



Issues & Threats During a Pandemic

Jodi Ito
Chief Information Security Officer
jodi@hawaii.edu

Information Security Team
infosec@hawaii.edu

Increased Threats to UH

- Several organizations (including UH) have noted a large increase of scans and RDP/SSH/VNC/DB bruteforcing attacks from non-attributable cloud providers such as Google, Microsoft, Amazon, DigitalOcean, and others since this summer.
- It is believed that this is due to ransomware operators forming a **cartel** to buy access to the networks of victimized organizations from other criminal groups, affiliates, and contractors who are offered a commission on the payout.
- In 2020, criminal gangs have been demanding ransom payments of over \$1 million. One of the largest demands was 136,000 BTC or \$1.5 billion for a global corporation.

Notable HE Ransomware Attacks

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



The screenshot shows the BBC News website interface. At the top, there's a navigation bar with the BBC logo, a 'Sign in' button, and links to Home, News, Sport, Reel, Worklife, Travel, and Future. Below this is a red banner with the word 'NEWS' in white. Underneath the banner is another red bar with links to Home, US Election, Coronavirus, Video, World, US & Canada, UK, Business, Tech, Science, and Stories. The 'Tech' link is highlighted. Below the navigation, the article title 'How hackers extorted \$1.14m from University of California, San Francisco' is displayed in large, bold, dark grey text. Below the title, it says 'By Joe Tidy' and 'Cyber reporter'. At the bottom left of the article preview, it says '29 June'.

How hackers extorted \$1.14m from University of California, San Francisco

By Joe Tidy
Cyber reporter

29 June

<https://www.bbc.com/news/technology-53214783>

Ransomware Gangs who Exfiltrate/Leak Stolen Data

Avaddon

ClOp

Conti/Ryuk

CryLock

Crysis/Dharma

DarkSide

DoppelPaymer

Egregor

Fonix

Light

LockBit

Maze

MountLocker

Nemty

Nefilim/Nephilim

Netwalker

OldGremlin

Pysa/Mespinoza

ProLock

RagnarLocker

RansomExx

Ranzy/Ako

Revil/Sodinokibi

Sekhmet

Snake

Snatch

SunCrypt

[◀ Back to blog](#)

NetWalker Blog

Secret data: HIDDEN DATA

Password:

Secret data publication in: 7d 17h 59m 42s

CareersUSA and founder/Chief Executive Officer Marilyn J. Ounjian have received numerous accolades, including the South Florida Business Journal's Business Woman and Business of the Year awards, and being named a regional finalist for Ernst & Young's Entrepreneur of the Year award.

[illegible]

Clients

[Archive](#)

[Contact Us](#)

 Search

Clients



Enerstar Rentals & Services

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

\$13M

2020-10-07 2530



 Makalot Industrial

http://www.makalot.com.tw/eng/

\$760m

 5%

2020-09-25 6018

 ThyssenKrupp System Engineering

 <http://thyssenkrupp.com>

\$35b

30r

 100%

2020-09-30 5893

MountLocker victims

October 21, 2020

Ransomware groups are going corporate

Derek B. Johnson

Follow @DerekDoesTech



Canon is among the companies targeted by a sophisticated ransomware attack this year. Ransomware groups are increasingly adopting the practices and tactics of the corporate businesses they target. (DennisM2)

As ransomware attacks have quickly morphed over the past few years into a billion-dollar business, the groups behind them are increasingly adopting the practices and tactics of the corporate businesses they target.

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

MOST POPULAR

Popular Emailed Recent

[B&N cyberattack calls into question the retailer's network segmentation practices](#)

[SC Media aces phishing test \(whew!\), but average score was only 52%](#)

[URL address spoofing flaw keeps mobile victims from determining fake, real sites](#)

[Cyber Solarium Commission lays out plan to secure supply chain](#)

[Phishing scams use redirects to steal Office 365, Facebook credentials](#)

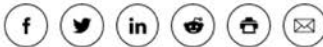


October 21, 2020

Ransomware groups are going corporate

Derek B. Johnson

[Follow @DerekDoesTech](#)



MOST POPULAR

Popular Emailed Recent



As ransomware attacks have quickly morphed over the past few years into a billion-dollar business, the groups behind them are increasingly adopting the practices and tactics of the corporate businesses they target.

