

Cybersecurity Law and Policy in the Second Trump Administration

November 2025

James (“Jim”) Dempsey
Managing Director, IAPP Cybersecurity Law Center
Lecturer, UC Berkeley Law School
Senior Policy Advisor, Stanford Program on
Geopolitics, Technology and Governance
jdempsey@berkeley.edu

Cybersecurity Law in the U.S.



Common Law (esp. negligence)

Criminal Statutes

Pre-Internet Consumer Protection Law (state and federal)

Privacy Laws – protecting personal data (state and federal)

Pre-internet Regulatory Frameworks

Breach Reporting Obligations (state and federal)

Gov't Procurement Rules

Critical Infrastructure Statutes and Regulations

National Security Law/Trade Law

National Cyber Strategy for Second Trump Administration

“By November 2025, we will have an emerging picture of cybersecurity policy in this term.”

Cyber strategy is still being drafted.
(National security strategy may come first.)

Expected elements of cyber strategy:

- Strengthen the role of ONCD
- Stress partnerships with the private sector instead of regulation
- “shift away from victims towards villains” = more offensive cyber



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

FY 25 budget: \$2.973 billion (same as FY 24)

FY 26 budget:

- President requested \$495 million cut (18%)
- House Appropriations approved \$135 million cut (4.6%)
- No action by the Senate

Workforce: $3200 - 1000 = 2200$ (not counting contractors)

“CISA’s effectiveness has been weakened by steep workforce and budget cuts that undermine its ability to support operators on the ground.” CSC 2.0 (Oct. 22, 2025)

Is Cybersecurity a Local Issue?



“Preparedness is most effectively owned and managed at the State, local, and even individual levels, supported by a competent, accessible, and efficient Federal Government. ... Citizens are the immediate beneficiaries of sound local decisions and investments designed to address risks, **including cyber attacks**, wildfires, hurricanes, and space weather.

Resilience strategy – anticipated for publication June 17, 2025.

Review of critical infrastructure policies – to be completed by Sept. 15, 2025.

It is the policy of the United States that **State and local governments and individuals** play a more active and significant role in **national resilience** and preparedness.”

Continuity vs. Change

EO 14306 (June 6, 2025) amended Biden EO 14144 (Jan. 16, 2025)

- Deleted provisions
 - Digital identity for access to gov services
 - Phishing-proof MFA on federal systems
 - NIST to develop new guidance on minimum cybersecurity practices
 - Requiring fed. agencies to use available PQC products
 - Urging fed. agencies to explore the use of AI for cybersecurity
- Kept provisions
 - Software attestation provisions for gov. purchases in EO 14028
 - Better management of the Federal use of open source
 - CISA threat hunting in federal systems
 - E2E encryption for federal voice and video comms
 - Improve federal interface with BGP
- The Cybersecurity Patchwork Quilt Remains Incomplete (July 16, 2025)
<https://www.lawfaremedia.org/article/the-cybersecurity-patchwork-quilt-remains-incomplete>

1. Cybersecurity Information Sharing Act (CISA 2015) Has Sunset

“Notwithstanding any other provision of law,” a private entity may --

- Monitor its information system or authorize third-party monitoring
- Share with, or receive from, any entity or the federal government a cyberthreat indicator or defensive measure
- Operate a defensive measure
- No use of information shared for enforcement purposes
- No hack back

September 30, 2025:

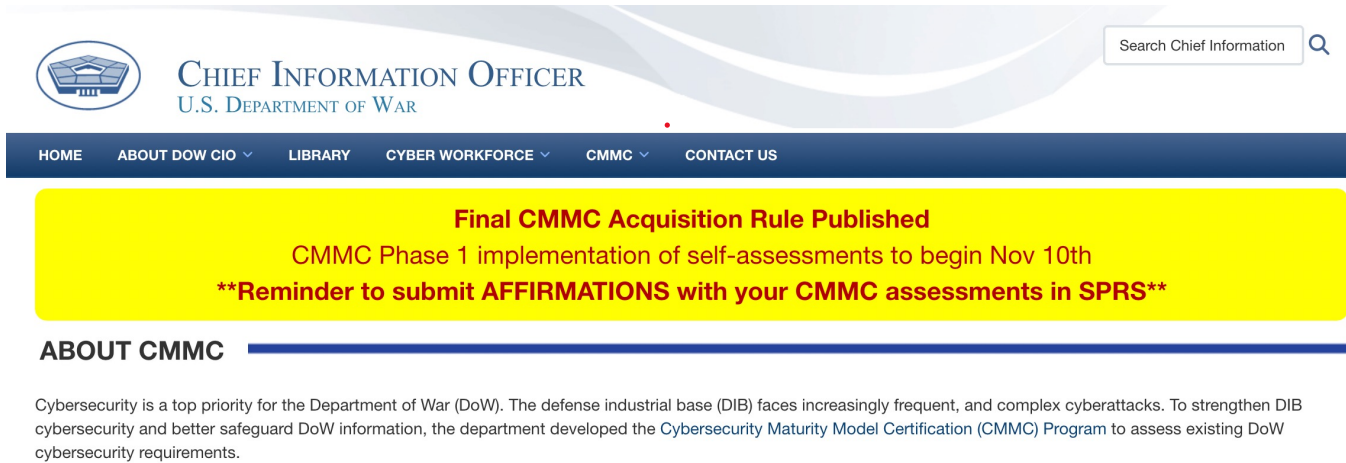


Alvesgaspar, CC BY-SA 3.0, via
Wikimedia Commons

NCD Cairncross, Oct. 24: “the
White House is for a 10-year clean
reauthorization of CISA”

Why do we need a law to give network operators permission to monitor their own network?

