Sponsored by:

COALFIRE FEDERAL

NDIA

CMMC: Update

Current As Of: May 2023

Sponsored by:

CALFIRE FEDERAL

NDIA

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Secure your Networks. Now**
  - **DFARS 7012 / NIST 800-171 impose current Contractual Obligations**
- **Self-Assessment did not incentivize companies to comply**
  - **Does not negate obligation to meet the Standards in the Cybersecurity Framework**

Sponsored by:

COALFIRE FEDERAL

TODAY'S SPEAKER

PARTNER, HINCKLEY ALLEN

Sponsored by:

COALFIRE FEDERAL

NDIA

Webinar: The Harsh Consequences of Cybersecurity Noncompliance

B. Stephanie Siegmann

Hinckley Allen & Snyder LLP

HINCKLEY ALLEN

Since 2021,Cyber-Attacks Have Been Increasing

- Malware-based attacks
- Phishing
- Spoofing
- Zero day exploits
- Denial-of-Service Attacks
- Supply Chain Attacks
- Insider Threats
- Vast majority of companies have experienced some form of a cyberattack over last 12 months

Sponsored by:

Executive Order 14028 – Improving Nation's Cybersecurity

- Issued in response to cyber attacks and perceived inability for government to respond because it lacked information from private sector
- Called for "bold" action
  - Remove any barriers to sharing threat information
  - Modernize federal government cybersecurity
  - Enhance software supply chain security
  - Establish DHS Cyber Safety Review Board
  - Standardize government's response to cybersecurity incidents
  - Improve detection of cybersecurity vulnerabilities and incidents on federal government networks
  - Improve government's investigative and remediation capabilities
- Required each federal agency to perform a comprehensive cyber review

Federal Cybersecurity Requirements

- Increasing minimum cybersecurity requirements being imposed by Executive Order and Regulations
- Increasing cybersecurity reporting requirements
  - Cyber Incident Reporting for Critical Infrastructure Act of 2022
  - SEC new requirements
  - Grant recipients – CHIPS Act
- Defense Federal Acquisition Regulations Supplement § 252.204-7012
  - Implement NIST SP 800-171
    - 14 Families of Controls
    - 110 Requirements
    - "rapidly report" cyber incidents within 72 hours of discovery
    - Cyber Incident Response Plan

October 6, 2021

DAG Lisa Monaco Announces DOJ's Civil Cyber-Fraud Initiative

Sponsored by:

COALFIRE FEDERAL

HINCKLEY ALLEN

Purpose of Initiative

- Change behaviors of the private sector
  - "For too long companies have chosen silence" rather than reporting breaches.
- Will use False Claims Act to pursue government contractors and grant recipients that "fail to follow cybersecurity standards."
- Government contractors will be held accountable for putting U.S. information and systems at risk.
- Three common cybersecurity failures to be targeted:
  - 1 – Knowingly providing deficient cybersecurity products or services
  - 2 – Knowingly misrepresenting cybersecurity practices or protocols
  - 3 – Knowingly violating obligations to monitor and report cybersecurity incidents and breaches

False Claims Act

- DOJ's Primary Civil Enforcement Tool
- FCA is extremely broad and imposes liability on anyone who:
  - "knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval;" or
  - "knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim"
  - Examples:
    - In bid, company says it is abiding by industry cybersecurity standards (*i.e.*, NIST SP 800-171)
    - During bidding process, contractor enters a score into the Supplier Performance Risk System (SPRS) that is inaccurate or unsubstantiated
    - In contract, company agrees to comply with cybersecurity standards
    - By filing claim/seeking payment, company represents it has complied with material contract provisions, including cybersecurity provisions

Whistleblower Provision

- Creates a strong financial incentive for **company insiders** to uncover and report fraud
- $2.2B in 2022 and 351 settlements 900 new whistleblower matters were opened in FY2020.
- Whistleblower recovery 15-30% of funds recovered.
- Recoveries in cyber-fraud cases could be millions of dollars.
- Treble damages = 3x the sum of each invoice/claim paid under government contracts + fines & attorney's fees

Sponsored by:

COALFIRE FEDERAL

HINCKLEY ALLEN

The First Settlement Under DOJ's Civil Cyber-Fraud Initiative Announced in March 2022

- Comprehensive Health Services LLC agreed to pay $930,000 to resolve FCA allegations.
- CHS, a provider of global medical services, had contracted to provide medical support services at government-run facilities in Iraq and Afghanistan.
  - CHS failed to maintain patients' medical records on secure network
  - CHS failed to take adequate cybersecurity steps to protect patient information
- Takeaways:
  - DOJ will aggressively pursue government contractors that fail to follow cybersecurity standards.
  - This case particularly egregious because it put confidential medical records at risk.
  - Company ignored concerns of staff about privacy of protected medical information and two whistleblowers then initiated this case.

