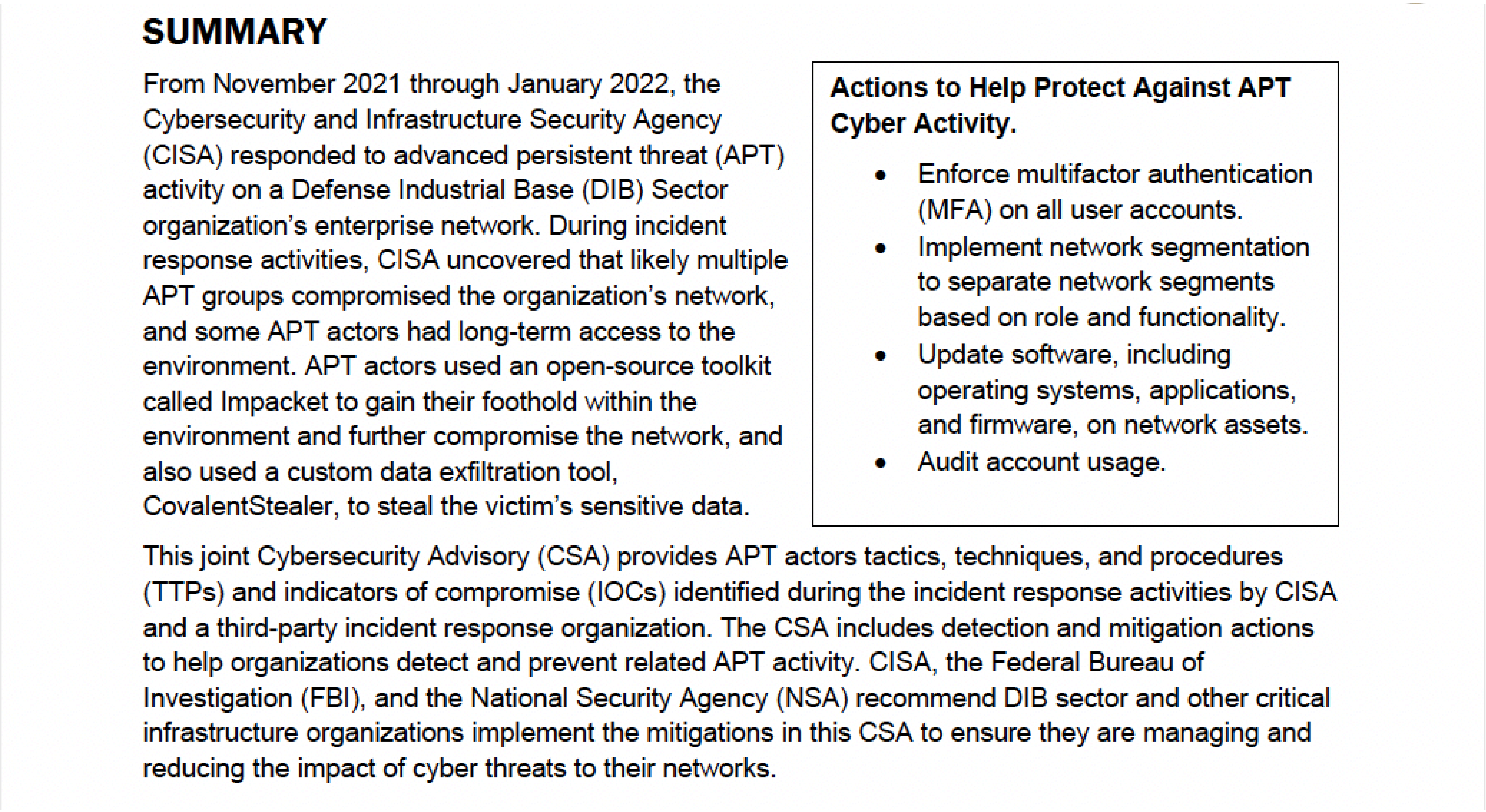
TLP:WHITE

Product ID: AA22-277A

October 4, 2022

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

https://www.cisa.gov/uscert/sites/default/files/publications/aa22-277a-impacket-and-exfiltration-tool-used-to-steal-sensitive-information-from-defense-industrial-base-organization.pdf



SUMMARY

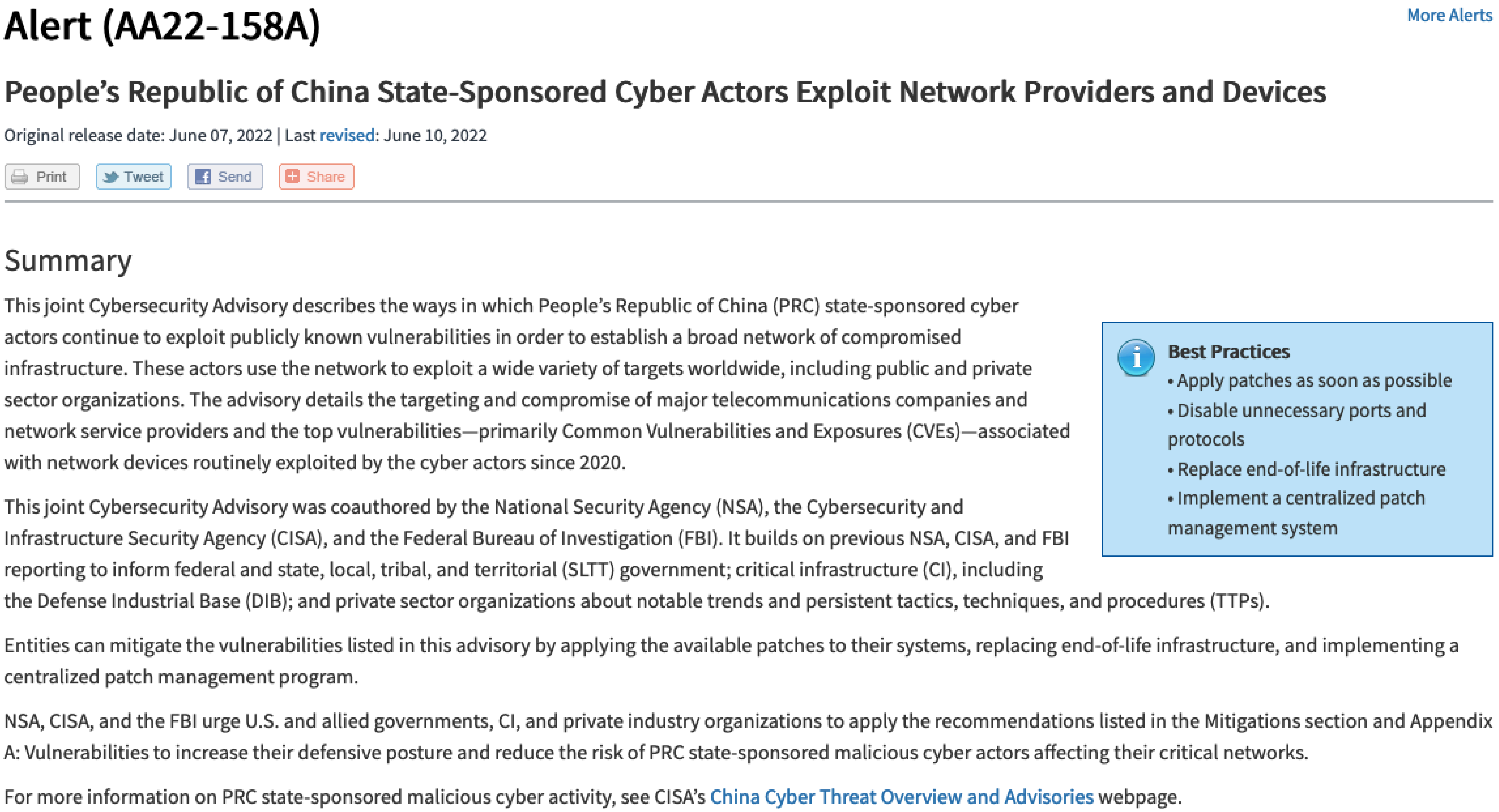
From November 2021 through January 2022, the Cybersecurity and Infrastructure Security Agency (CISA) responded to advanced persistent threat (APT) activity on a Defense Industrial Base (DIB) Sector organization's enterprise network. During incident response activities, CISA uncovered that likely multiple 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.