2. CMMC Has Landed



The screenshot shows the official website of the Chief Information Officer of the U.S. Department of War. The header includes the DoW logo and navigation links: HOME, ABOUT DOW CIO, LIBRARY, CYBER WORKFORCE, CMMC, and CONTACT US. A prominent yellow banner reads: "Final CMMC Acquisition Rule Published", "CMMC Phase 1 implementation of self-assessments to begin Nov 10th", and "**Reminder to submit AFFIRMATIONS with your CMMC assessments in SPRS**". Below the banner, the "ABOUT CMMC" section begins with a paragraph explaining the program's purpose.

Final CMMC Acquisition Rule Published
CMMC Phase 1 implementation of self-assessments to begin Nov 10th
****Reminder to submit AFFIRMATIONS with your CMMC assessments in SPRS****

ABOUT CMMC

Cybersecurity is a top priority for the Department of War (DoW). The defense industrial base (DIB) faces increasingly frequent, and complex cyberattacks. To strengthen DIB cybersecurity and better safeguard DoW information, the department developed the Cybersecurity Maturity Model Certification (CMMC) Program to assess existing DoW cybersecurity requirements.

Nov. 10, 2025:

- 3-year phased roll-in began
- CMMC clauses will start appearing in contracts

<https://business.defense.gov/Engage/News/Newsfeed-Repository/Article/4303493/its-official-cmmc-has-landed/>

“Complaining to the world that the CMMC is too hard ... you’re foolish What you’re saying is you’re noncompliant.”

-Katie Arrington, Acting DoW CIO, June 5, 2025.

DFARS 252.204-7012 (Dec. 2017) → NIST SP 800-171

3. False Claims Act

"Together with DoD and other agency partners, the Department of Justice will continue to pursue and litigate violations of cybersecurity requirements to hold **contractors** accountable when they violate their cybersecurity commitments." Assistant AG Brett Shumate, Sept. 30, 2025.

Illumina Inc. to Pay \$9.8M to Resolve False Claims Act Allegations Arising from Cybersecurity Vulnerabilities in Genomic Sequencing Systems

Thursday, July 31, 2025

For Immediate Release

PRESS RELEASE

Georgia Tech Research Corporation Agrees to Pay \$875,000 to Resolve Civil Cyber-Fraud Litigation

Tuesday, September 30, 2025

For Immediate Release

Case 1:22-cv-02698-JPB Document 23 Filed 08/22/24 Page 1 of 99

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA *ex rel.*
CHRISTOPHER CRAIG and
KYLE KOZA,

Civil Case No.:
1:22-cv-02698-JPB

Plaintiff,

v.

GEORGIA TECH RESEARCH CORP.
and BOARD OF REGENTS OF THE
UNIVERSITY SYSTEM OF GEORGIA
(d/b/a THE GEORGIA INSTITUTE OF
TECHNOLOGY),

Defendants.

JURY TRIAL DEMAND

UNITED STATES' COMPLAINT-IN-INTERVENTION

Plaintiff the United States of America (United States) brings this action against Defendants Georgia Tech Research Corporation (GTRC) and the Board of

4. DOJ Takedowns

All News

Blogs

Photo Galleries

Podcasts

Press Releases

Speeches

Videos

Justice Department Announces Coordinated Disruption Actions Against BlackSuit (Royal) Ransomware Operations

Monday, August 11, 2025

Share >

For Immediate Release

Office of Public Affairs

Law Enforcement Seizes Servers, Domains, and Approximately \$1 Million in Laundered Proceeds Owned By BlackSuit (Royal) Ransomware

The Justice Department announced today coordinated actions against the BlackSuit (Royal) Ransomware group which included the takedown of four servers and nine domains on July 24, 2025. The takedown was conducted by the Department of Homeland Security's Homeland Security Investigations (HSI), the U.S. Secret Service, IRS Criminal Investigation (IRS-CI), the FBI, and international law enforcement from the United Kingdom, Germany, Ireland, France, Canada, Ukraine, and Lithuania. These actions include the unsealing of a warrant for the seizure of virtual currency valued at \$1,091,453 at the time of the seizure. The unsealing was announced today jointly by the U.S. Attorney's Offices for the Eastern District of Virginia and the District of Columbia.

[Archived News](#)



EAST BAY

Case 3:21-mj-70945-LB Document 2 Filed 06/07/21 Page 1 of 1

FILED

Jun 07 2021

SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

AO 109 (Rev. 11/13) Warrant to Seize Property Subject to Forfeiture

UNITED STATES DISTRICT COURT
for the
Northern District of California

In the Matter of the Seizure of
(Briefly describe the property to be seized)
Application by the United States for a Seizure
Warrant for One Account for Investigation of 18
U.S.C. Section 981(a)(1)(A) and other offenses

Case No. 3:21-mj-70945-LB

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests that certain property located in the Northern District of California be seized as being subject to forfeiture to the United States of America. The property is described as follows:
Approximately 63.7 BTC (the "Subject Funds") accessible from the following cryptocurrency address (the "Subject Address")
XXXXXXXXXXXX950kjpjcwuy4uj39ym43hs6cfsegq

I find that the affidavit(s) and any recorded testimony establish probable cause to seize the property.

