Navigating the Civil Cyber-Fraud Initiative and Cybersecurity Compliance

A Guide for Government Contractors

November 30, 2021

Today's Presenters

Brian E. Finch
Partner
Public Policy
+1 202.663.8062
brian.finch@pillsburylaw.com

Meghan D. Doherty
Counsel
Government Contracts & Disputes
+1 703.770.7519
meghan.doherty@pillsburylaw.com

Tamara D. Bruno
Partner
Insurance Recovery & Advisory
+1 713.276.7608
tamara.bruno@pillsburylaw.com

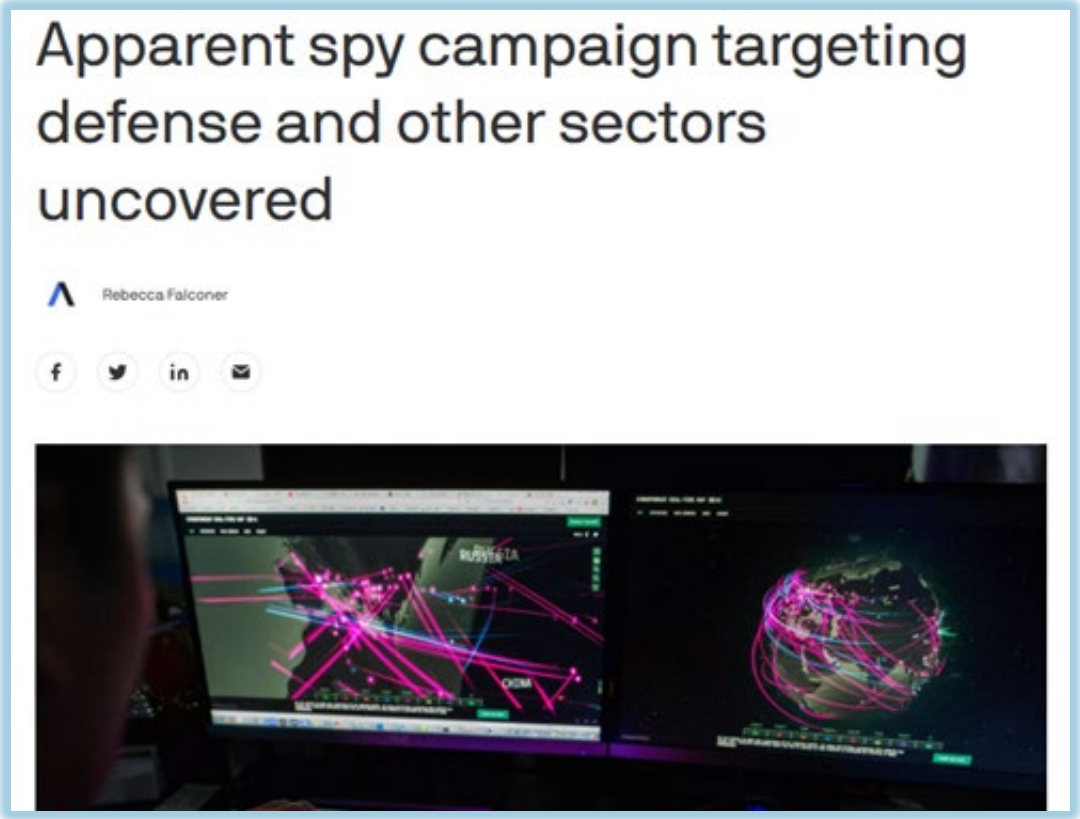
pillsbury

DOJ Announces Civil Cyber-Fraud Initiative