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.

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.

https://www.cisa.gov/uscert/ncas/alerts/aa22-158a



Alert (AA22-158A)

People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices

Original release date: June 07, 2022 | Last revised: June 10, 2022

Summary

This joint Cybersecurity Advisory describes the ways in which People's Republic of China (PRC) state-sponsored cyber actors continue to exploit publicly known vulnerabilities in order to establish a broad network of compromised infrastructure. These actors use the network to exploit a wide variety of targets worldwide, including public and private sector organizations. The advisory details the targeting and compromise of major telecommunications companies and network service providers and the top vulnerabilities—primarily Common Vulnerabilities and Exposures (CVEs)—associated with network devices routinely exploited by the cyber actors since 2020.

This joint Cybersecurity Advisory was coauthored by the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI). It builds on previous NSA, CISA, and FBI reporting to inform federal and state, local, tribal, and territorial (SLTT) government; critical infrastructure (CI), including the Defense Industrial Base (DIB); and private sector organizations about notable trends and persistent tactics, techniques, and procedures (TTPs).

Best Practices
- Apply patches as soon as possible
- Disable unnecessary ports and protocols
- Replace end-of-life infrastructure
- Implement a centralized patch management system

Entities can mitigate the vulnerabilities listed in this advisory by applying the available patches to their systems, replacing end-of-life infrastructure, and implementing a centralized patch management program.

NSA, CISA, and the FBI urge U.S. and allied governments, CI, and private industry organizations to apply the recommendations listed in the Mitigations section and Appendix A: Vulnerabilities to increase their defensive posture and reduce the risk of PRC state-sponsored malicious cyber actors affecting their critical networks.

For more information on PRC state-sponsored malicious cyber activity, see CISA's China Cyber Threat Overview and Advisories webpage.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

https://www.cisa.gov/uscert/ncas/alerts/aa22-279a

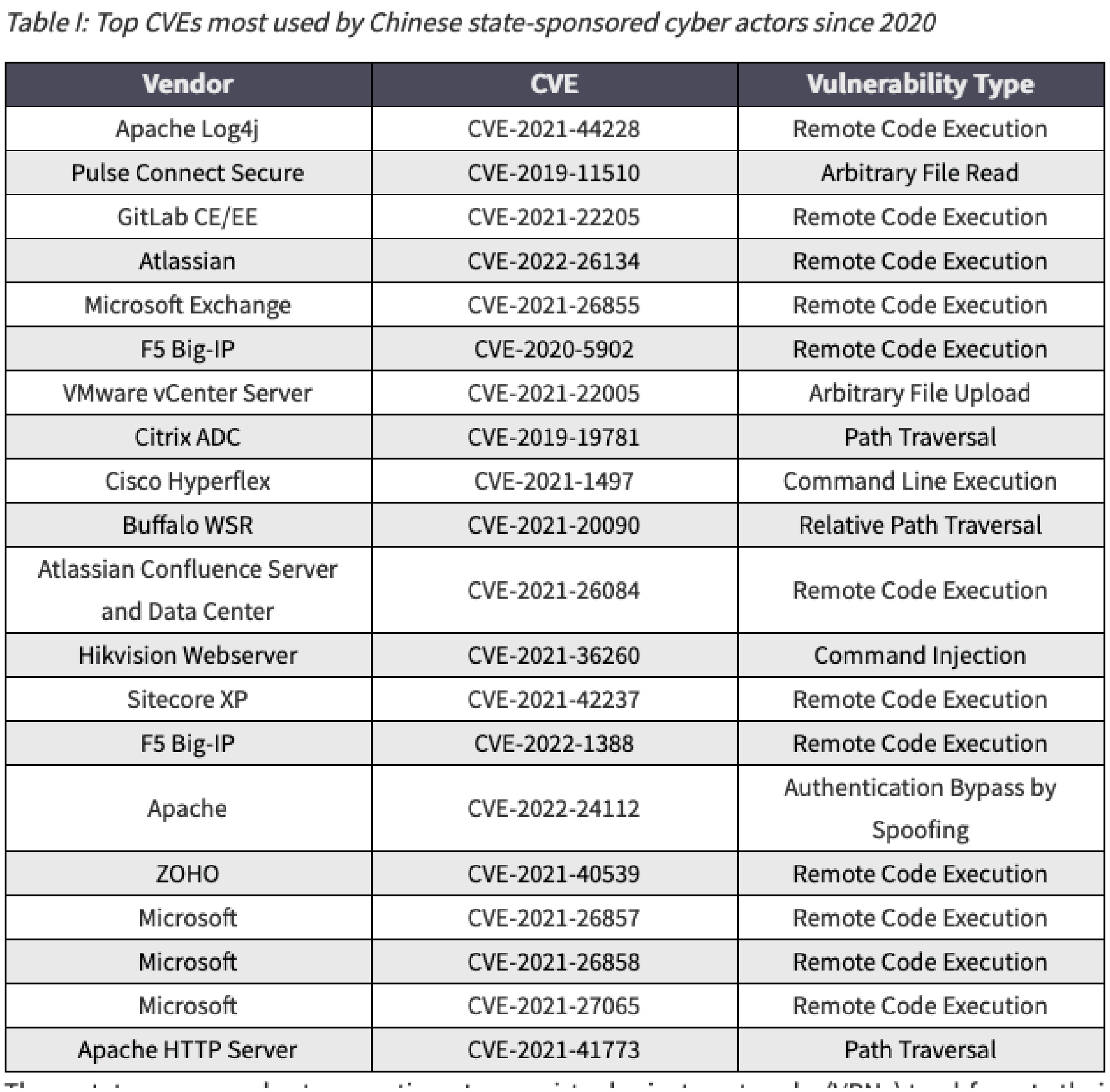


Table I: Top CVEs most used by Chinese state-sponsored cyber actors since 2020

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.

Recent UH Incidents

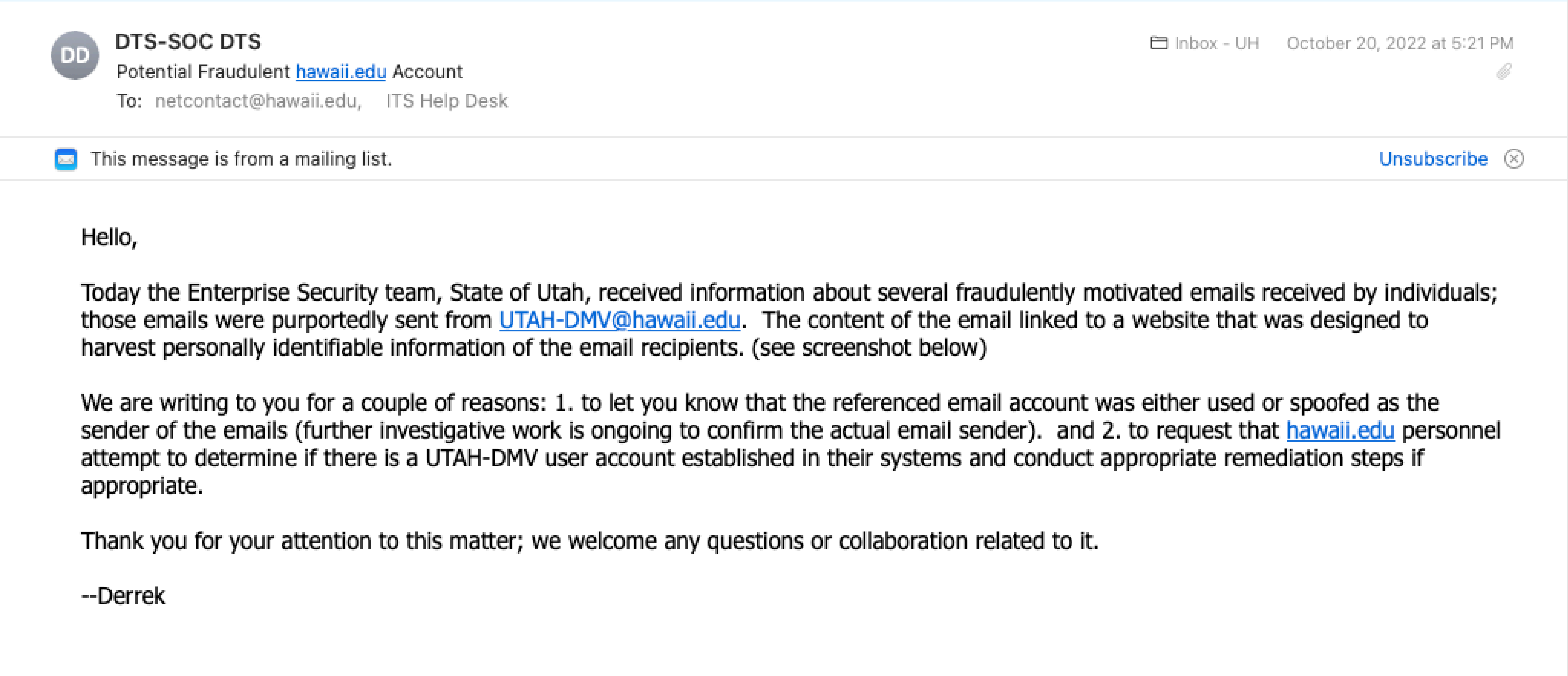
IoT, MFD, Unsecure Devices on UH Network