YOU ARE COMMANDED to execute this warrant and seize the property on or before 6/21/2021
(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must also give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to
United States Magistrate Judge Laurel Beeler
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)
☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 6/7/2021 9:10 am CJB
Judge's signature

City and state: San Francisco CA Laurel Beeler
Laurel Beeler, United States Magistrate Judge
Printed name and title

5. Federal Trade Commission – the nation’s de facto privacy and data security regulator

“**unfair** or **deceptive** acts or practices in or affecting commerce are ... unlawful.”

- Section 5 of the FTC Act (1914, 1938)

Since 2000, FTC has brought about 100 data breach cases: Equifax, Zoom, GoDaddy, Drizly, CafePress, Chegg.



“Man Controlling Trade,” Photo: Gray Brechin © Creative Commons BY-NC-ND

5. FTC – unfairness

“The Commission has steadfastly maintained that companies that collect, use, share, or transmit **consumers’ personal** data must employ **reasonable security measures**, including encryption of sensitive information, to protect such information from unauthorized access, use, or disclosure.” (Citing unfairness cases.)

“Companies that promise that their service is secure or encrypted, but fail to use end-to-end encryption where appropriate, might deceive consumers who reasonably expect that level of confidentiality. Further, **certain circumstances** may require **reasonable security measures** such as end-to-end encryption, and the failure to implement such measures might constitute an **unfair** practice.”

Letter from FTC Chair Andrew Ferguson to tech companies, Aug. 21, 2025

<https://www.ftc.gov/news-events/news/press-releases/2025/08/ftc-chairman-ferguson-warns-companies-against-censoring-or-weakening-data-security-americans-behest>

5. Recent FTC Enforcement Actions

- Disney – videos published on YouTube - targeted ads - violation of **COPPA** (kids' privacy)
- Apitor Technology Co. - **China**-based robot toy maker – **COPPA** – **location** information – 3d party
- Iconic Hearts (Sendit App) – social media messaging app - **COPPA**, Sec. 5 deception, plus Sec. 5 **unfairness**
 - Unfair: sending child and teen users messages, sometimes of a provocative, romantic, or sexual nature, for the purpose of tricking them into purchasing subscriptions
- Aylo Group (Pornhub) – distribution of CSAM and NCM is an **unfair** trade practice

6. Americans' Data As a National Security Issue

The Data
Security Rule
began as EO
13873 (2019)

Cybersecurity Risk from
Kaspersky to TikTok
(May 2025)

<https://www.lawfaremedia.org/article/cybersecurity-risk-from-kaspersky-to-tiktok>

PRESS RELEASE

Justice Department Implements Critical National Security Program to Protect Americans' Sensitive Data from Foreign Adversaries

Friday, April 11, 2025

Share



For Immediate Release

Office of Public Affairs

Department Answers Frequently Asked Questions, Provides Guidance, and
Issues Limited Enforcement Policy for First 90 Days

6. DOJ Sensitive Data Rule

Prohibits or restricts

- U.S. persons
- from providing countries of concern or
- covered persons
- access to
- U.S. persons' bulk sensitive data or
- U.S. government-related data.

Bulk thresholds measured over a year, ranging from:

- human genomic data for 100 persons;
- personal identifiers like email addresses or usernames for 100,000 persons
- Regulates investment, employment, and vendor relationships
- All provisions in effect as of October 6, 2025

6. PADFAA (Protecting Americans' Data from Foreign Adversaries Act)

- Regulates only data brokers
- A data broker is defined to include an entity that makes available data of United States individuals that the entity did not collect directly from such individuals to another entity that is not acting as a service provider.
 - Key exceptions are:
 - First-party data
 - Consent
 - Providing a product where access to the data is not the product or service
 - News reporting
 - Reporting information that is available to the public
 - Disclosure to service provider.
- “personally identifiable sensitive data” includes a wide array of individuals’ PII, as well as personal communications and information identifying individuals’ online activities.
- Enforced by the FTC
- PADFAA regulates a narrower set of entities than DSP, but a wider array of data

6. DSP and PADFAA Resources

iapp

U.S. Data Security Program

Cheat Sheet

The U.S. Department of Justice's final rule on protecting Americans' sensitive data took effect on 8 April 2025. The Data Security Program was pursuant to Executive Order 14117 and is implemented by the DOJ's National Security Division. The DSP establishes controls to prevent adversaries, and those subject to their control and direction, from accessing bulk U.S. sensitive personal data and U.S. government-related data.

Scope

The Data Security Program applies to any U.S. person that engages in transactions involving U.S. sensitive personal data or U.S. government-related data when there is a potential for access by covered persons or countries of concern.

A **transaction** is within the scope of the rule if:

- ✓ It involves any access by a country of concern or covered person to any bulk U.S. sensitive personal data or government-related data.
- ✓ It involves:
 - Data brokerage
 - Vendor agreements
 - Employment agreements
 - Investment agreements

Access means logical or physical access, including the ability to obtain, read, copy, decrypt, edit, divert, release, affect, alter the state of or otherwise view or receive, in any form, including through information systems, information technology systems, cloud-computing platforms, networks, security systems, equipment or software.

Currently, there are six designated **countries of concern**:

1. China (including Hong Kong and Macau)
2. Cuba
3. Iran
4. North Korea
5. Russia
6. Venezuela

Thresholds for bulk data

Sensitive personal data means human genomic and other human "omic" biometric identifiers, precise geolocation data, personal financial data, personal health data, covered personal identifiers or any combination thereof. "Bulk" personal data is defined by numerical thresholds. The thresholds apply 12-month period and may be met through a single transaction or multiple transactions.