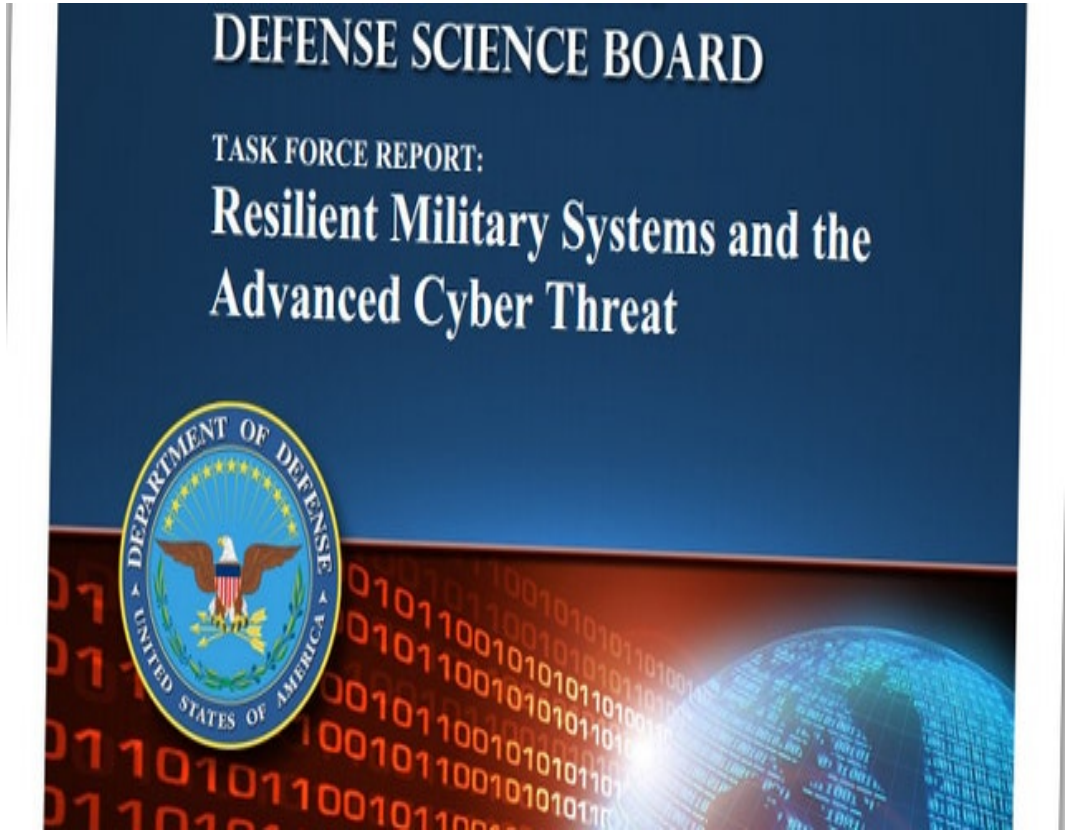
- **“For too long, companies have chosen silence under the mistaken belief that it is less risky to hide a breach than to bring it forward and to report it.”**
  - Deputy Attorney General Lisa Monaco, announcing in October the Justice Department’s Civil Cyber-Fraud Initiative.
- Monaco added that the Initiative is intended to “ensure that taxpayer dollars are used appropriately and guard the public fisc and public trust.”

pillsbury

Why Would Justice Announce This?