- 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.

Lab equipment compromised

- Information Security was recently notified of a potential fraudulent hawaii.edu account used to spoof Utah DMV services
- Upon further investigation it was discovered that a device that was not intended for public access was compromised and sending the fraudulent emails
- The device was running an open source operating system and default credentials were posted in a GitHub repository which was previously used to compromise. Although the administrator changed the main password, it was discovered that there was an additional service account that did not require a password and could obtain root access due to improper security controls

Email Reporting the Compromise



DTS-SOC DTS

Potential Fraudulent hawaii.edu Account

To: netcontact@hawaii.edu, ITS Help Desk

October 20, 2022 at 5:21 PM

This message is from a mailing list.

Hello,

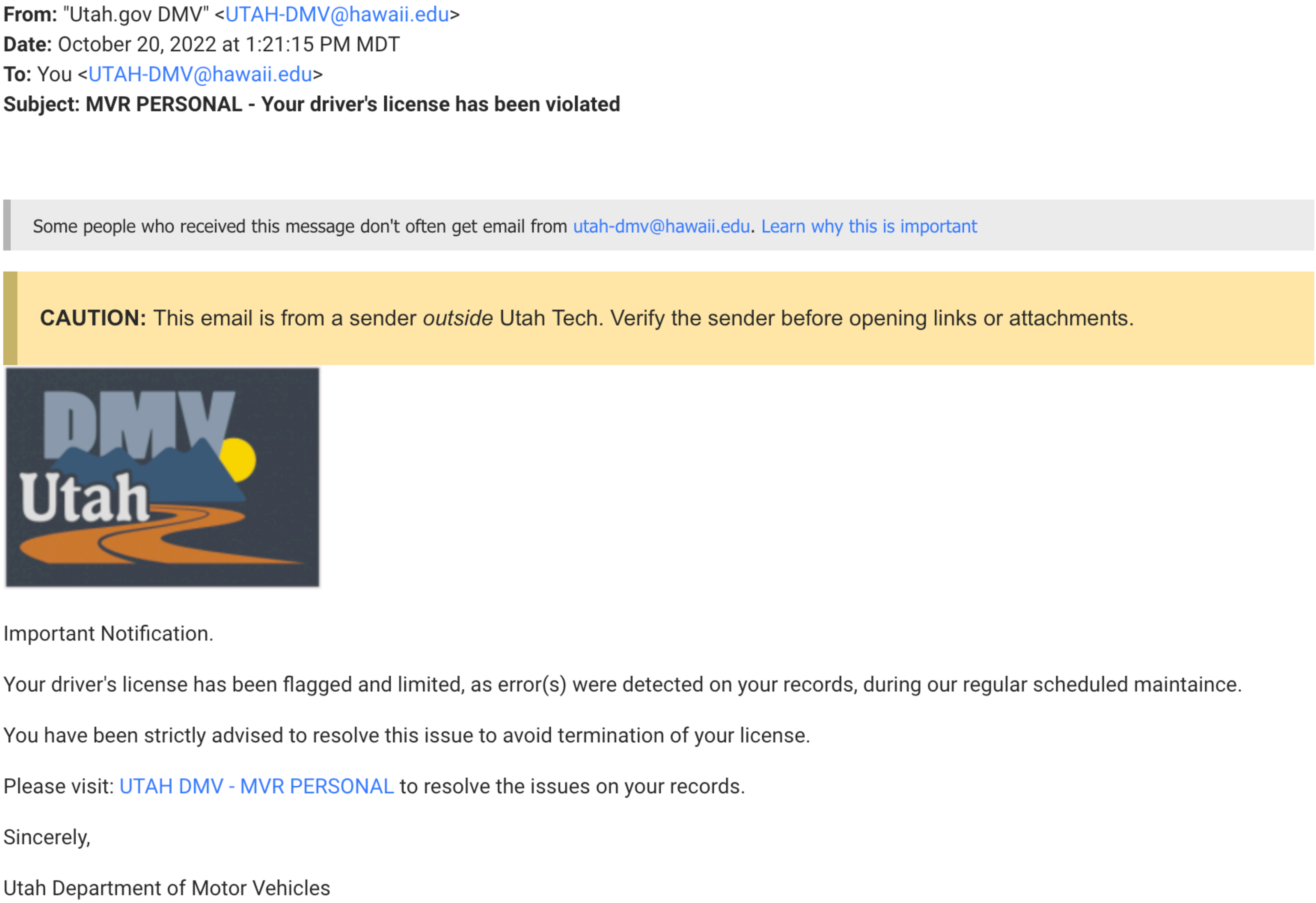
Today the Enterprise Security team, State of Utah, received information about several fraudulently motivated emails received by individuals; those emails were purportedly sent from UTAH-DMV@hawaii.edu. The content of the email linked to a website that was designed to harvest personally identifiable information of the email recipients. (see screenshot below)

We are writing to you for a couple of reasons: 1. to let you know that the referenced email account was either used or spoofed as the sender of the emails (further investigative work is ongoing to confirm the actual email sender). and 2. to request that hawaii.edu personnel attempt to determine if there is a UTAH-DMV user account established in their systems and conduct appropriate remediation steps if appropriate.

Thank you for your attention to this matter; we welcome any questions or collaboration related to it.

--Derrek

Screenshot of the phishing email



From: "Utah.gov DMV" <UTAH-DMV@hawaii.edu>
Date: October 20, 2022 at 1:21:15 PM MDT
To: You <UTAH-DMV@hawaii.edu>
Subject: MVR PERSONAL - Your driver's license has been violated

Some people who received this message don't often get email from utah-dmv@hawaii.edu. Learn why this is important

CAUTION: This email is from a sender *outside* Utah Tech. Verify the sender before opening links or attachments.

Important Notification.

Your driver's license has been flagged and limited, as error(s) were detected on your records, during our regular scheduled maintaince.

You have been strictly advised to resolve this issue to avoid termination of your license.

Please visit: UTAH DMV - MVR PERSONAL to resolve the issues on your records.