Type	Bulk threshold
Human genomic data	More than 100 U.S. persons
Human "omic" data (§ 202.224)	More than 1,000 U.S. persons
Biometric identifiers (§ 202.204)	More than 1,000 U.S. persons
Precise geolocation data (§ 202.242)	More than 1,000 U.S. persons
Personal financial data (§ 202.240)	More than 10,000 U.S. persons
Personal health data (§ 202.241)	More than 10,000 U.S. persons
Covered personal identifiers (§ 202.212)	More than 100,000 U.S. persons
Combined data (§ 202.205(g))	Aggregate for the lowest threshold of U.S. persons or U.S. data in that category of data

Selected definitions

Data Security Program Cheat Sheet

<https://iapp.org/resources/article/data-security-program-cheat-sheet/>

Data brokers, beware: Distinguishing PADFAA from the DOJ's DSP <https://iapp.org/news/a/data-brokers-beware-distinguishing-padfaa-from-the-doj-s-dsp>

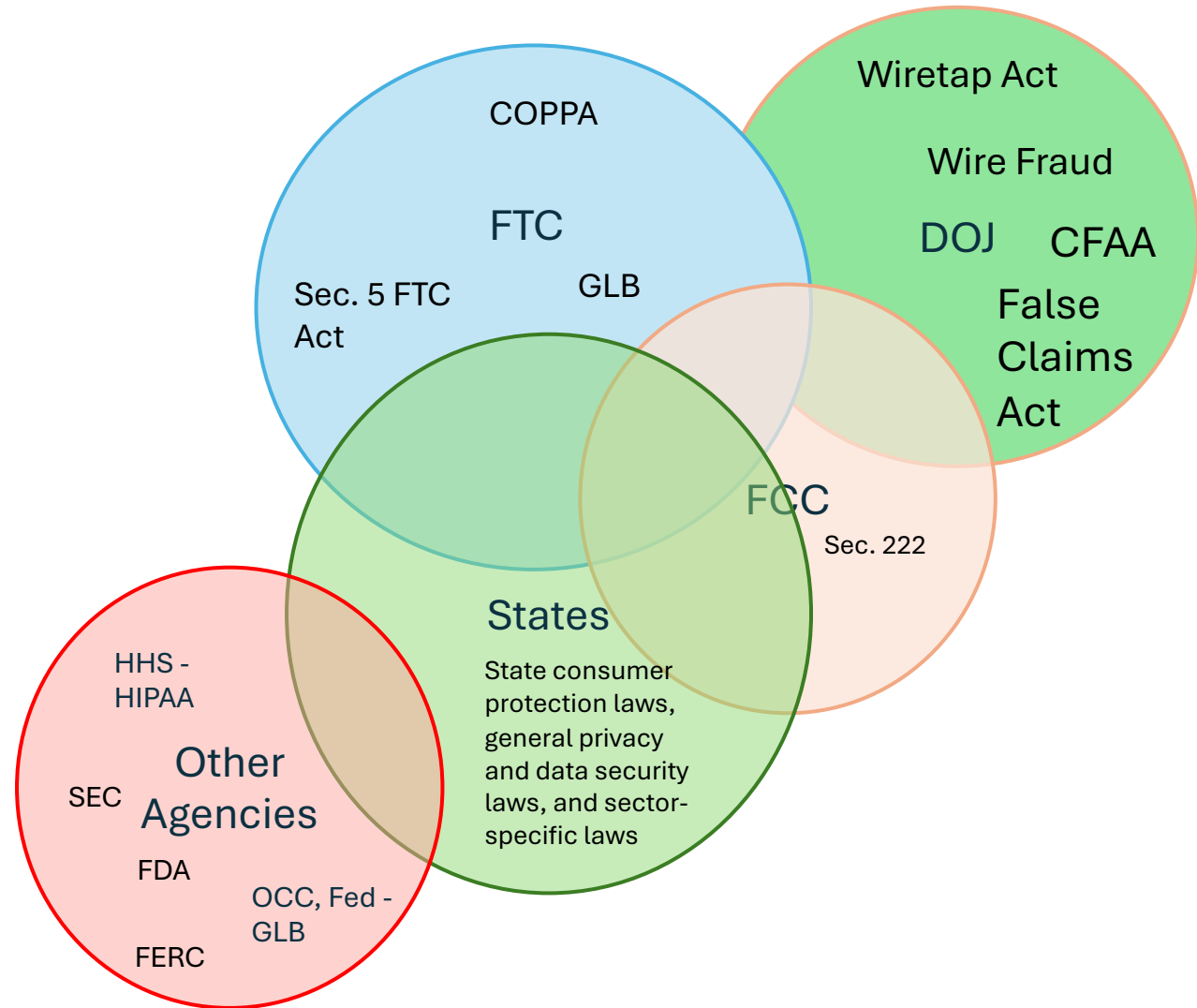
DOJ FAQs, Compliance Guide and Enforcement Policy <https://www.justice.gov/opa/pr/justice-department-implements-critical-national-security-program-protect-americans-sensitive>

Sensitive Data Rule

<https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern>

7. The States

- Unlike many other countries, the U.S. has no single federal privacy statute, cybersecurity law, or “data protection authority.”
- This leaves important authority to the states.



7. The States

All 50 states (+ DC, Guam, PR, VI) have a **breach notice** law.

All 50 states + have some form of general consumer protection law prohibiting **unfair** and/or **deceptive** acts or practices

“All businesses are required to maintain **reasonable data security**. The failure to do so is considered an **unfair or deceptive** act under Vermont’s Consumer Protection Act.” Vermont AG, 2018

31 states have statutes specifically requiring businesses to adopt **data security practices for personal information**

Most are similar to California – require “**reasonable**” security measures

Sectoral cybersecurity laws or regulations

insurance industry (based on the NAIC model) – 25 states

financial services – New York DFS

hospitals - New York Dept of Health, Title 10 NYCRR section 405.46

States have authority to enforce **HIPAA Security Rule**

32 states have **False Claims Acts** – many can be used where a contract with the state government includes a cybersecurity clause.