CHS Wasn't the First Cybersecurity FCA Settlement

The New York Times | https://www.nytimes.com/2019/07/31/technology/cisco-tech-flaw-sales.html

Cisco to Pay $8.6 Million to Settle Government Claims of Flawed Tech

By Katie Benner and Kate Conger

July 31, 2019

WASHINGTON — Cisco Systems agreed on Wednesday to pay $8.6 million to settle claims that it sold video surveillance technology that it knew had a significant security flaw to federal, state and local government agencies.

Cisco will pay civil damages in connection with software that it sold to various government agencies, including Homeland Security, the Secret Service, the Army, the Navy, the Marines, the Air Force and the Federal Emergency Management Agency, according to a government complaint unsealed on Wednesday.

Eighteen states, including New York and California, and the District of Columbia joined the Justice Department in the claim against Cisco, one of the world's largest sellers of software and equipment to businesses and governments; 15 states and the District of Columbia recovered under the settlement. The case was filed in the Federal District Court for the Western District of New York under the False Claims Act, which addresses fraud and misconduct in federal government contracts.

The government said the video surveillance software it bought from Cisco was "of no value" because it did not "meet its primary purpose: enhancing the security of the agencies that purchase it." In many cases, the Cisco software actually reduced the protection provided by other security systems, the complaint said.

Cisco said in a statement that it was pleased to resolve the dispute. "There was no allegation or evidence that any unauthorized access to customers' video occurred as a result of the architecture," Robyn Blum, a Cisco spokeswoman, said in a statement.

The software vulnerability was identified in 2008 by a whistle-blower, James Glenn, who was working as a Cisco subcontractor in Denmark when he discovered that he could hack into the video software and take over the surveillance system without being detected, according to his lawyers at Constantine Cannon.

Cybersecurity Noncompliance Could Also Result in State Enforcement Actions

- As the Cisco settlement illustrates, State Attorneys Generals could also institute actions against companies with weak cybersecurity.
- Cisco could have avoided significant liability if it had taken action after being alerted to the security flaws.
- **BUT** Cisco failed to report or remedy this security flaw for several years.
  - This is a recurring problem that results in significant liability!

CARNIVAL CORPORATION JUNE 2022 SETTLEMENT

- Carnival agreed to pay more than $6 million to settle lawsuits by 46 states. They waited 10 months to disclose a cyberattack that occurred in May 2019.
  - Largest fine came from New York State Department of Financial Services (DFS):

    Uncovered evidence that Carnival had been the subject of four cybersecurity incidents between 2019 and 2021, including two ransomware attacks. Cybersecurity incidents involved the unauthorized access of the companies' information systems, leading to the exposure of customers' sensitive, personal data. Carnival violated the DFS Cybersecurity Regulation by failing to implement Multi-Factor Authentication, failing to promptly report the first cybersecurity event to DFS as required by state regulations, and failing to conduct adequate cybersecurity training for their personnel.

Aerojet's Recent $9 Million Settlement

- In 2015, Brian Marcus filed a FCA case against his former employer, Aerojet Rocketdyne.
- Alleged Aerojet had lied about cybersecurity compliance to obtain DOD and NASA contracts.
- In 2018, case unsealed and publicly filed but DOJ chose not to intervene.
- Two weeks after Civil Cyber-Fraud Initiative announced, DOJ filed Statement of Interest.
- With DOJ's help, whistleblower defeated Aerojet's Summary Judgment motion.