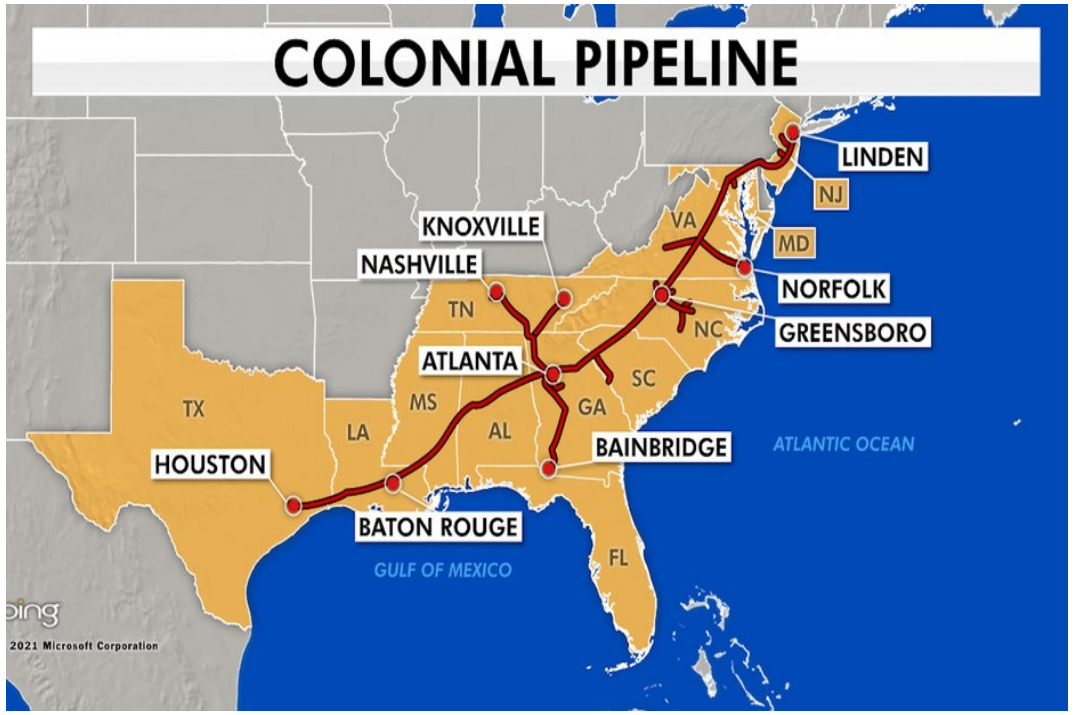


There Have Been Years Of Hacking of Gov't Contractors



pillsbury

It’s Not Just “Defense” Contractors Either



pillsbury

Even Worse, Stories Continue About “Hidden” Hacks

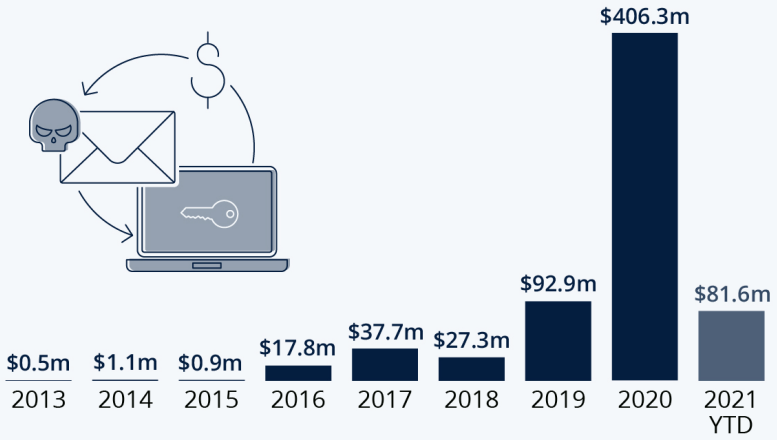
MARKETS | FINANCIAL REGULATION

Many Company Hacks Go Undisclosed to SEC Despite Regulator Efforts

SEC Commissioner Robert Jackson says a clear rule about when to report a cyberattack would be helpful to the market

Crypto Ransom Payments Skyrocketed in 2020

Total value of cryptocurrency received by known ransomware addresses*



* currencies included: Bitcoin Cash, Bitcoin, Ethereum, Tether; as of May 10, 2021
Source: chainalysis.com

statista

pillsbury

Growing Pressure To Make Hacks Public

- Looming bills in Congress would require disclosure of data breaches.
- For the first time, also seeing pressure for companies to report ransomware payments as well.
- This is on top of requirements for defense contractors and certain regulated entities to disclose breaches.
- The SEC has weighed in as well, sending investigation letters to companies following Solar Winds and other hacks.
- US agencies like TSA stepping up pressure on pipelines, aviation, rail and other sectors.

pillsbury

Civil Cyber-Fraud Initiative

- Combine the DOJ's expertise in civil fraud enforcement, government procurement and cybersecurity to combat new and emerging cyber threats to the security of sensitive information and critical systems.
- Utilize the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients.
- The initiative will hold accountable entities or individuals that put U.S. information or systems at risk by knowingly **providing deficient cybersecurity products or services**, knowingly **misrepresenting their cybersecurity practices or protocols**, or knowingly **violating obligations to monitor and report cybersecurity incidents and breaches**.