7. State Enforcement

- Unfair Competition Law
- False Advertising Law
- Reasonable Data Security Law
- K-12 Pupil Online Personal Information Protection Act
- Confidentiality of Medical Information Act

9	SUPERIOR COURT OF THE STATE OF CALIFORNIA	
10	FOR THE COUNTY OF LOS ANGELES	
11		
12	THE PEOPLE OF THE STATE OF CALIFORNIA,	Case No. 25STCV32380
13		COMPLAINT FOR PERMANENT INJUNCTION, CIVIL PENALTIES, AND OTHER EQUITABLE RELIEF
14		
15		(CIVIL CODE, §§ 56.06(d), 56.101(a), 56.10(a); BUS. & PROF. CODE, §§ 17200 <i>et seq.</i> , 17500 <i>et seq.</i>)
16	v.	
17	ILLUMINATE EDUCATION, INC., a corporation,	
18	Defendants.	
19		
20	Plaintiff, the People of the State of California (“Plaintiff” or the “People”), by and through	
21	Rob Bonta, Attorney General of the State of California, bring this action against Illuminate	
22	Education, Inc. (“Illuminate” or “Defendant”) for violations of California’s consumer and privacy	
23	laws. The People allege the following facts based on information and belief:	



ROB BONTA
Attorney General

Translate Website | Traducir Sitio Web

HOMEABOUTMEDIA CAREERSREGULATIONSRESOURCESPROGRAMSAPPOINTMENTSCONTACT

Attorney General Bonta Joins States in Securing \$5.1 Million in Settlements from Education Software Company for Failing to Protect Students’ Data

Press Release / Attorney General Bonta Joins States in Securing \$5.1 Million...



Thursday, November 6, 2025

Contact: (916) 210-6000, agpresso@doj.ca.gov

OAKLAND — California Attorney General Rob Bonta, Connecticut Attorney General William Tong, and New York Attorney General Letitia James today announced that they have secured \$5.1 million and injunctive terms from educational technology company Illuminate Education, Inc.

California Cybersecurity Audits

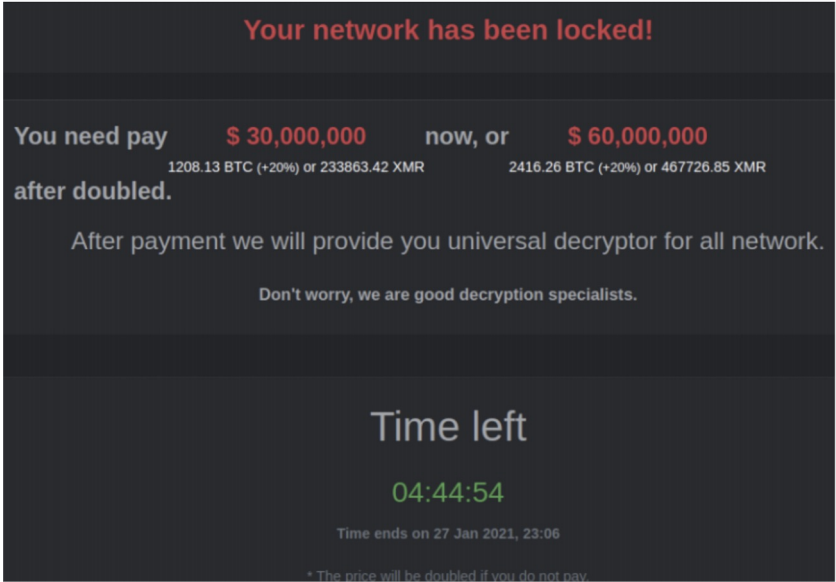
CPPA adopted rule,
July 24, 2025

Requires businesses
"whose processing of
consumers' personal
information presents a
significant risk to
consumers' privacy or
security to ... perform a
cybersecurity audit on
an annual basis."

- Audit must assess, "if applicable," 24 specific controls, including:
 - multifactor authentication — including MFA that is resistant to phishing attacks for employees, service providers, and contractors;
 - strong passwords;
 - encryption of personal information at rest and in transit;
 - account management and access controls;
 - inventory data flows, hardware, and software;
 - secure configuration;
 - patch management;
 - vulnerability scanning;
 - logging;
 - training.

<https://iapp.org/news/a/california-adopts-cybersecurity-audit-rule-outlining-reasonable-cybersecurity>

8. Critical Infrastructure



~~SENSITIVE SECURITY INFORMATION~~

U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

<u>NUMBER</u>	Security Directive Pipeline-2021-02
<u>SUBJECT</u>	Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing
<u>EFFECTIVE DATE</u>	July 26, 2021
<u>EXPIRATION DATE</u>	July 26, 2022
<u>CANCELS AND SUPERSEDES</u>	Not Applicable
<u>APPLICABILITY</u>	Owners and Operators of a hazardous liquid and natural gas pipeline or a liquefied natural gas facility notified by TSA that their pipeline system or facility is critical ¹
<u>AUTHORITY</u>	49 U.S.C. 114(d), (f), (l) and (m)
<u>LOCATION</u>	

Revised and reissued:
May 1, 2025

2023: A Major Change in U.S. Policy

STRATEGIC OBJECTIVE 1.1: ESTABLISH CYBERSECURITY REQUIREMENTS TO SUPPORT NATIONAL SECURITY AND PUBLIC SAFETY

The American people must have confidence in the critical services underpinning their lives and the nation's economy. While voluntary approaches to critical infrastructure cybersecurity have produced meaningful improvements, the lack of mandatory requirements has resulted in inadequate and inconsistent outcomes. Today's marketplace insufficiently rewards—and often disadvantages—the owners and operators of critical infrastructure who invest in proactive measures to prevent or mitigate the effects of cyber incidents.