Sincerely,

Utah Department of Motor Vehicles

OneScreen devices used as Web Proxy device

- Information Security detected suspicious traffic from a device doing extensive port scans to a large number of internet hosts.
- After further investigation it was identified as a OneScreen display board utilizing a sharing application built in for remote video input.
- Since it was connected to wireless, this allowed remote attackers to exploit a zero day in the application and enable it to be used as a web proxy device.
- Negative effects of a Web Proxy - threat actors can use proxies to obfuscate their actual IP address and make it look like University of Hawaii is attacking

OneScreen Vulnerability

- OneScreen is a smart display with touchscreen capabilities
- Android OS with “userdebug” mode on
- 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

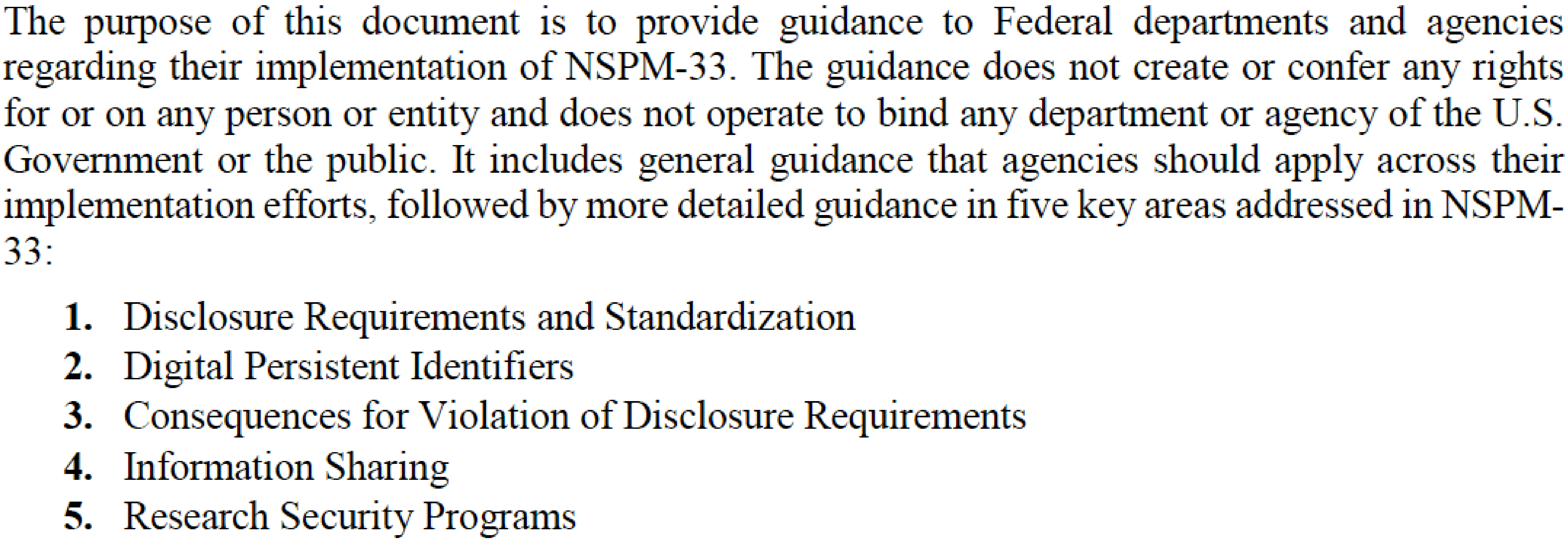
Multi-function Devices/Printers on UH Network

- 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.

Research Regulations & Compliance Update

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

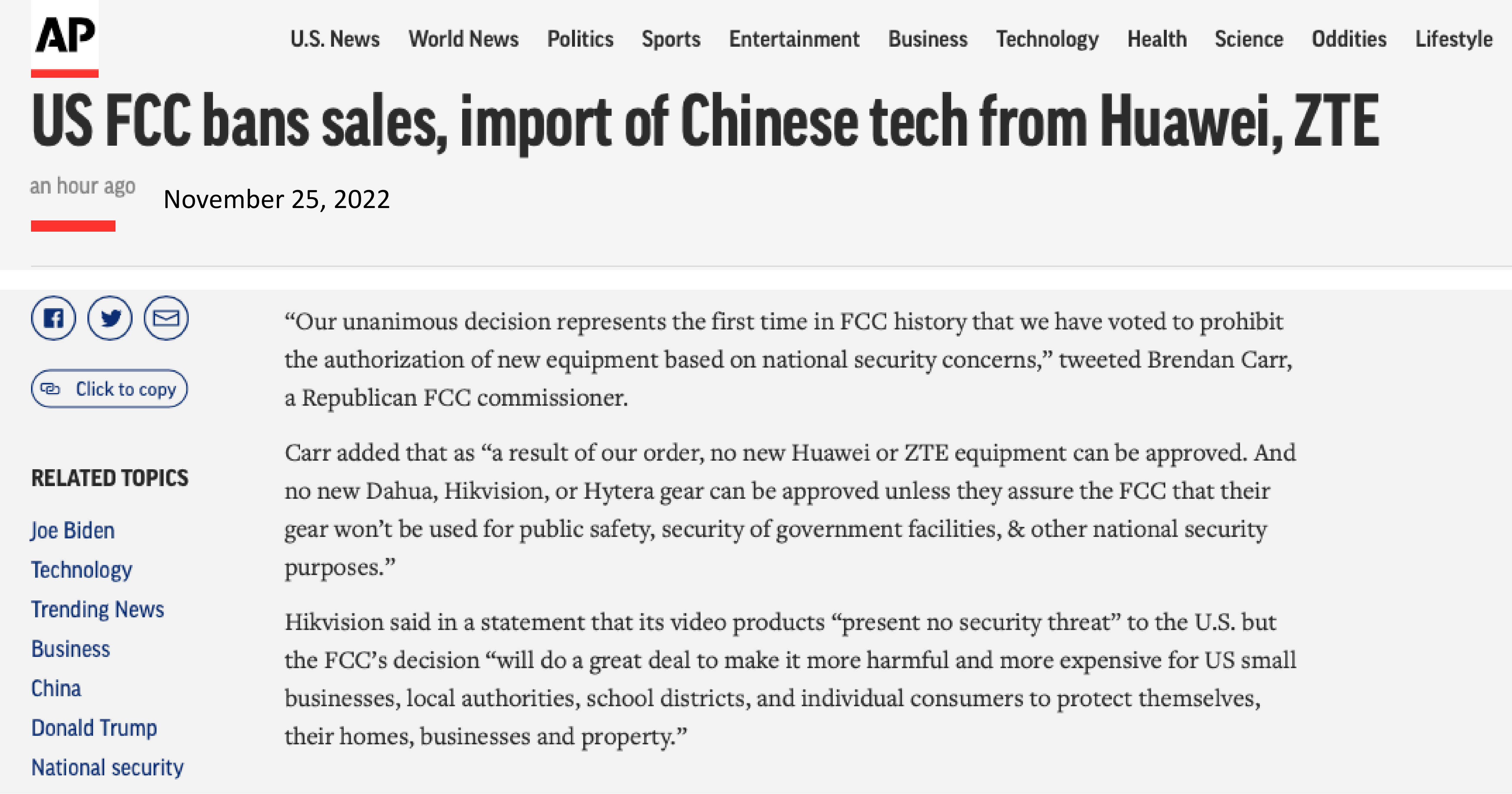


The purpose of this document is to provide guidance to Federal departments and agencies regarding their implementation of NSPM-33. The guidance does not create or confer any rights for or on any person or entity and does not operate to bind any department or agency of the U.S. Government or the public. 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