pillsbury

The False Claims Act

- 31 U.S.C. §§ 3729-3733
- Federal Government's primary tool to combat fraud
- Imposes penalties and damages on parties who **knowingly** submit false or fraudulent claims for payment to the Federal Government
  - Directly submitting a claim and causing submission of a false claim
  - Express or implied false certification
- Knowing/knowingly:
  - Actual knowledge
  - Deliberate ignorance
  - Reckless disregard

pillsbury

False Claims Act Damages

- FCA violators are liable for a penalty per false claim. Penalties are adjusted for inflation and currently range from $11,803 and $23,607.
- FCA violators are liable for **treble** damages.
- Court may assess **double** damages if:
  - furnished Government with all information known about the violation within 30 days after the date on which the defendant first obtained the information
  - fully cooperated with any Government investigation of such violation
  - at the time defendant furnished the Government with the information about the violation, no criminal prosecution, civil action, or administrative action had commenced and the defendant did not have actual knowledge of the existence of an investigation
- Cost of bringing the civil action.

pillsbury

Qui Tam Relators

- The FCA allows for *qui tam* relators, or whistleblowers, to initiate civil cases on behalf of the Government and recover a portion of the damages
  - Any person or entity with knowledge may bring such a case– there is no requirement that the relator be personally harmed by the violation
  - In the government contracts context, *qui tam* relators are often employees or former employees of the contractor
  - Relators may be covered by whistleblower protections, so contractors must be careful not to retaliate against such individuals

pillsbury

Examples of FCA Initiatives

- Procurement Collusion Strike Force
  - Multi-agency initiative announced in November 2019 with the goal of detecting, investigating, prosecuting, and deterring antitrust crimes such as bid-rigging and related fraudulent schemes in government contracting and grants
  - More than 30 active investigations, strike force teams in 22 U.S. Attorney's offices, significant penalties
- Cryptocurrency initiative
- Pandemic Relief

pillsbury

FCA Cybersecurity Case Law

- *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.,* 381 F. Supp. 3d 1240 (E.D. Cal. 2019).
  - May 2019, California district court declined to dismiss a *qui tam* case alleging that a contractor falsely certified its cybersecurity compliance under DoD and NASA contracts.
- *United States, et. al., ex. rel. James Glenn v. Cisco Systems, Inc.,* Case No. 1:11-cv-00400-RJA, (W.D.N.Y. July 31, 2019).
  - July 2019, DOJ entered into $8 million settlement related to contractor's failure to comply with cybersecurity standards.
- *United States ex rel. Adams v. Dell Computer Corp.,* 15-cv-608 (D.D.C. Oct. 8, 2020).
  - October 2020, D.C. district court dismissed a *qui tam* case alleging that the contractor failed to disclose security vulnerabilities in a product that it sold to the Government. The court found that the failure was not material to the agency's payment for the product because the product was not required to be defect-free.

pillsbury

Relevant Cybersecurity Obligations

- FAR 52.204-21, "Basic Safeguarding of Covered Contractor Information Systems"
  - Requires application of basic safeguarding requirements when processing, storing, or transmitting Federal Contract Information (FCI) in or from covered contractor information systems
  - 15 Controls (15 of the NIST 800-171 controls)
  - "Basic cyber hygiene"
- DFARS 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting"
  - Provide "adequate security" for covered defense information which "at a minimum" requires contractors to implement 110 Security controls from NIST SP 800-171
  - Include the clause in subcontracts for which performance will involve covered defense information or operationally critical support
  - Report cyber incidents within 72 hours of discovery
- DFARS 252.204-7019, -7020, -7021