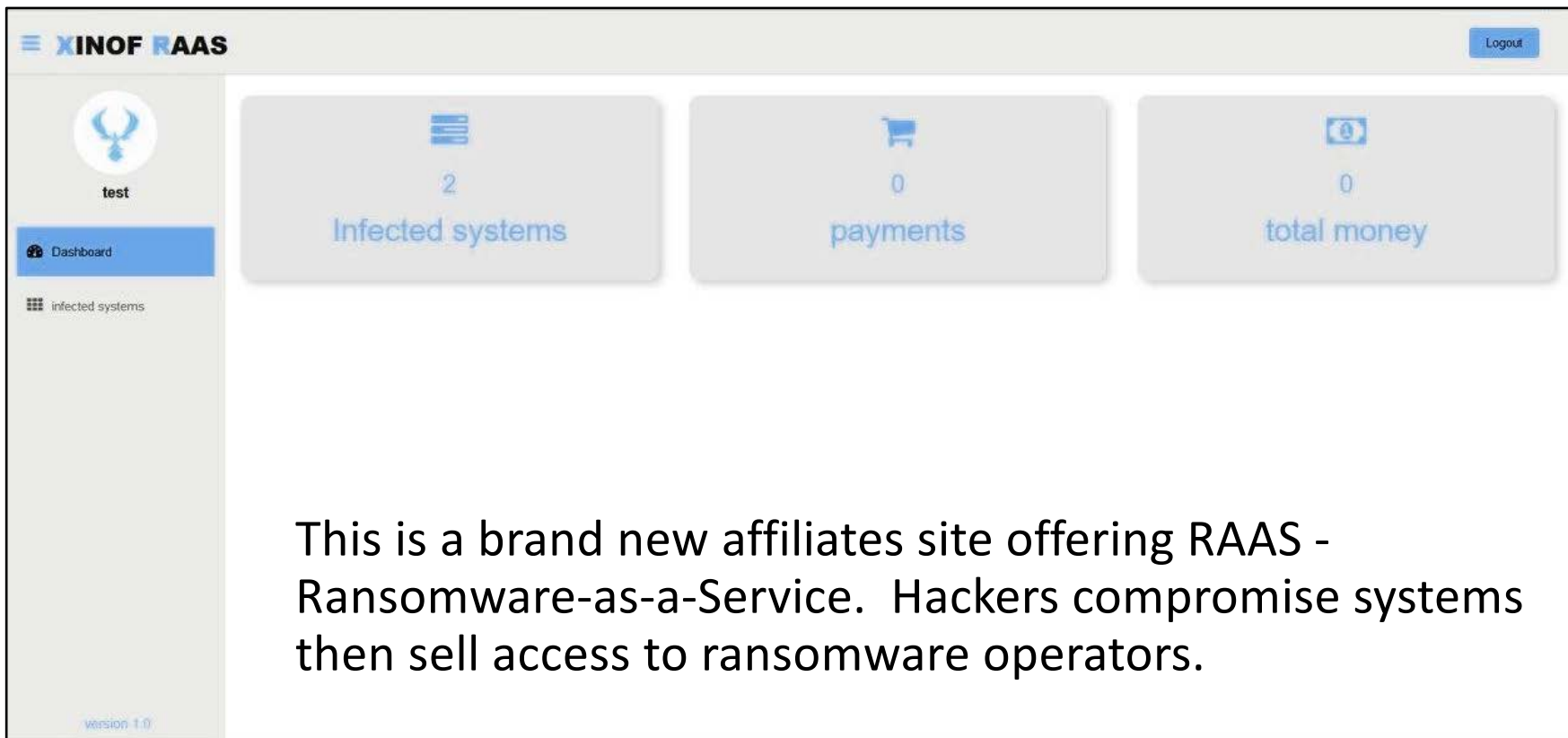
More and more, ransomware groups (and some argue the larger cybercrime ecosystem) are gravitating towards joint partnerships and profit sharing arrangements with other hacking groups, introducing tools to measure the efficiency of their work, creating playbooks and scripts during the negotiation phase,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

Canon is among the companies targeted by a sophisticated ransomware attack this year. Ransomware groups are increasingly adopting the practices and tactics of the corporate businesses they target. (DennisM2)

As ransomware attacks have quickly morphed over the past few years into a billion-dollar business, the groups behind them are increasingly adopting the practices and tactics of the corporate businesses they target.

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

RAAS - Ransomware-as-a-Service



The screenshot displays the XINOF RAAS dashboard. The header includes the 'XINOF RAAS' logo and a 'Logout' button. The left sidebar features a user profile for 'test' and navigation links for 'Dashboard' and 'infected systems'. The main content area shows three summary cards: 'Infected systems' with a count of 2, 'payments' with a count of 0, and 'total money' with a count of 0. The version 'version 1.0' is noted in the bottom left corner.

This is a brand new affiliates site offering RAAS - Ransomware-as-a-Service. Hackers compromise systems then sell access to ransomware operators.

Two Threats to Watch Out For...