Regulation can level the playing field, enabling healthy competition without sacrificing cybersecurity or operational resilience. Our strategic environment requires modern and nimble regulatory frameworks for cybersecurity tailored for each sector's risk profile, harmonized to reduce duplication, complementary to public-private collaboration, and cognizant of the cost of implementation. New and updated cybersecurity regulations must be calibrated to meet the needs of national security and public safety, in addition to the security and safety of individuals, regulated entities, and their employees, customers, operations, and data.

Sector-by-Sector, Existing Authorities

“... an owner or operator of a vessel or facility [that the Secretary believes may be involved in a transportation security incident] shall prepare and submit to the Secretary a **security plan** for the vessel or facility ... [which shall] include provisions for ... (iv) **communications systems**; (v) detecting, responding to, and recovering from **cybersecurity risks** that may cause transportation security incidents. Maritime Transportation Security Act - 46 U.S.C. § 70103:

Feb. 2024:

- Maritime Security Directive 105–4, Cyber Risk Management Actions for Ship-to-Shore Cranes Manufactured by People's Republic of China Companies
- Coast Guard - Proposed rule: Cybersecurity in the Marine Transportation System



8. Trend Slowed, Has Now Ended

- Issued under the federal Safe Drinking Water Act, 42 U.S. Code § 300g–2, which gives states primary enforcement responsibility for federal drinking water standards if states have in place adequate procedures for the enforcement of State water quality regulations, including conducting such monitoring and making such inspections as the Administrator may require by regulation.
- Stayed: Missouri v. EPA (8th Cir. July 12, 2023)
- Rescinded: October 2023



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF WATER

March 3, 2023

MEMORANDUM

SUBJECT: Addressing PWS Cybersecurity in Sanitary Surveys or an Alternate Process

FROM: Radhika Fox
Assistant Administrator

A handwritten signature in black ink, appearing to be "R. Fox", is written over the name and title of the sender.

TO: State Drinking Water Administrators
Water Division Directors, Regions I-X

Cyber-attacks against critical infrastructure facilities, including public water systems (PWSs), are increasing.^{1,2} Past incidents have shown that these attacks have the potential to disable or contaminate the delivery of drinking water to consumers and other essential facilities like hospitals.^{3,4,5,6} While some

EXCLUSIVE NATIONAL SECURITY

T-Mobile Hacked in Massive Chinese Breach of Telecom Networks

Carrier joins growing list of known victims, including AT&T and Verizon, of the major Chinese spying operation

By [Sarah Krouse](#) [Follow](#) and [Dustin Volz](#) [Follow](#)

Updated Nov. 15, 2024 7:23 pm ET

FCC Issues Cybersecurity Proposal and Ruling

Full Title: Protecting The Nations Communications Systems From Cybersecurity Threats

Document Type: Notice of Proposed Rulemaking

Bureau(s): Public Safety and Homeland Security

Description:

FCC issues Notice of Proposed Rulemaking and Declaratory Ruling to protect communications systems from cybersecurity threats.

DA/FCC #: FCC-25-9

Docket No: 22-329

Related Document(s):

News Release - [FCC to Require Carriers to Secure Networks](#)

Document Dates

Released On: Jan 16, 2025

Effective Date: Jan 16, 2025

Adopted Date: Jan 15, 2025

Issued On: Jan 16, 2025

Contact: Haille Laws

Tags:

[Cybersecurity](#) - [Public Safety](#)

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of

Protecting the Nation’s Communications Systems
from Cybersecurity Threats

)
)
)
)
)

PS Docket No. 22-329

For consideration
at FCC’s Nov. 20,
2025, meeting

ORDER ON RECONSIDERATION*

Adopted: []

Released: []

By the Commission:

TABLE OF CONTENTS

Heading	Paragraph #
I. INTRODUCTION.....	1
II. BACKGROUND.....	5
A. Recent Commission Action to Protect the Nation’s Communications Systems.....	7
B. Other Communications Sector Cybersecurity Measures	10
C. The Communications Assistance for Law Enforcement Act (CALEA).....	12
D. January 2025 Declaratory Ruling and Notice of Proposed Rulemaking	15
III. DISCUSSION	23
A. Adoption of the Declaratory Ruling Was Unlawful and Unnecessary	23
1. The Declaratory Ruling misinterpreted CALEA.....	24
2. The Declaratory Ruling is ineffective at promoting cybersecurity	29
B. The NPRM Is Unnecessary.....	35
IV. ORDERING CLAUSE.....	36

Thomas M. Johnson, Jr.
202.719.4550
tmjohnson@wiley.law



Wiley Rein LLP
2050 M St NW
Washington, DC 20036
Tel: 202.719.7000

wiley.law

October 16, 2025

VIA ECFS

Marlene H. Dortch, Secretary
Federal Communications Commission
45 L Street N.E.
Washington, D.C. 20554

<https://business.cch.com/CybersecurityPrivacy/tradeassociation/fcc/calealetter.pdf>

Re: *Protecting the Nation's Communications Systems from Cybersecurity Threats*, PS Docket No. 22-329