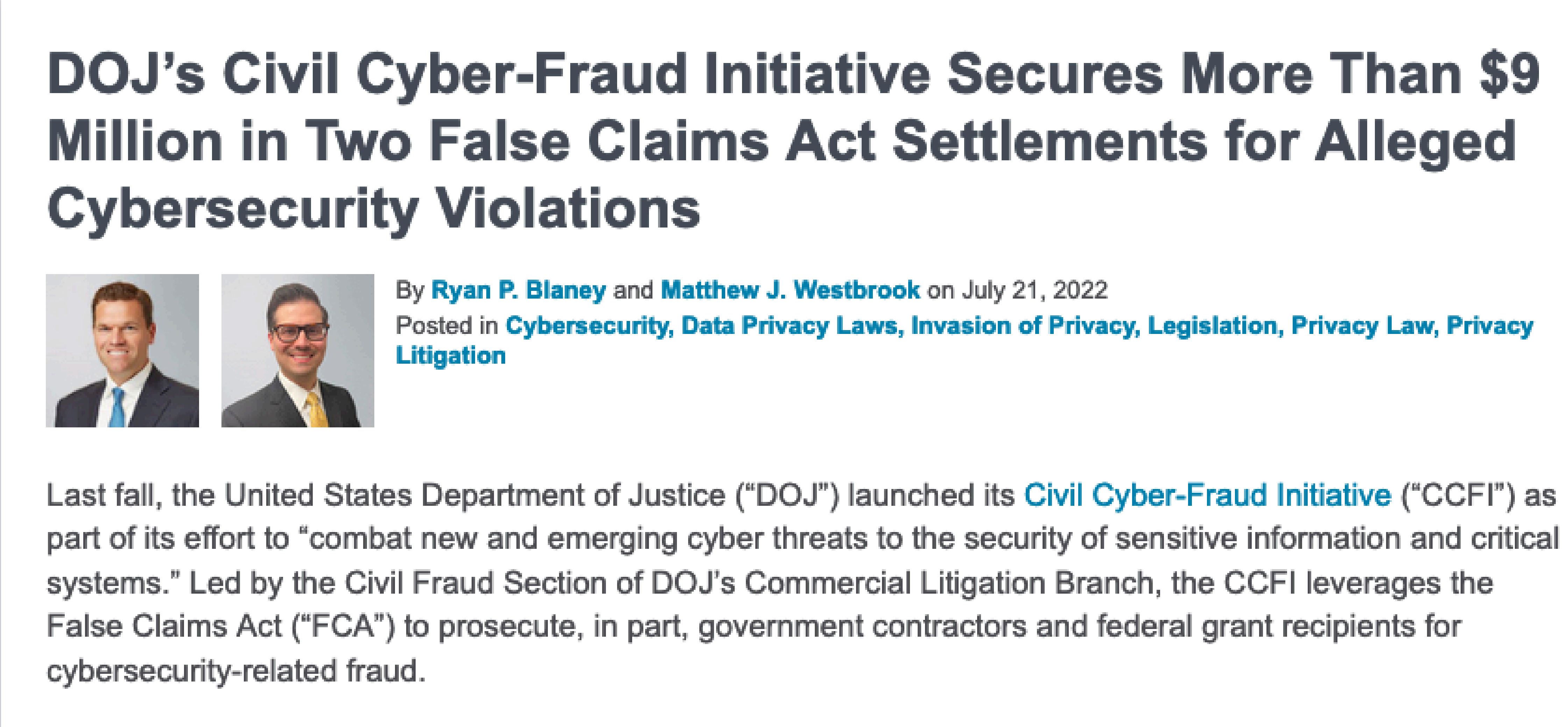
November 25, 2022

“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.”

https://apnews.com/article/biden-technology-donald-trump-national-security-federal-communications-commission-6904d9fc598321fadc8bccb430efd800



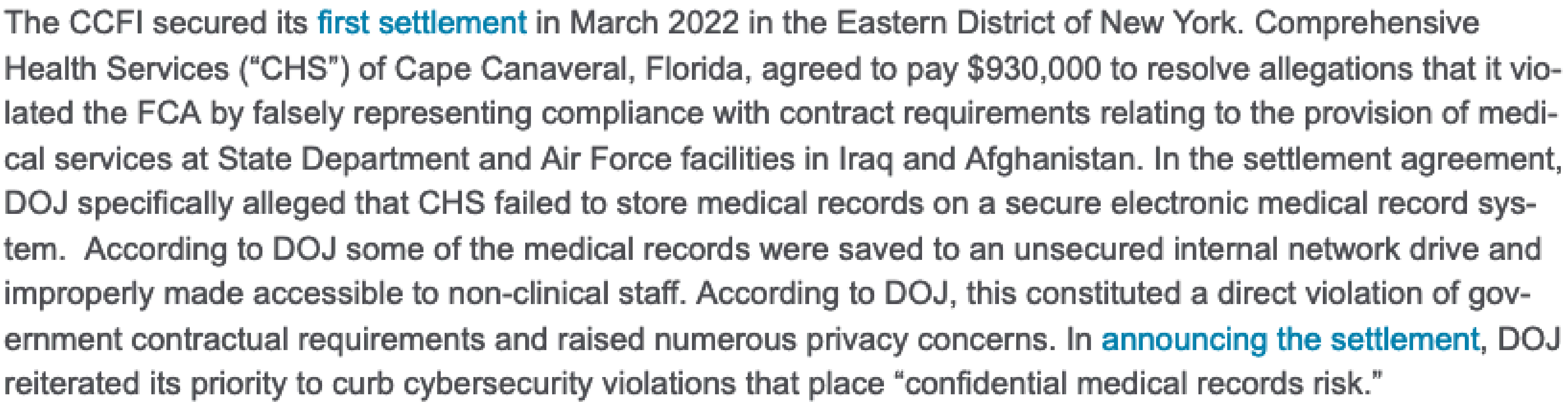
DOJ’s Civil Cyber-Fraud Initiative Secures More Than $9 Million in Two False Claims Act Settlements for Alleged Cybersecurity Violations

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

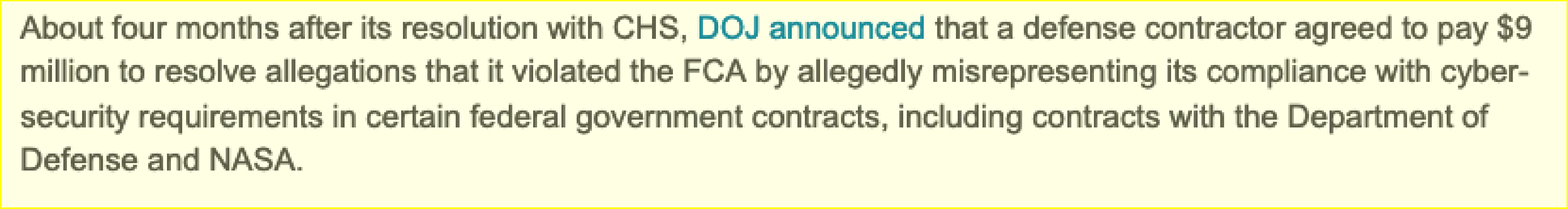
Last fall, the United States Department of Justice (“DOJ”) launched its Civil Cyber-Fraud Initiative (“CCFI”) as part of its effort to “combat new and emerging cyber threats to the security of sensitive information and critical systems.” Led by the Civil Fraud Section of DOJ’s Commercial Litigation Branch, 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."