- Credential Stuffing
 - Attacker uses credentials stolen from other websites in order to gain access into the target organization
- Malware (SpearPhishing)
 - Attacker infects victim machines with malware in order to gain access into the target organization

Credential Stuffing

Collection of Public Data Dumps

12,755 files totaling 708GB

4.6 billion credentials

Matches on "@hawaii.edu"

146,774 credentials

4,402 credentials (complexity match)

1,649 passwords reset since 2019

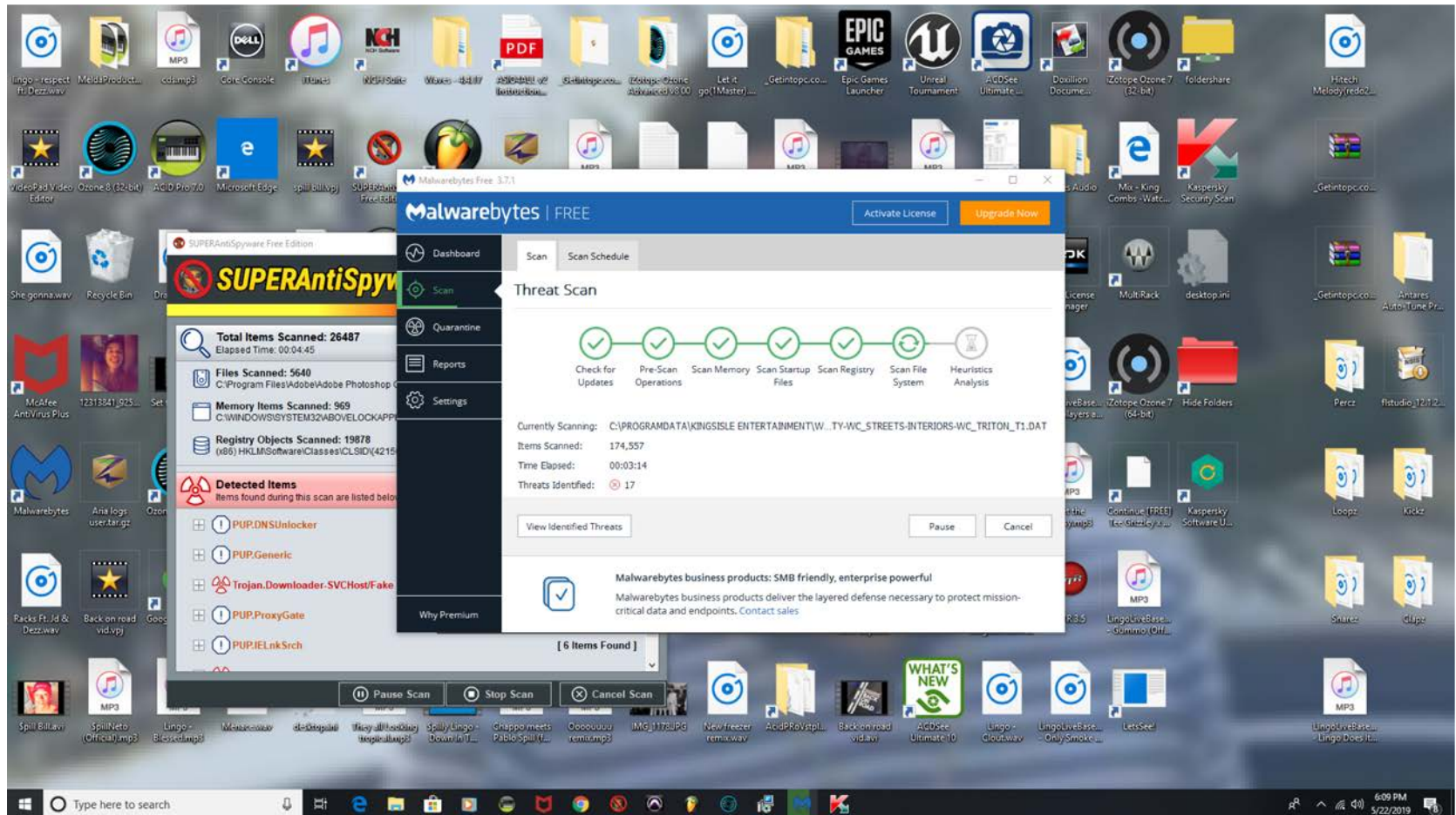
Chegg breach accounted for
82% of password resets at UH