Dear Ms. Dortch:

CTIA – The Wireless Association (“CTIA”), NCTA – The Internet & Television Association (“NCTA”), and USTelecom – The Broadband Association (“USTelecom”) (collectively, the “Associations”), respectfully file this letter to supplement their pending Petition for Reconsideration (“Petition”) and subsequent *ex parte* filings in the above-captioned proceeding.¹ That Petition urged the Federal Communications Commission (“FCC” or “Commission”) to rescind a January 2025 Declaratory Ruling that interprets the Communications Assistance for Law Enforcement Act (“CALEA”) to require that providers “ensure” their entire networks are

"information sharing" - 21 times

"collaborative" or "collaboration" or "collaborating" - 36 times

"partnership" between industry - 17 times

"Providers take these actions **voluntarily**, and these actions taken on their own volition **do not waive, limit, or otherwise affect providers' legal rights. Nor** do these actions represent **any concession as to the scope of regulatory** or statutory jurisdiction by any government entity."

Telecom Measures Aimed at China

- FCC revocation of authorizations to operate – China Mobile, China Telecoms (America), Pacific Networks, China Unicom (Americas)
- Rip and replace China-made switches (Huawei and ZTE)
- Covered equipment list <https://www.fcc.gov/supplychain/coveredlist>
- CFIUS – July 2025 - Suirui's acquisition of Jupiter - completed in 2020
- “Bad labs” - FCC has withdrawn or denied recognition for 15 equipment test labs owned or controlled by the Chinese government

<https://cybersecuritylawfundamentals.com/chapter-16>



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

[Topics](#) ▾ [Spotlight](#) [Resources & Tools](#) ▾ [News & Events](#) ▾ [Careers](#) ▾ [About](#) ▾

[Home](#) / [News & Events](#) / [Cybersecurity Advisories](#) / [Cybersecurity Advisory](#) / Countering Chinese State-Sponsored Actors Compromise ...

CYBERSECURITY ADVISORY

Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System

Last Revised: September 03, 2025

Alert Code: AA25-239A



EAST BAY

- [CVE-2024-21887](#) ⓘ - Ivanti Connect Secure and Ivanti Policy Secure web-component command injection vulnerability, commonly chained after CVE-2023-46805 (authentication bypass)
- [CVE-2024-3400](#) ⓘ - Palo Alto Networks PAN-OS GlobalProtect arbitrary file creation leading to OS command injection. The CVE allows for unauthenticated remote code execution (RCE) on firewalls when GlobalProtect is enabled on specific versions/configurations.
- [CVE-2023-20273](#) ⓘ - Cisco Internetworking Operating System (IOS) XE software web management user interface post-authentication command injection/privilege escalation (commonly chained with CVE-2023-20198 for initial access to achieve code execution as root) [[T1068](#) ⓘ]
- [CVE-2023-20198](#) ⓘ - Cisco IOS XE web user interface authentication bypass vulnerability
 - While exploiting CVE-2023-20198, the APT actors used the Web Services Management Agent (WSMA) endpoints `/webui_wsma_Http` or `/webui_wsma_Https` to bypass authentication and create unauthorized administrative accounts. In some cases, the APT actors obfuscated requests by “double encoding” portions of the path, e.g., `/%2577eb%2575i_%2577sma_Http` or `/%2577eb%2575i_%2577sma_Https` [[T1027.010](#) ⓘ]. Observed requests varied in case, so hunting and detection should be case-insensitive and tolerant of over-encoding.
 - After patching this CVE, WSMA endpoints requests are internally proxied, and the system adds a `Proxy-Uri-Source HTTP` header as part of the remediation logic. The presence of `Proxy-Uri-Source` header in traffic to `/webui_wsma_*` indicates a patched device handling the request, not exploitation. This can help distinguish between vulnerable and remediated systems when analyzing logs or captures.
- [CVE-2018-0171](#) ⓘ - Cisco IOS and IOS XE smart install remote code execution vulnerability