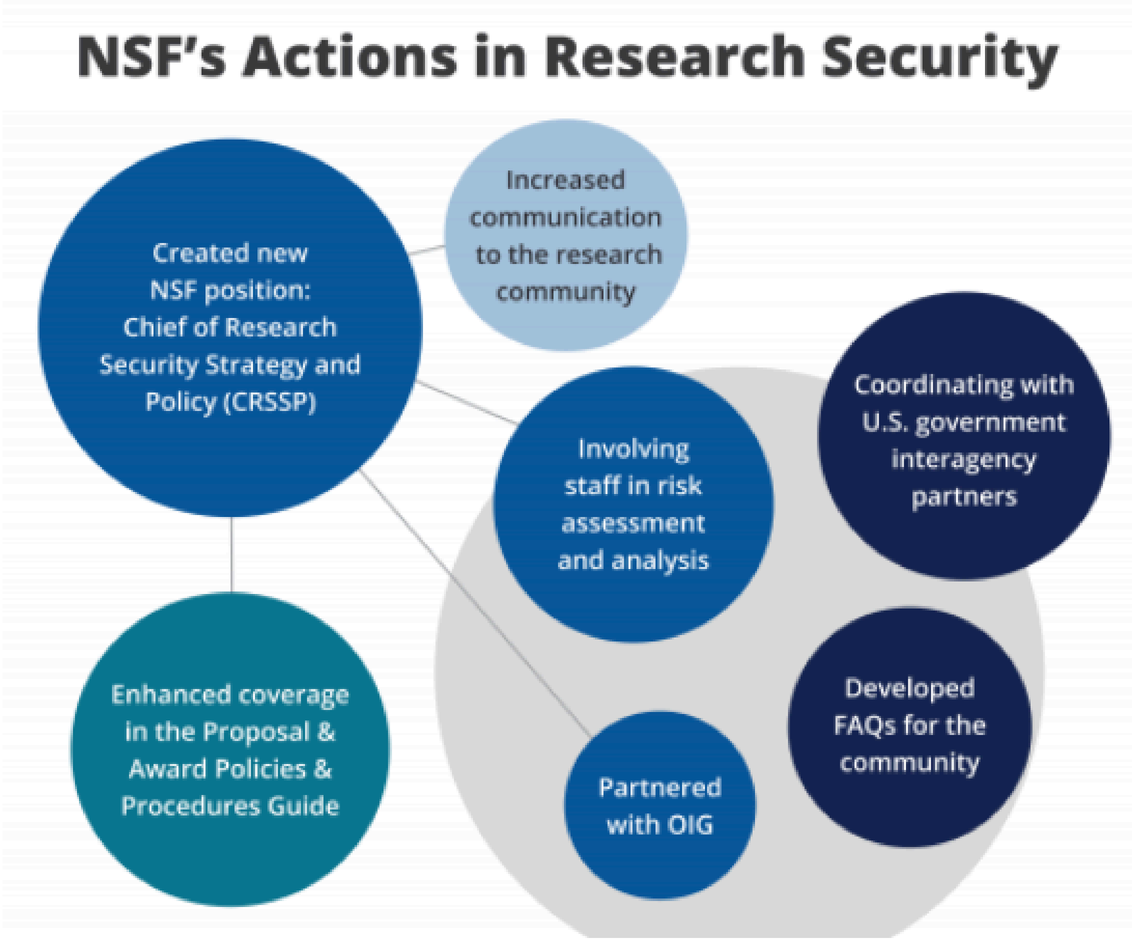
About four months after its resolution with CHS, DOJ announced that a defense contractor agreed to pay $9 million to resolve allegations that it violated the FCA by allegedly misrepresenting its compliance with cybersecurity requirements in certain federal government contracts, including contracts with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

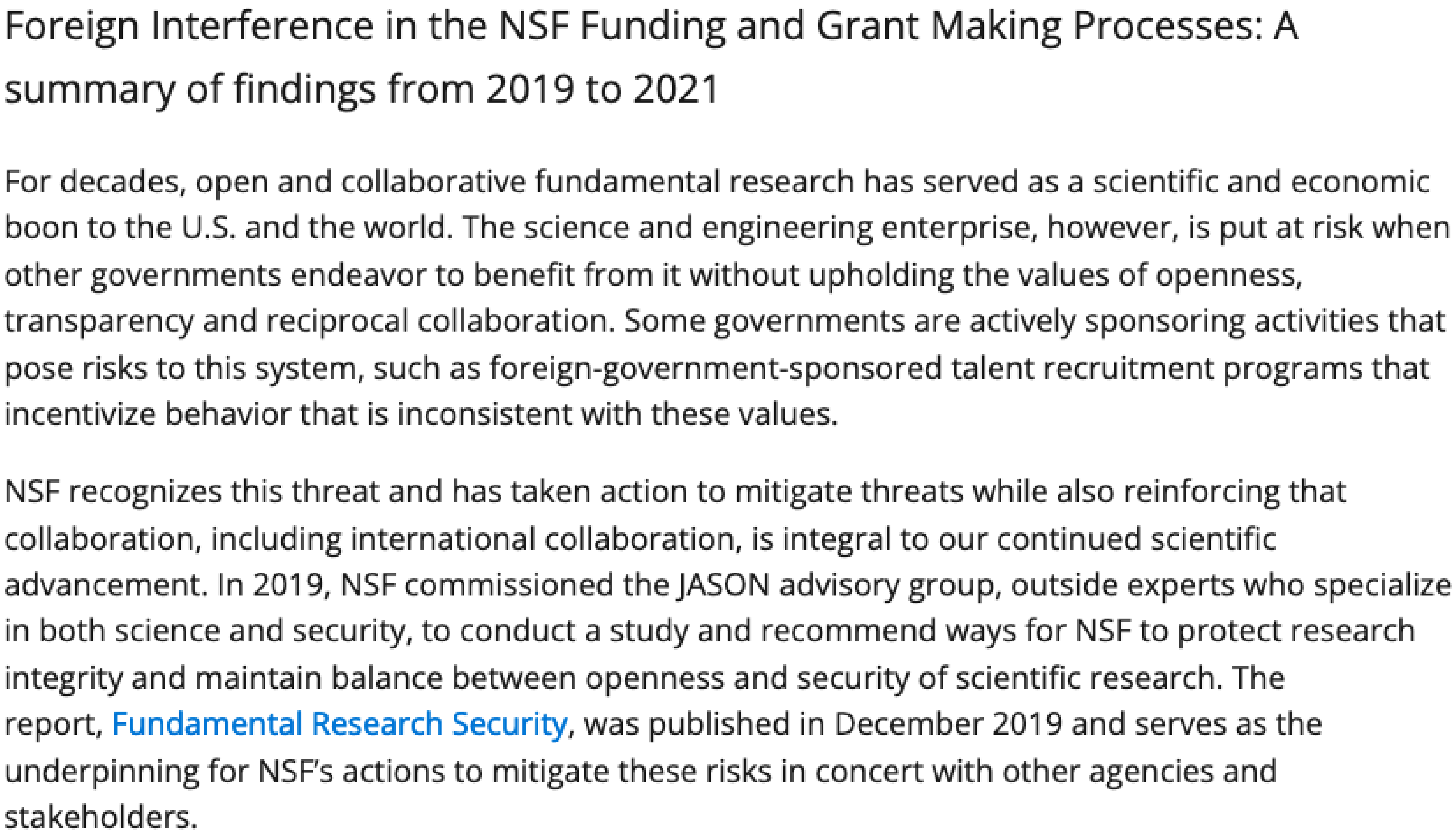
NSF's research security initiatives seek to:

- 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
Created new NSF position: Chief of Research Security Strategy and Policy (CRSSP)
Increased communication to the research community
Involving staff in risk assessment and analysis
Coordinating with U.S. government interagency partners
Enhanced coverage in the Proposal & Award Policies & Procedures Guide
Partnered with OIG
Developed FAQs for the community