<https://haveibeenpwned.com/>

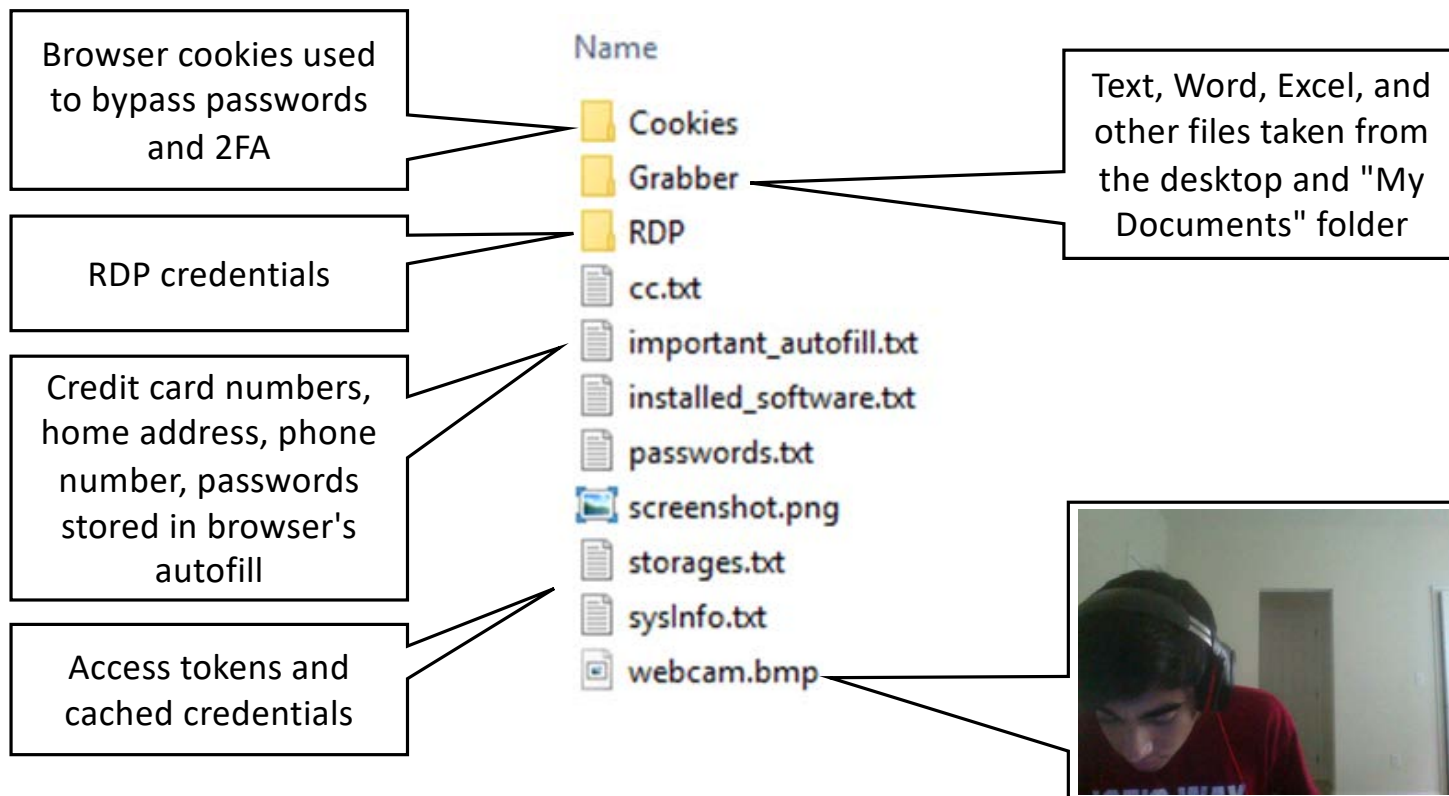
Cafepress.com_1.2kk.txt	38,049 KB
Cafepress.com_11kk.txt	345,562 KB
Canva.com_98k.txt	3,230 KB
Canva.com_904k.txt	29,893 KB
Canva.com-orig_137kk.txt	23,762,811 KB
CashCrate.com_6kk.txt	195,829 KB
Cex.io_95k.txt	3,117 KB
CFire.mail.ru_8.7kk.txt	267,713 KB
CFire.mail.ru_924k.txt	27,951 KB
ChatBooks.sql-orig_15.8kk.txt	6,487,924 KB
ChatBooks_2kk.txt	68,313 KB
CheatGamer.com_337k.txt	10,660 KB
Chegg.com_29kk.txt	978,945 KB
Chegg.com-orig_39.8kk.txt	8,755,782 KB
ChristianPassions_997k.txt	113,621 KB
ClixSense.com_2.2kk.txt	69,928 KB
CoinBulb.com_587k.txt	20,420 KB
Corevin.com_732k.txt	22,543 KB
CouponMom_1.1kk.txt	349,674 KB
DaFont.com_661k.txt	21,492 KB
DailyMotion_823k.txt	27,080 KB
DailyMotion-EmailPass_1kk.txt	34,896 KB

MALWARE

This screenshot was taken when malware executed on a victim's PC. This user has **McAfee**, **SUPERAntiSpyware**, **MalwareBytes**, and **Kaspersky**.



This malware will **steal data** from the computer and **send** it off to its Command and Control, then **delete itself** so the user will find no evidence of an infection and take no action (e.g. don't change passwords)



This malware will steal passwords from all browsers, email, FTP, chat, and other programs.
12 UH users were affected by this malware.

