Federal Bar Association

VIRTUAL
QUI TAM CONFERENCE
FEBRUARY 23-25, 2022

The False Claims Act as a Weapon against Cybersecurity Fraud

Colleen Kennedy, Deputy Chief, USAO for the Eastern District of California (Sacramento)

Michael Ronickher, Partner, Constantine Cannon, Washington, D.C.

Jennifer Short, Partner, Blank Rome LLP, Washington, D.C.

Moderator: Renée Brooker, Partner, Tycko & Zavareei LLP, Washington, DC

What is cybersecurity?

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

https://www.cisa.gov/uscert/ncas/tips/ST04-001

What is meant by cybersecurity fraud for purposes of our discussion?

- new and emerging cyber threats to the security of sensitive information and critical systems involving government programs and operations
- government contractors and grant recipients who receive federal funds, when they fail to follow required cybersecurity standards
- need not involve government contracts or grants *expressly for* cybersecurity because all government contractors and grantees must meet certain cybersecurity requirements
- hold accountable entities or individuals that put U.S. information or systems at risk

President Biden's **Executive Order** on Improving the Nation's Cybersecurity

- Issued May 2021
- Response (in part) to software provider SolarWinds hack
- Require government agencies & contractors to bolster their cybersecurity, share info. re: cyber threats
- Create standards for government & contractors
- Create labeling requirements for contractor devices & software sold to government
- Require contractors to report data breaches to the government
- Create a Cybersecurity Safety Review Board (pvt. & gov't) to review breaches in real time.
- https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

DOJ's New Civil Cyber-Fraud Initiative

- Announced October 6, 2021
- False Claims Act as the tool to pursue cybersecurity fraud by government contractors and grant recipients.
- Will hold accountable entities or individuals that put U.S. information or systems at risk by (1) knowingly providing deficient cybersecurity products or services, (2) knowingly misrepresenting their cybersecurity practices or protocols, or (3) knowingly violating obligations to monitor and report cybersecurity incidents and breaches, https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative

Cyber-Fraud Whistleblowers

Issue Spotting in Developing Cases That Would Fall Under The DOJ Cyber-Fraud Initiative

- Do you need an actual breach or just a risk of breach?
- Do you need an expert witness?
- What standards should be applied for contractors under the FCA in a continually developing space?
- Do National Institute of Standards and Technology (NIST) standards apply?
- Are the legal theories any different than the usual procurement fraud case?
- Are there ways to calculate damages that are different than the usual procurement fraud case?

Cases Cited by DOJ Civil Frauds of Cyber Fraud Examples

- Netcracker Technology Corp. and Computer Sciences Corp. Agree to Settle Civil False Claims Act Allegations, https://www.justice.gov/opa/pr/netcracker-technology-corp-and-computer-sciences-corp-agree-settle-civil-false-claims-act
- IBM Agrees to Pay $14.8 Million to Settle False Claims Act Allegations Related to Maryland Health Benefit Exchange, https://www.justice.gov/opa/pr/ibm-agrees-pay-148-million-settle-false-claims-act-allegations-related-maryland-health
- Electronic Health Records Vendor to Pay $57.25 Million to Settle False Claims Act Allegations, https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-5725-million-settle-false-claims-act-allegations
- Kansas Hospital Agrees to Pay $250,000 To Settle False Claims Act Allegations, https://www.justice.gov/usao-ks/pr/kansas-hospital-agrees-pay-250000-settle-false-claims-act-allegations
- Oracle Agrees to Pay U.S. $199.5 Million to Resolve False Claims Act Lawsuit, https://www.justice.gov/opa/pr/oracle-agrees-pay-us-1995-million-resolve-false-claims-act-lawsuit
- VMWare and Carahsoft Agree to Pay $75.5 Million to Settle Claims that they Concealed Commercial Pricing and Overcharged the Government, https://www.justice.gov/opa/pr/vmware-and-carahsoft-agree-pay-755-million-settle-claims-they-concealed-commercial-pricing

What is SolarWinds?

SolarWinds Inc.-American public-traded company, Austin, Texas, develops software for commercial and **government customers** to help manage their networks, systems, and information technology infrastructure.

Early 2020- **Russian government hackers** broke into SolarWinds' systems & implanted malicious code in its "Orion" software, a platform used by tens of thousands of customers to monitor and manage its computer networks.

Like most software providers, SolarWinds periodically sends updates to its customers to fix bugs, improve security, or improve the program's performance. When it did so in March 2020, it unwittingly sent updates of Orion to its customers that included the **malicious code**. This embedded code mimicked the language of the Orion software, allowing the malicious code to "**hide in plain sight**," and gave hackers a doorway into otherwise secured networks, including **government & government contractor networks**.