Credit: National Science Foundation

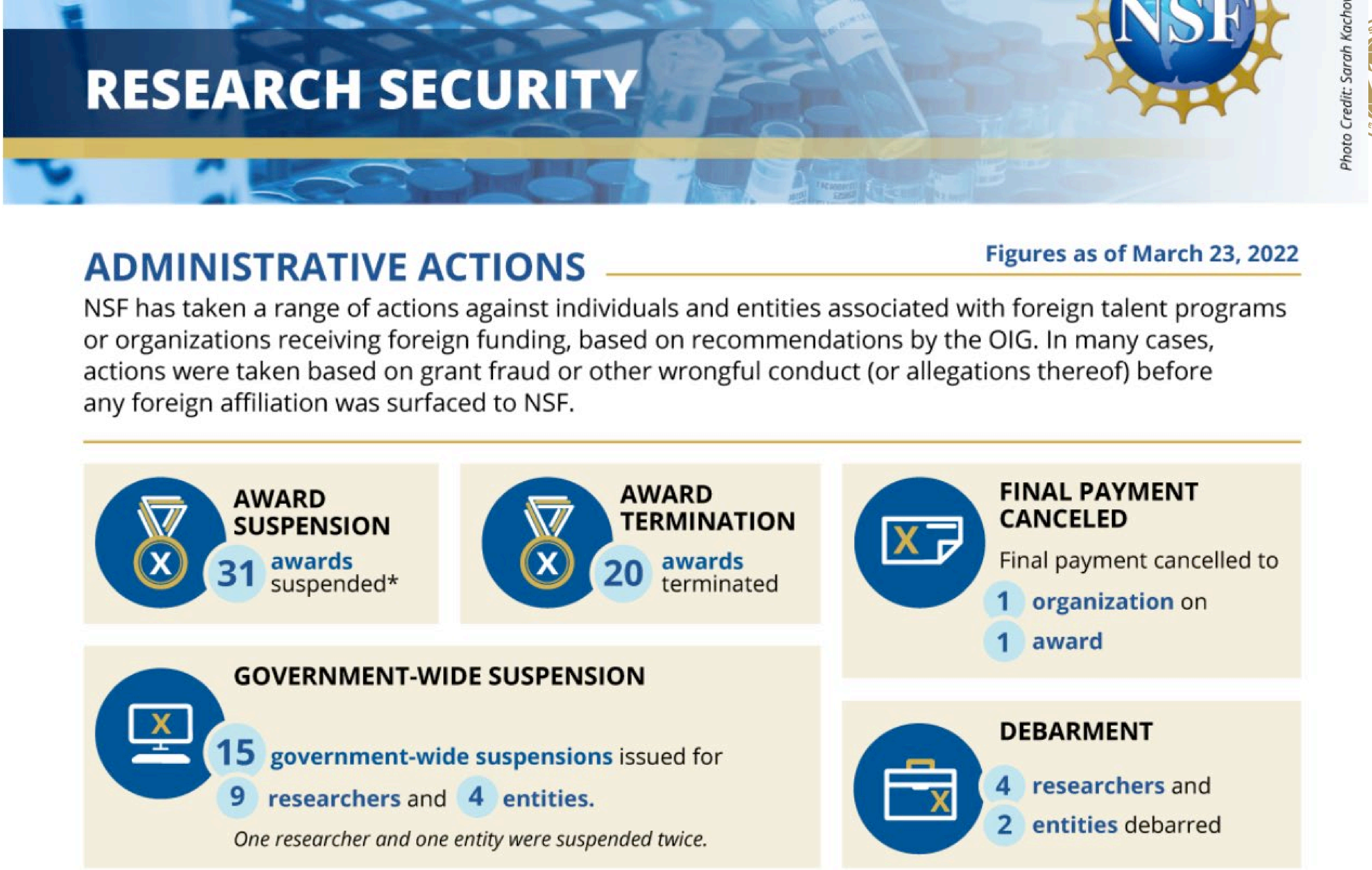
View the high resolution PDF image here



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 Kacho

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:

$11.2 M

Grant funds recovered by NSF

7

Other entities involved

26

Organizations of higher education/ small businesses involved*

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

27

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

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

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

Key Regulations and Penalties – Research-related (1)

Regulation	Description	Penalty
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	

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

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

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

Protected Data

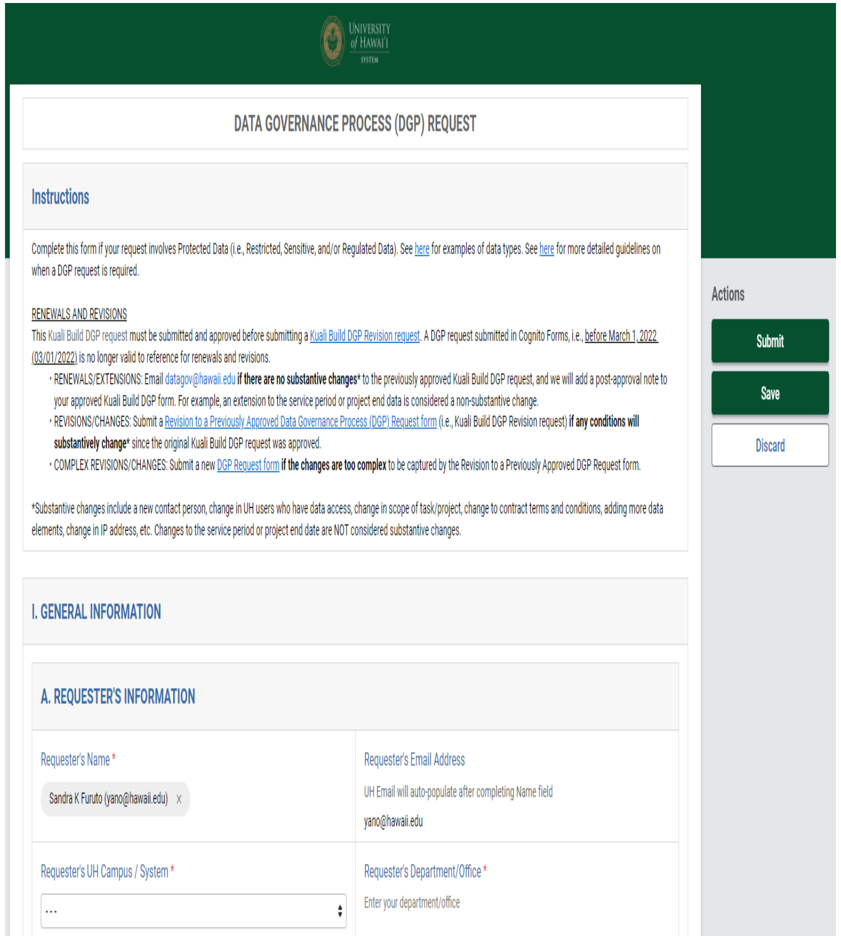
Examples of Data / Information by Category from EP2.214

	Protected Data		
Public	**Restricted**	**Sensitive**	**Regulated**
No risk	**Low risk**	**Medium risk**	**High risk**
Student Data • Name • Major field of study • Class (i.e., freshman, sophomore, etc.) 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 Data • UH email address / username • Address (street name, #) • Personal phone # 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 • Salary & payroll info Other Data • PII responses on sensitive topics (illegal activities, addiction, sexual behavior and orientation, housing/food insecurity, etc.)	FN / first initial and LN with the following: • SSN • Driver's license • Hawaiʻi 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

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 Kuali Build DGP request must be submitted and approved before submitting a Kuali 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 Kuali Build DGP request, and we will add a post-approval note to your approved Kuali Build DGP form. For example, an extension to the service period or project end data is considered a non-substantive change.
- REVISIONS/CHANGES: Submit a Revision to a Previously Approved Data Governance Process (DGP) Request form (i.e., Kuali Build DGP Revision request) **if any conditions will substantively change*** since the original Kuali 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 * Sandra K Furuto (yano@hawaii.edu) x	Requester's Email Address 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

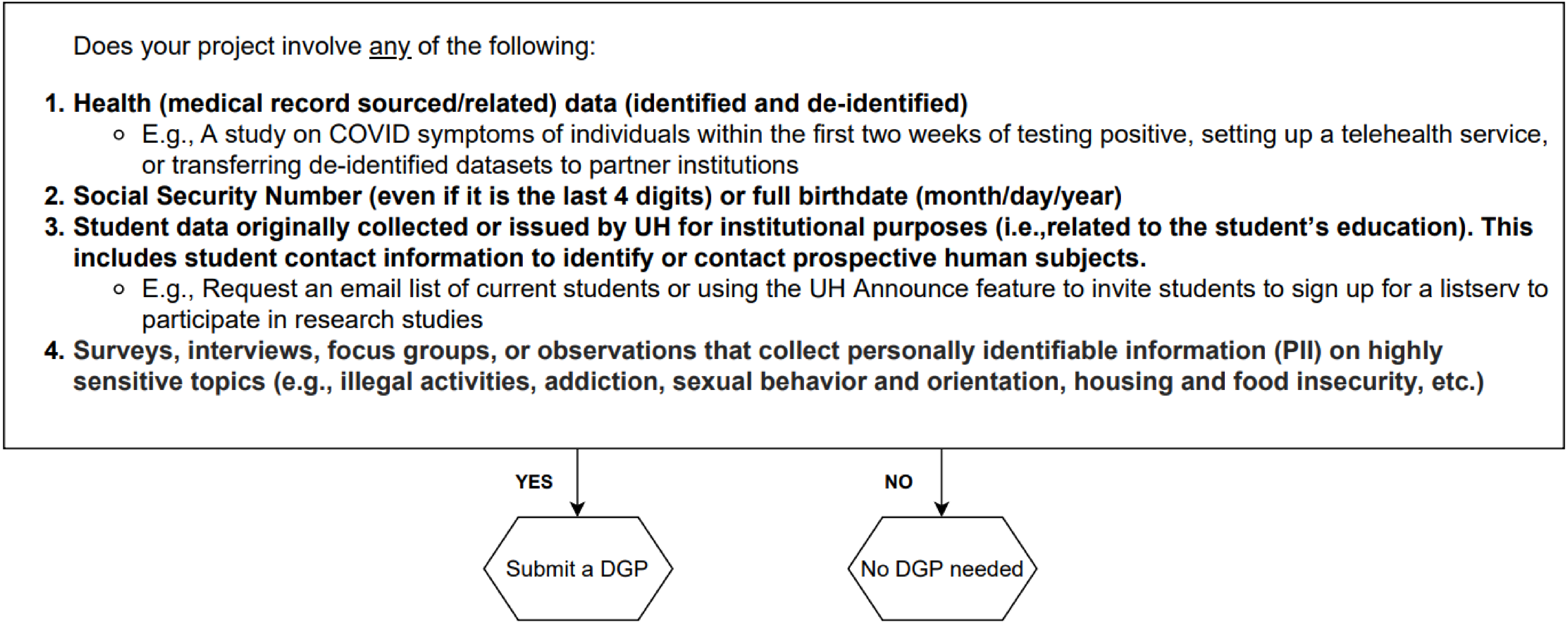
https://datagov.intranet.hawaii.edu/dgp/