Google Chrome		https://www.car2go.com/en/a	
Google Chrome		http://www.audiobooks.com/a	1
Google Chrome		https://www.roblox.com/	
Google Chrome		https://postmates.com/apply	
Google Chrome		https://us.battle.net/accou	!
Google Chrome		https://login.live.com/ppse	
Google Chrome		https://accounts.google.com	
Google Chrome		https://auth.zappos.com/ap/	
Google Chrome		https://www.facebook.com/	
Google Chrome		https://cas.uni.edu/cas/log	
Google Chrome		https://passport.twitch.tv/	
Google Chrome		https://www.paypal.com/web	
Google Chrome		https://idp.thrivent.com/n	
Google Chrome		https://sm-prd11.ucollabora	a
Mozilla Firefox		https://accounts.google.c	
Mozilla Firefox		https://bandcamp.com	cr
Mozilla Firefox		https://www.facebook.com	
Mozilla Firefox		https://www.paypal.com	
Mozilla Firefox		https://www.lynda.com	
Mozilla Firefox		https://austin.bibliocomm	
Mozilla Firefox		https://www.reddit.com	
Mozilla Firefox		https://accounts.google.c	
Mozilla Firefox		https://app.roll20.net	
Mozilla Firefox		https://memberidentity.uf	
Mozilla Firefox		https://www.dominos.com	
Mozilla Firefox		https://us.battle.net	c
Mozilla Firefox		https://twitter.com	



Things we do to ourselves

- "self phished" ourselves

DoNotReply@hawaii.edu

UH LMS Notice - Certification Signup

To: jodi@hawaii.edu,

Reply-To: DoNotReply@hawaii.edu

Inbox - UH August 20, 2020 at 7:42 AM



Certification Signup

You have signed up for **COVID-19 Safety Training Certification**.

Certification Details

Target Date:

Get **more information** at the [COVID-19 Safety Training Certification](#) certification page.

You are receiving this email because you have signed up for COVID-19 Safety Training Certification.

[University of Hawai'i](#) - Knowledge Sharing powered by **Saba Cloud!** | © [Saba](#)

WFH issues

- Transitioning to digital/electronic workflows could introduce more risk
 - Use of email for information exchange/sharing
 - Sharing/exchange of "protected" information
 - Acquisition of & routing for signatures for internal processes
- Flood in the use of (and request to use) "microservices"
 - Zoom integration tools
 - Academic tools
 - Need to review privacy policies, data security, terms & conditions
- Using @hawaii.edu as a "user account" (gmail account) to sign up on other services



Keeping up with “Regs”



FEDERAL REGISTER

The Daily Journal of the United States Government



0 Sign in Sign up

Rule

Federal Acquisition Regulation: Prohibition on Contracting With Entities Using Certain Telecommunications and Video Surveillance Services or Equipment

A Rule by the [Defense Department](#), the [General Services Administration](#), and the [National Aeronautics and Space Administration](#) on 07/14/2020



a.k.a. NDAA 889 / HHS 889

<https://www.federalregister.gov/documents/2020/07/14/2020-15293/federal-acquisition-regulation-prohibition-on-contracting-with-entities-using-certain>

PUBLISHED DOCUMENT

Start Printed Page 42665

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

ACTION:
Interim rule.

SUMMARY:
DoD, GSA, and NASA are amending the Federal Acquisition Regulation (FAR) to implement section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 ([Pub. L. 115-232](#)).

DOCUMENT DETAILS

Printed version:
[PDF](#)

Publication Date:
[07/14/2020](#)

Agencies:
[Department of Defense](#)
[General Services Administration](#)
[National Aeronautics and Space Administration](#)

Dates:
Effective: August 13, 2020.

Effective Date:
[08/13/2020](#)

Document Type:
Rule

Document Citation:

Section 889's Two Prohibitions

https://acquisition.gov/FAR-Case-2019-009/889_Part_B



- Part A: Effective **August 13, 2019**, the Government may not **obtain** (through a contract or other instrument) certain telecommunications equipment or services produced by five named Chinese companies or their subsidiaries and affiliates
- Part B: Effective **August 13, 2020**, the Government may not contract with an entity that **uses** certain telecommunications equipment or services, as a substantial or essential component of any system, or as critical technology as part of any system, produced by any of the same five named Chinese companies or their subsidiaries and affiliates
 - *Use is “regardless of whether that use is in performance of a Federal contract”*

What does this mean?

- As of August 13, 2020, government agencies are prohibited from contracting with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system
- Prohibition applies regardless of whether or not that usage is in performance of work under a Federal contract
- UH cannot purchase/use any telecom or video surveillance equipment or services from:
 - Huawei Technologies Company
 - ZTE Corporation
 - Hytera Communications Corporation
 - Hangzhou Hikvision Digital Technology Company
 - Dahua Technology Company
 - or any subsidiary or affiliate of these entities

Why are these changes important?



The danger our Nation faces from foreign intelligence actors looking to infiltrate our systems has never been greater.



NDAA prohibitions against nefarious networks like Huawei will ensure our Nation remains secure. This Administration is committed to working with Congress to keep America strong through implementing the NDAA prohibitions.



Bad actors are persistent in trying to infiltrate US networks – often exploiting technologies from the identified Chinese companies to do so. The Trump Administration shares Congress's strong commitment to addressing insidious threats to the Nation's national security and intellectual property.