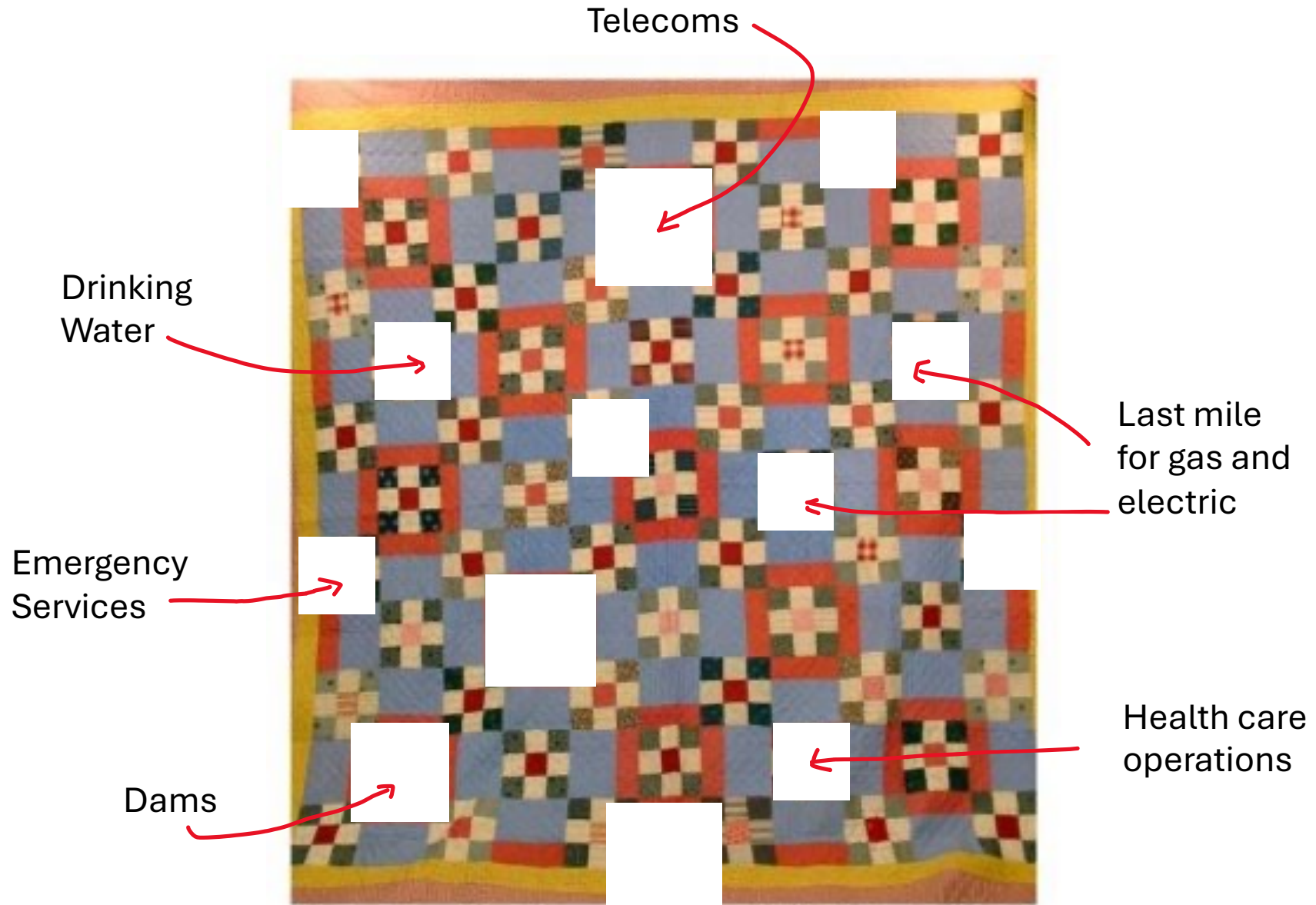
Submarine cable security (Aug. 2025)

Submarine cable licenses must certify that

- they have created and will implement and update a cybersecurity and physical security **risk management plan that:**
- describes how the applicant will take **reasonable measures** to ensure the confidentiality, integrity, and availability of its systems and services, and
- **identifies the cybersecurity risks** the applicant faces, the controls it uses or plans to use to mitigate those risks, and how the applicant will **ensure that these controls** are applied effectively.

<https://docs.fcc.gov/public/attachments/FCC-25-49A1.pdf>

Critical Infrastructure Regulatory Standards



9. AI



FEDERAL REGISTER

The Daily Journal of the United States Government



PD Presidential Document

Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

A Presidential Document by the Executive Office of the President on 11/01/2023



Mentioned “security” –
126 times; “cybersecurity”
– 11 times.

PDF

Document Details

Executive Order Details

Table of Contents

PUBLISHED DOCUMENT: 2023-24283 (88 FR 75191)

Executive Order 14110 of October 30, 2023

Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1 . Purpose. Artificial intelligence (AI) holds extraordinary potential for both promise and peril.

Revoked: Jan. 20, 2025.

9. AI

[Home](#) [Sections](#) [Browse](#) [Search](#) [Reader Aids](#) [My FR](#)



FEDERAL REGISTER

The Daily Journal of the United States Government



PD Presidential Document

Removing Barriers to American Leadership in Artificial Intelligence

A Presidential Document by the Executive Office of the President on 01/31/2025

[PDF](#)
[Document Details](#)
[Executive Order Details](#)
[Table of Contents](#)
[Public](#)

PUBLISHED DOCUMENT: 2025-02172 (90 FR 8741)

[Executive Order 14179](#) of January 23, 2025

Removing Barriers to American Leadership in Artificial Intelligence

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered:

Section 1 . Purpose. The United States has long been at the forefront of artificial intelligence (AI) innovation, driven by the strength of our free markets, world-class research institutions, and entrepreneurial spirit. To maintain this leadership, we must develop AI systems that are free from ideological bias or engineered social agendas. With the right Government policies, we can solidify our

No mention of
“cybersecurity;” mentions
“security” twice, in the
phrase “national security.”

10. Most Impactful Regulator of American Businesses?



EmDee, CC BY-SA 4.0, via Wikimedia Commons

10. EU Cybersecurity Regulation

- GDPR – data security measures for personal data and data breach notice; gives the DPAs enforcement authority over the security of personal data.
- NIS2 - network and information systems - covers not only providers of electronic communications networks but also a wide range of critical infrastructure providers (electricity, transportation, banking, health care, drinking water, etc). Sets detailed requirements.
- Digital Operational Resilience Act (DORA) – financial services sector.
- Cyber Resilience Act (CRA) - mandates cybersecurity standards for connected hardware and software products sold in the EU.
- Radio Equipment Directive (RED) – wireless devices
- EU Cybersecurity Act - authorizes the European Union Agency for Cybersecurity (ENISA) and created a framework for a voluntary cybersecurity certifications
- IAPP Resources <https://iapp.org/resources/article/european-strategy-for-data-overview-of-new-regulations/>

Where to go?

The federal government should use its procurement power

- Software
- Utilities purchased by DoW





Thank you. Questions?

James (“Jim”) Dempsey

jdempsey@berkeley.edu