- **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

When the DGP Applies for Research

- Applies to specific types of research data
  - Health data, SSN/DOB, student data, collection of highly sensitive PII
- Can be internal or external to UH
  - Internal – involves data outside your normal purview (e.g., study involving analysis of student data)
  - External – third party services involving a transfer of research data (e.g., purchasing a dataset from a registry)
- Mainly applies to people data (PII and de-identified data)

4 Types of Data Requiring 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.)**

http://go.hawaii.edu/N3V

Activities Requiring a DGP

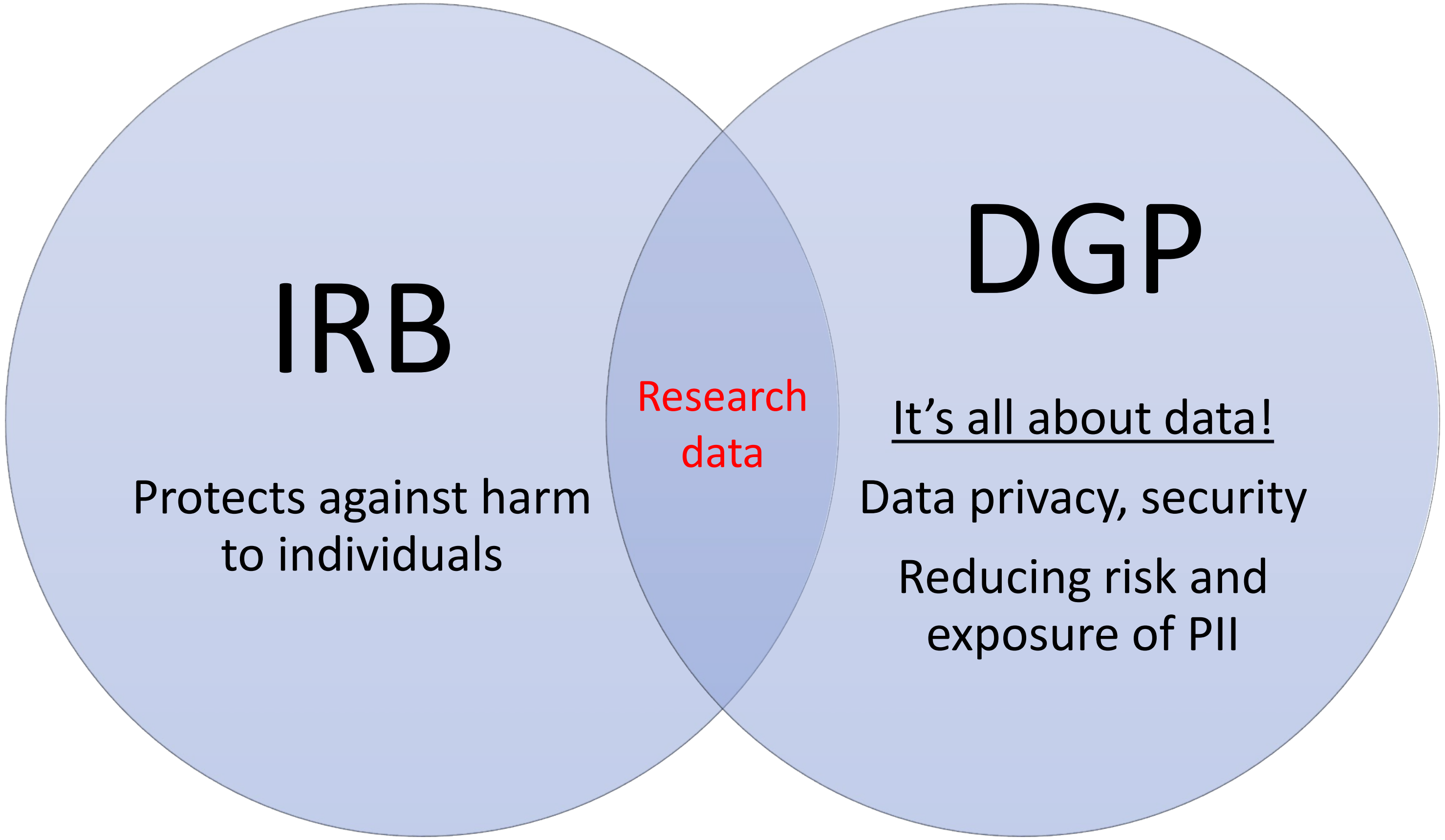
- Purchasing a product/services from a third party vendor
  - Telehealth or translation services
- Releasing data to an external party or website
  - Cloud-based services
- Requesting data you normally do not have access to
  - A researcher wants grade data to evaluate a study on student cell phone addiction
- Conducting research for a thesis/dissertation
  - A graduate student requests student outcomes of Native Hawaiians
- Storing non-UH data from a third party
  - Program doing a study for HIDOE on concussions, downloading data from databanks
- Collecting self-reported data
  - Health-related survey to help at risk populations

DGP Materials Required

- DGP request: https://datagov.intranet.hawaii.edu/dgp/
- Unsigned agreement (MOA/MOU, DUA/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.

Why DGP When We Already Have IRB?



IRB

Protects against harm to individuals

Research data

DGP

It's all about data!

Data privacy, security

Reducing risk and exposure of PII

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

Annual Information Security Awareness Training (ISAT)

Who	Per AP2.215, required for all UH employees, including student and graduate assistants, RCUH, and UHF employees (with a few exceptions: e.g., BU01)
What	Annual ISAT training, <1 hour to complete
Where	https://hawaii.edu/infosec/training/
When	On or before your anniversary date
Why	Federal compliance requirements, increased cybersecurity risk, reduce data breaches and exposures

ISAT Rollout: PeopleSoft and RCUH Employees

Campus	Valid ISAT	Total Employees	% Compliant
System	499	567	88.0%
Manoa	3,061	8,366	36.6%
Hilo	316	819	38.6%
West O‘ahu	262	397	66.0%
Hawai‘i CC	180	292	61.6%
Honolulu CC	127	484	26.2%
Kapi‘olani CC	245	504	48.6%
Kaua‘i CC	74	191	38.7%
Leeward CC	337	441	76.4%
Maui College	210	340	61.8%
Windward CC	98	231	42.4%
RCUH	371	2,265	16.4%
TOTAL	**5,780**	**14,897**	**38.8%**

As of 10/12/22

Questions?

Sean Cleveland, seanbc@hawaii.edu

Sandra Furuto, yano@hawaii.edu

Valerie Iinuma, viinuma@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