The Federal Government alone experiences hundreds of thousands of digital assaults every day. Malicious actors are persistent, usually well-funded and constantly changing their tactics. They often exploit technologies from the identified Chinese companies to do so. The Administration shares Congress' strong commitment to addressing insidious threats to the Nation's national security and intellectual property.



The Trump Administration is keeping our government systems strong against nefarious networks like Huawei by leaning into Congress's Huawei ban with an aggressive posture.

Part A - The Government Cannot Obtain Prohibited Telecom

Part A became effective on **August 13, 2019**.

Part A prohibits the government from obtaining (through a contract or other instrument) certain telecommunications equipment (including video surveillance equipment) or services produced by the following *covered entities* and their subsidiaries and affiliates:

- **Huawei Technologies Company**
- **ZTE Corporation**
- **Hytera Communications Corporation**
- **Hangzhou Hikvision Digital Technology Company**
- **Dahua Technology Company**

The Department of Defense has the authority to add additional companies to this list.

Part A has been added to the Federal Acquisition Regulation (FAR) at [FARsubpart 4.21](#).

Note that the Part A ban also applies to **commercial items** ([FAR 12.301\(d\)\(6\)](#)) and **micro-purchases** ([FAR 13.201\(j\)](#)).

Have questions about GSA's implementation of Section 889? See [GSA's 889 Part A Q&As](#)

Part B - Government Contractors Cannot Use Prohibited Telecom

Part B is effective **August 13, 2020**.

Part B prohibits the government from contracting with any entity that uses certain telecommunications equipment or services produced by the *entities* listed in the statute.

- The Government cannot contract with an entity 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.
- The prohibition applies to every sector and every dollar amount. **Your ability to enter into contracts with the Government will be impacted by Part B.**
- After conducting a reasonable inquiry, entities will represent whether they do or do not use prohibited telecommunications equipment or services.

Part B has been added to the Federal Acquisition Regulation (FAR) at [FARsubpart 4.21](#).

New Interim DFARS Rules

- DFARS Clause 252.204-7020: NIST SP 800-171 DoD Assessment Methodology
 - Effective November 1, 2020
 - Must submit a self assessment of 800-171 compliance on SPRS website before award
 - <https://www.sprs.csd.disa.mil/reference.htm>
- DFARS Clause 252.204-7021: Cybersecurity Maturity Model Certification (CMMC)
 - By Oct. 2025, CMMC certification will be required for ALL DoD contracts
 - Phased rollout
 - FY 21: 15 contractors will be selected (including subcontractors)



UNCLASSIFIED



Projected CMMC Roll-Out

- OUSD(A&S) is working with Services and Agencies to identify candidate programs that will have the CMMC requirement during FY21-FY25 phased roll-out

Total Number of New Prime Contracts Awarded Each Year with CMMC Requirement				
FY21	FY22	FY23	FY24	FY25
15	75	250	479	479

	Total Number of Prime Contractors and Sub-Contractors with CMMC Requirement				
	FY21	FY22	FY23	FY24	FY25
Level 1	899	4,490	14,981	28,714	28,709
Level 2	149	749	2,497	4,786	4,785
Level 3	452	2,245	7,490	14,357	14,355
Level 4	0	8	16	24	28
Level 5	0	8	16	24	28
Total	1,500	7,500	25,000	47,905	47,905


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

DISTRIBUTION A. Approved for public release

UNCLASSIFIED

Eventually Student Info will be CUI

Home > Controlled Unclassified Information (CUI) > CUI Category: Student Records



Use the CUI logo

Contact Us

Contact an Agency

About CUI

- CUI History
- FAQs

CUI Registry

- Categories
- CUI Markings
- Limited Dissemination Controls
- Decontrol
- Registry Change Log
- Policy and Guidance
- Glossary

CUI Reports

CUI Training

CUI Resources

CUI Blog

CUI Category: Student Records

Banner Marking for Specified Authorities: CUI//SP-STUD

Banner Marking for Basic Authorities: CUI

Category Description:	As per 20 USC 1232g, the Family Educational Rights and Privacy Act of 1974, an education record which is comprised of those records which are directly related to a student.
Category Marking:	STUD
Alternative Banner Marking for Basic Authorities:	CUI//STUD
Banner Format and Marking Notes:	<p>Banner Format: CUI//Category Marking//Limited Dissemination Control</p> <p>Marking Notes:</p> <ul style="list-style-type: none">• The CUI Control Marking may consist of either the word "CONTROLLED" or the acronym "CUI", depending on agency policy.• Category marking is optional when marking Basic CUI unless required by agency policy. Example: CUI//Limited Dissemination Control.• Category Marking preceded by "SP-" is required when marking Specified CUI. Example: CUI//SP-Category Marking//Limited Dissemination Control• Whether CUI is Basic or Specified is determined by the applicable Safeguarding and/or Dissemination Authority for a given instance of CUI.• Separate multiple Category Markings by a single forward slash (/) and list Category Markings alphabetically. Example: CUI//Category Marking A/Category Marking B//Limited Dissemination Control• Category Markings for Specified CUI precede Category Markings for Basic CUI. Example: CUI//SP-Category Marking/Category Marking//Limited Dissemination Control• Separate multiple Limited Dissemination Controls by a single forward slash (/). Example: CUI//Category Marking//Limited Dissemination Control/Limited Dissemination Control• Reference 32 CFR 2002.20 , CUI Marking Handbook , Limited Dissemination Controls and individual agency policy for additional and specific marking guidelines