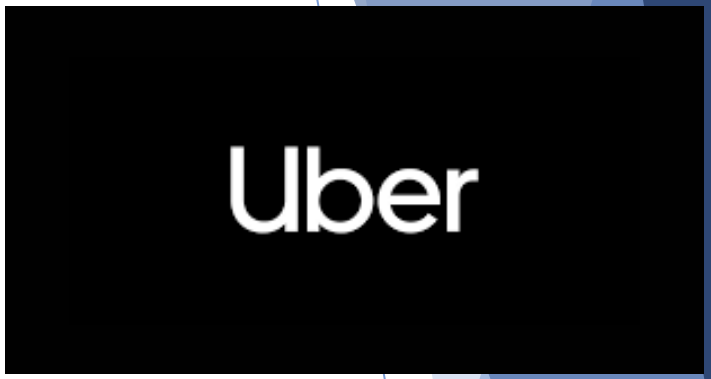
Significance of Aerojet Case and Settlement

- First-of-its-kind cybersecurity non-compliance FCA case to get to trial
  - Overcame Motions to Dismiss and for Summary Judgement
    - Court ruled that issues of materiality and damages would go to the jury
- Less than 24 hours after jury impaneled, Aerojet agreed to pay $9 million and undisclosed amounts for attorney fees and another claim to settle
  - Whistleblower (Marcus) received $2.61 million = 29% of recovery
  - DOJ's Press release highlighted the critical role whistleblowers like Markus "with insider information and technical expertise" can serve "in identifying knowing cybersecurity failures and misconduct."
- DAG Monaco referenced *Aerojet* settlement in a speech on July 19, 2022:
  - Cyber Civil-Fraud Initiative's work recently resulted in a defense contractor agreeing to pay $9 million to resolve allegations that it misrepresented its compliance with cybersecurity requirements in NASA and Department of Defense contracts – this is the second such settlement under this initiative. Holding contractors accountable for their cybersecurity promises will enhance resiliency against cyber intrusions across the government, the public sector and key industries.

4/23 FCA Settlement - Cybersecurity Failures on Florida's Medicaid Enrollment Website

- Jelly Bean Communications Design and its manager agreed to pay $293,771 to resolve FCA allegations that it failed to properly secure personal information on federally funded Florida children's health insurance website that it created, hosted, and maintained.
  - Website used by parents of children aged 5-17 to apply for child health insurance
- Jelly Bean contractually required to provide a fully-functional hosting environment that complied with HIPAA.
- Contrary to its representations, Jelly Bean did not provide a secure hosting for personal information and failed to properly maintain, patch, and update its software systems and its related websites, leaving the site and data Jelly Bean collected from applicants vulnerable to cyberattacks.
- In Dec. 2020, more than 500,000 health insurance applications had been hacked
  - Involved DOBs, social security numbers, financial information, and insurance information.
- The investigation revealed that Jelly Bean had NOT updated or patched some of the software used on the website SINCE 2013

Example of Criminal Liability for Concealing Data Breach - *United States v. Joseph Sullivan*



- Joe Sullivan was Uber's Chief Security Officer
  - Former federal cybercrimes prosecutor
  - Worked at Facebook and eBay as cybersecurity expert
  - When trial started was on leave from job as CSO at Cloudfare
- Uber hacked in 2014
- While FTC conducting investigation and during settlement negotiations, Uber hacked again in 2016
- Paid hackers $100,000 in bitcoin through a bug bounty program
  - Hackers signed a non-disclosure agreement with Uber
- Data of 57 million Uber passengers and drivers compromised
  - Names and driver's license numbers of 600,000 drivers
  - Names, emails, and mobile phone numbers of 57 million Uber users
- 2016 hack kept secret for over a year
- Sullivan charged with five felonies

UNITED STATES OF AMERICA, Plaintiff, v. JOSEPH SULLIVAN, Defendant.	CASE NO. 3:20-cr-00337 WHO VIOLATIONS: 18 U.S.C. § 1505 – Obstructing Proceedings of the Federal Trade Commission; 18 U.S.C. § 4 – Misprision of a Felony; 18 U.S.C. § 1343 – Wire Fraud SAN FRANCISCO VENUE

SUPERSEDING INDICTMENT

The Grand Jury charges:

Introductory Allegations

At all times relevant to this Indictment:

1. The United States Federal Trade Commission ("FTC") was an independent agency of the United States. The FTC's Division of Privacy and Identity Protection oversaw and investigated, among other things, issues related to consumer privacy, identity theft, and information security.