pillsbury

Cybersecurity Maturity Model Certification ("CMMC") 2.0

- A comprehensive framework to protect the defense industrial base from increasingly frequent and complex cyberattacks
- On November 4, 2021 DoD announced major changes to the CMMC program, including:
  - Decreased number of assessment levels from 5 to 3
  - **Self-assessments** at Level 1 and Level 2
    - unless handling "critical national security information"
  - Reduces the total number of practices required and aligns the required practices with standards issued by the National Institute of Standards and Technology (NIST)
  - Allows Plans of Action & Milestones (POA&Ms)
  - Allows for waivers to CMMC requirements under certain, limited circumstances
  - Rulemaking is estimated to be complete in 9-24 months

pillsbury

Insurance for Cyber-Related FCA Claims

- Potentially Responsive Insurance Policy Programs:
  - Directors and Officers (D&O) Liability Insurance
  - Cyber
  - E&O/Professional Liability

pillsbury

D&O Liability Insurance

- Typically no exclusion for cyber-related claims
- Coverage for targeted individuals
- Coverage for public companies likely limited to Securities Claims, but broader coverage typical for private companies

pillsbury

Cyber Insurance

- Policy terms differ significantly
- Not all cyber policies include liability coverage
- Some require an alleged privacy or security breach to trigger liability coverage
- Cyber policies may exclude claims brought “by or on behalf of” government entities

pillsbury

E&O/Professional Liability Insurance

- May include specific exclusions for cyber/FCA claims
- Insuring provisions may be less likely to apply, but dependent on FCA claim allegations and scope of "professional services" covered
  - *See, e.g.*, *Affinity Living Grp. v. Starstone Specialty Ins. Co.*, 959 F.3d 634 (4th Cir. 2020) (holding that FCA action for Medicaid claims where no services were provided "arose" out of the insured's "rendering or failure to render medical professional services" to trigger PL coverage)

pillsbury

Common FCA Claim Coverage Issues

- Coverage for investigations?
- May be addressed by specific policy terms
  - *See, e.g., Guaranteed Rate, Inc. v. ACE Am. Ins. Co.*, 2021 WL 3662269, at *2 (Del. Super. Ct. Aug. 18, 2021) (holding that a False Claims Act CID was "a civil, administrative or regulatory investigation against the Insured" and not excluded by professional services exclusion)
- Investigative demands may qualify as a general "claim"
  - *See, e.g., Conduent State Healthcare, LLC v. AIG Specialty Ins. Co.*, 2019 WL 2612829, at *2 (Del. Super. Ct. June 24, 2019) (holding that a CID from the Texas AG investigating possible Medicaid fraud was a "Claim" as "a written demand for money, services, non-monetary relief or injunctive relief")

pillsbury

Common FCA Claim Coverage Issues

- Insured v. Insured exclusions
  - Generally meant for insurers not to cover infighting, but language is often broader
  - Negotiate limit to claims brought by the insured company
  - Look for whistleblower exception

pillsbury

Common FCA Claim Coverage Issues

- Fraud exclusions
  - Frequently require final adjudication of fraud
  - Insurability of fraud can be dependent on state law
    - *RSUI Indemnity Co. v. Murdock*, 248 A.3d 887 (Del. Mar. 3, 2021) (no state policy against coverage for fraud)
    - Cal. Ins. Code § 533 (prohibiting coverage for "willful" conduct)
  - Negotiate most favorable jurisdiction clause
  - Negotiate severability provision

pillsbury

Common FCA Claim Coverage Issues

- Limitations on covered damages
  - Exclusions for penalties/multiplied damages
    - Negotiate for inclusion or coverage where permitted by the most favorable jurisdiction
  - Insurability of restitution/disgorgement
    - *See, e.g., Astellas US Holdings Inc. v. Starr Indemnity & Liability Co.*, No. 17-cv-08220 (N.D. Ill. Oct. 8, 2021) (holding FCA settlement amount labeled "restitution" was compensatory damages, not disgorgement, and coverage was permitted under Illinois law)

pillsbury

Tips for Maximizing Coverage

- Review D&O and cyber policies with coverage counsel and work with broker to negotiate policy language
  - Note market is currently difficult for both
- Consider coverage implications of settlement terms
  - Characterization of claimed conduct
  - Characterization of damages
  - Allocation of settlement amounts

pillsbury

Questions?

pillsbury