<https://www.archives.gov/cui/registry/category-detail/student-records>



Draft Federal Student Aid Strategic Plan FY2020-24



- <https://studentaid.gov/sites/default/files/fy2024-strategic-plan-draft.pdf>
- Strategic Goal 4: Strengthen Data Protection and Cybersecurity Safeguards
 - 4.2: Improve student privacy data and cybersecurity controls of IHEs through outreach and communication, to mitigate future cyber incidents and breaches
 - 4.3: Build an effective cybersecurity culture through employee awareness, training and accountability focused on protecting systems and data
 - “Performance metrics” mentions assessment findings & OMB compliance audits



ITS Security Initiatives



Free Certificates!

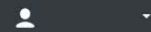
- InCommon Certificates are now available at no charge:
 - <http://www.hawaii.edu/siteic/incommon/>
- All UH websites should be using a certificate (SHA-2)
- All CAS URL registrations will require a certificate (https) in 2021
 - Be on the lookout for retirement of TLS v1.1
 - TLS v1.1 deprecated earlier this year



OpenVAS is now ScanUH



ScanUH Start Scanning ▾ Views ▾ Request Access Contact Us ▾



UNIVERSITY of HAWAII®

ScanUH

<https://scanuh.hawaii.edu>

Submit Scan

Submitting a Scan

Use the form below to start a vulnerability scan on target subnets and/or IP addresses within the UH System. This scanner will not scan any addresses that fall outside of UH. Keep in mind that you may only scan targets you have been authorized for.

To scan an address you have not yet been approved for, submit a request on our [Request Access Page](#).

To scan the computer you are visiting this page from, please visit our [Self Scan Page](#).

In times of high volume, your scan task may not start immediately and instead be placed in a queue. In the event that this happens, your scan will be started once previous scans complete and resources free up.

Scans originate from the 128.171.171.24/29 network.

Your Approved Targets

Check/uncheck to add/remove scan targets

Subnet/IP



Scan Targets

List each target on a newline in the textbox below

128.171.171.24/29

Scheduled Scanning (Optional)

[Enable Scheduling](#)

Alive Testing (Enabled by Default)

Internal Scanning Solutions

- Nessus Scanner w/ Tenable.sc
 - Self hosted scanner behind your firewall
- Nessus Agents w/ Nessus Manager (and ScanUH Soontm)
 - Lightweight; install agent on each machine

<https://www.hawaii.edu/infosec/assets/vuln-scan/>

[UH Login Required]

Cyber Hygiene Best Practices

Home > Minimum Security Standards > Cyber Hygiene Best Practices

Cyber Hygiene Best Practices

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

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

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

Best Practice	Description	References
1 Anti-Malware Software and Host Based Firewalls	<p>Install Anti-Malware software and ensure its signatures are regularly updated. Anti-Malware software is a key protective measure to detect, quarantine, and remove various types of malware.</p> <p>McAfee anti-virus software is licensed by the University of Hawaii (UH), Information Technology Services (ITS) site license for use by active UH faculty, staff, and students: https://www.hawaii.edu/askus/1254</p> <p>In addition to installing Anti-Malware software, most modern Operating Systems include built-in firewalls, which are commonly referred to as Host Based Firewalls. Host Based Firewalls run on your device and provide an additional layer of protection from network cyberattacks.</p>	<ul style="list-style-type: none"> US-CERT Security Tip (ST18004) Protecting Against Malicious Code: https://us-cert.cisa.gov/ncas/tips/ST18-271 ITS MSS 8.1 — Ensure Anti-Malware Software and Signatures are Updated US-CERT Security Tip (ST04004) Understanding Firewalls for Home and Small Office Use: https://us-cert.cisa.gov/ncas/tips/ST04-004 ITS MSS 9.1 — Apply Host-Based Firewalls or Port Filtering

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

Source: <https://www.hawaii.edu/infosec/minimum-standards/cyber-hygiene/>

UH ITS Minimum Security Standards

Minimum Security Standards

As part of the UH Data Classifications Policy (EP 2.214) technical guidelines for each data classification category shall be followed to prevent the inadvertent exposure and inappropriate disclosure of Institutional Data that are considered protected data.