2. In or about February 2015, Uber Technologies, Inc. ("Uber") informed the FTC that it had learned of a data breach it had suffered in September 2014 (hereinafter the "2014 Data Breach"). In or about March 2015, the FTC informed Uber that the FTC was evaluating Uber's data security program

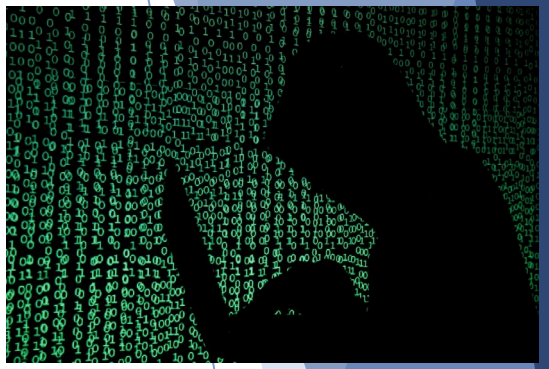
Two Hackers Given Leniency and One Testified At Sullivan's Trial

- October 2019 – Vasile Mereacre, a Canadian national, and Brandon Glover pleaded guilty to hacking/extortion conspiracy involving plot to extract cyber ransoms from Uber and Lynda.com/LinkedIn
- Mereacre testified at Sullivan's trial pursuant to plea agreement requiring him to cooperate in criminal investigation of Uber's data breach
  - Hackers scolded Uber for their carelessness with passwords, failure to use two-factor authentication, and leaving a AWS key on a public site.
  - Mereacre sent an email stating: "Uber should have mandatory 2 step authentication on GitHub. ALL INTERNAL data was able to downloaded and seen. Your security steps are very poorly done, the lack of negligence [sic] and care here is zero to none. Your employees are careless and don't care about security."
  - Uber paid the hackers $100,000 via bitcoin and required them to sign non-disclosure agreements

GUILTY

- After 3 week trial and 2 ½ days of deliberations, jury convicted Sullivan of obstruction of justice and misprision of felony
- Going forward, DOJ intends to prosecute individuals that hide or conceal data breaches from public
  - DOJ: We will not tolerate concealment of important information from the public by corporate executives more interested in protecting their reputation and that of their employers than in protecting users. Where such conduct violates the federal law, it will be prosecuted.
  - FBI: Companies storing their customers' data have a responsibility to protect that data and do the right thing when breaches occur. The FBI and our government partners will not allow rogue technology company executives to put American consumers' personal information at risk for their own gain.
- What does this mean?
- DOJ sought a sentence of 15 months' imprisonment
- Uber paid $148 Million to settle case with DOJ – Non-Prosecution Agreement

How to avoid becoming a target of DOJ's Civil Cyber-Fraud Initiative



- Implement a strong cybersecurity program.
  - Ensure it incorporates criteria in NIST SP 800-171.
  - Companies should review and regularly update cybersecurity controls.
  - Provide extensive training about cyber controls.
    - It is essential that your employees (and potential whistleblowers) understand that you take cybersecurity seriously.
    - Respond/investigate any complaints regarding cybersecurity.
- A cyber incident by itself ordinarily is not sufficient to create FCA liability.
- FCA liability arises where companies knowingly fail to comply with **material** statutory/regulatory obligations or **material** requirements of government contract.
- Thus, if your company has a cyber-breach and knowingly fails to report it to the government (since DFARS Section 7012, contractors have been required to report these events), then your company could face FCA liability.

Increased Threat of Liability for Weak Cybersecurity

- In addition to FCA civil liability, there is potential for criminal liability in future
  - SEC disclosure requirements for cybersecurity incidents and protocols (must be made within 4 business days)
  - New obligations under Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) are coming
  - When federal government investigates civil complaint, will it find other violations?
    - Export violations (ITAR, EAR, deemed exports – **NOTE:** DoC/BIS's increased admin enforcement penalties)
    - CFIUS issues
    - Sanctions violations or other financial crimes
    - False statements or obstruction/witness tampering

Lax Cybersecurity Resulting in Data Breach Creates Other Liability Risks

- Federal Trade Commission Actions
- Class Actions
- State Attorney General Enforcement Actions

B. STEPHANIE SIEGMANN

Hinckley Allen & Snyder LLP

www.hinckleyallen.com

ssiegmann@hinckleyallen.com

(617) 378-4181 (o)

(617) 320-5045 (c)