University of Hawai'i Data Classification

Public Data	Protected Data		
Public (No Risk)	Restricted (Low Risk)	Sensitive (Medium Risk)	Regulated (High Risk)
No privacy considerations.	Data used internally within the UH community but not released to external parties without a contract or memorandum of agreement.	Data subject to privacy considerations.	Highly sensitive data that is subject to state breach notification requirements, financial fines, or other penalties.
Definition: Institutional Data where access is not restricted and is subject to open records requests	Definition: Institutional Data used for UH business only. Restricted data will not be distributed to external parties except under the terms of a written memorandum of agreement or contract. Data is maintained in a physically secured location.	Definition: Institutional Data subject to privacy or security considerations or any Institutional Data not designated as public, restricted, or regulated. Data is maintained in a physically secured location.	Definition: Institutional Data where inadvertent disclosure or inappropriate access requires a breach notification in accordance with HRS §487N or is subject to financial fines. Social Security Number (SSN) and personal financial information fall within this category. Data is maintained in a physically secured location.

[UH Login Required] Examples of Data / Information by Category

Minimum Security Standards by Device [UH Login Required]

Below are links to the minimal standards based on the type of UH Institutional Data Category (Public, Restricted, Sensitive, and Regulated) and device type (Endpoints, Servers, and MFDs).

The standards listed in the respective tables are based on the Center for Internet Security's (CIS) Controls, which are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks.

The standards listed below are a subset of the CIS Controls based on its applicability to the University of Hawai'i.



Per Executive Policy 2.214 - Institutional Data Classification Categories and Information Security Guidelines:

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

Source: <https://www.hawaii.edu/infosec/minimum-standards/>

UH ITS Minimum Security Standards Mapping

ITS has mapped the Minimum Security Standards (MSS) against:

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

Points to remember:

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

ITS Minimum Security Standards Mapping by Cybersecurity Maturity Model Certification Levels 1 to 3			
ITS Minimum Security Standards	CMMC Controls Mapping Levels 1 to 3		
	Level 1	Level 2	Level 3
1 - Inventory and Control of Hardware Assets: Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access. (CIS Control 1)			
1.1 - Maintain Detailed Asset Inventory: Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not. (CIS Control 1.4)	<input type="checkbox"/> AC.1.001 <input type="checkbox"/> AC.1.002	<input type="checkbox"/> CM.2.061 <input type="checkbox"/> CM.2.064	
1.2 - Maintain Asset Inventory Information: Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network. (CIS Control 1.5)		<input type="checkbox"/> CM.2.061 <input type="checkbox"/> CM.2.064	

ITS Minimum Security Standards Mapping by HIPAA Safeguard Type					
ITS Minimum Security Standards	HIPAA Safeguard Type				
	Administrative	Physical	Technical	Organizational	Policies and Procedure and Documentation Requirements
1 - Inventory and Control of Hardware Assets: Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access. (CIS Control 1)					
1.1 - Maintain Detailed Asset Inventory: Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not. (CIS Control 1.4)		<input type="checkbox"/> 164.310(b) <input type="checkbox"/> 164.310(c) <input type="checkbox"/> 164.310(d) <input type="checkbox"/> (2)(ii)			
1.2 - Maintain Asset Inventory Information: Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network. (CIS Control 1.5)		<input type="checkbox"/> 164.310(b) <input type="checkbox"/> 164.310(c) <input type="checkbox"/> 164.310(d) <input type="checkbox"/> (2)(ii)			

ITS Minimum Security Standards Mapping by PCI DSS SAQ Type				
ITS Minimum Security Standards	PCI DSS 3.2.1 Controls Mapping by SAQ Type			
	SAQ A	SAQ C	SAQ C-VT	SAQ P2PE
1 - Inventory and Control of Hardware Assets: Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access. (CIS Control 1)				
1.1 - Maintain Detailed Asset Inventory: Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not. (CIS Control 1.4)		<input type="checkbox"/> 9.9(a) <input type="checkbox"/> 9.9.1(a)(b)(c) <input type="checkbox"/> 11.1.1	<input type="checkbox"/> 12.3.3	<input type="checkbox"/> 9.9(a) <input type="checkbox"/> 9.9.1(a)(b)(c)
1.2 - Maintain Asset Inventory Information: Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network. (CIS Control 1.5)		<input type="checkbox"/> 9.9(a) <input type="checkbox"/> 9.9.1(a)(b)(c) <input type="checkbox"/> 11.1.1	<input type="checkbox"/> 12.3.3	<input type="checkbox"/> 9.9(a) <input type="checkbox"/> 9.9.1(a)(b)(c)



Fall DG & IS Briefings



- Fall Data Governance and Information Security briefings:
 - Two identical sessions
 - Friday, Oct. 30: 9 – 11am
 - Monday, Nov. 9: 12 – 2pm
- Topics to be covered:
 - Current threats & vulnerabilities
 - Policy and regulation updates
 - Zoom guidelines and issues
 - Open records request handling
 - ADA updates
- One more DG & IS session – RESEARCH FOCUSED
 - Tentative date: Dec. 3 – time: TBD

And.... Drum roll please!



IS COMING SOON!!

(More details at DG & IS Briefing next week!)



Questions?

jodi@hawaii.edu
infosec@hawaii.edu