Cybersecurity Requirements

- National Institute of Standards and Technology – "**NIST Cybersecurity Framework**", NIST 800-171, https://www.nist.gov/cyberframework/framework
- **FAR 52.204-21** Basic Safeguarding of Covered Contractor Information Systems, 48 CFR 52.204-21
- "**DFARS 7012**" - 48 C.F.R. § 3252.204-7012(b)(2)(i)
- Cybersecurity Maturity Model Certification (**CMMC**), https://www.federalregister.gov/documents/2021/11/17/2021-24880/cybersecurity-maturity-model-certification-cmmc-20-updates-and-way-forward
- Other evolving cybersecurity standards

NIST Special Publication 800-171
Revision 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

TABLE 1: SECURITY REQUIREMENT FAMILIES

FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

Safeguarding Covered Defense Information – The Basics

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, is required in all contracts except for contracts solely for the acquisition of COTS items. In addition the Contractor shall include the clause in subcontracts for which performance will involve **covered defense information** or **operationally critical support.**

Covered defense information is used to describe information that requires protection under DFARS Clause 252.204-7012. It is defined as unclassified controlled technical information (CTI) or other information as described in the CUI Registry (http://www.archives.gov/cui/registry/category-list.html), that requires safeguarding/dissemination controls **AND IS EITHER** marked or otherwise identified in the contract and provided to the contractor by DoD in support of performance of the contract; **OR** collected/developed/received/transmitted/used/stored by the contractor in performance of contract.

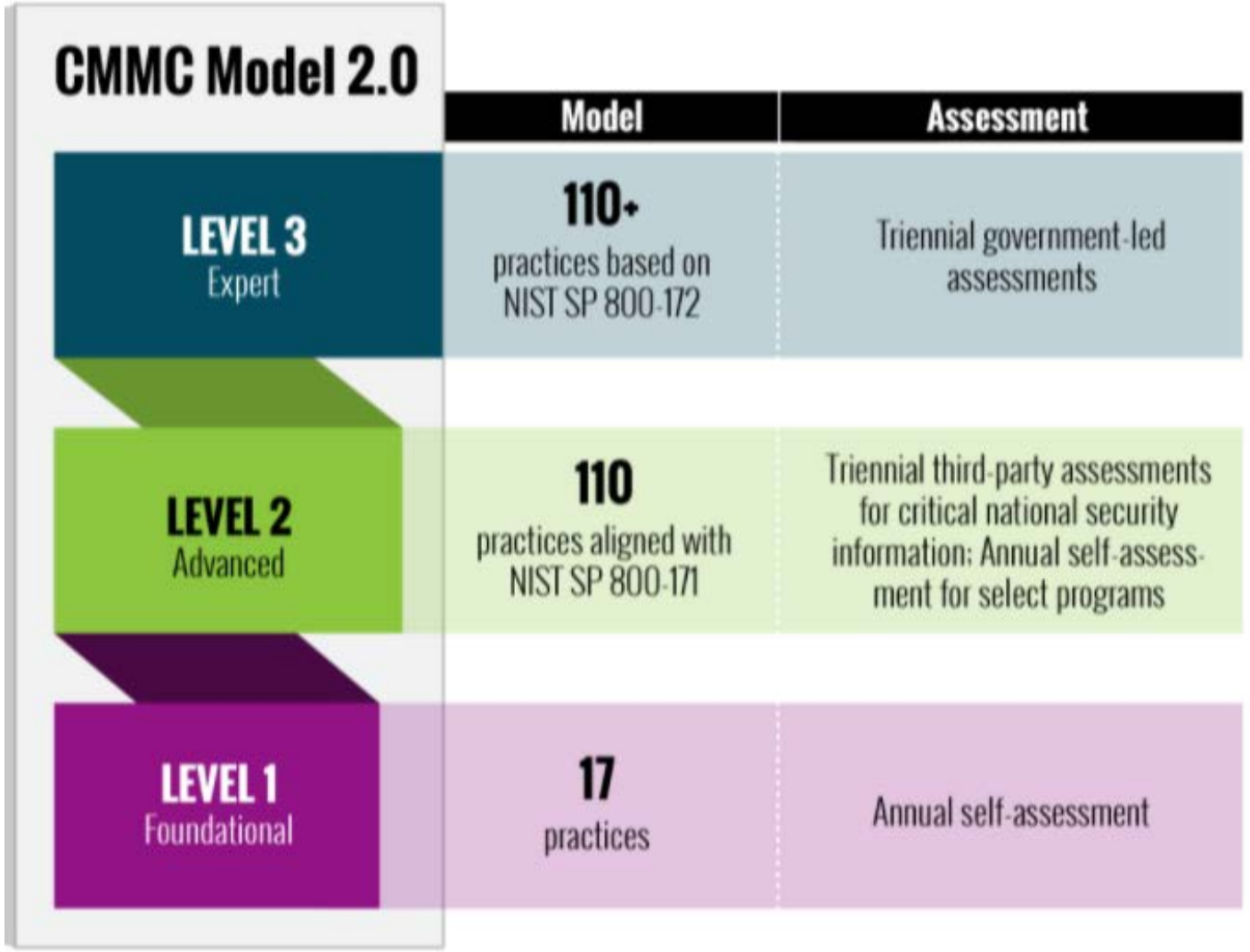
Operationally critical support is defined as supplies/services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

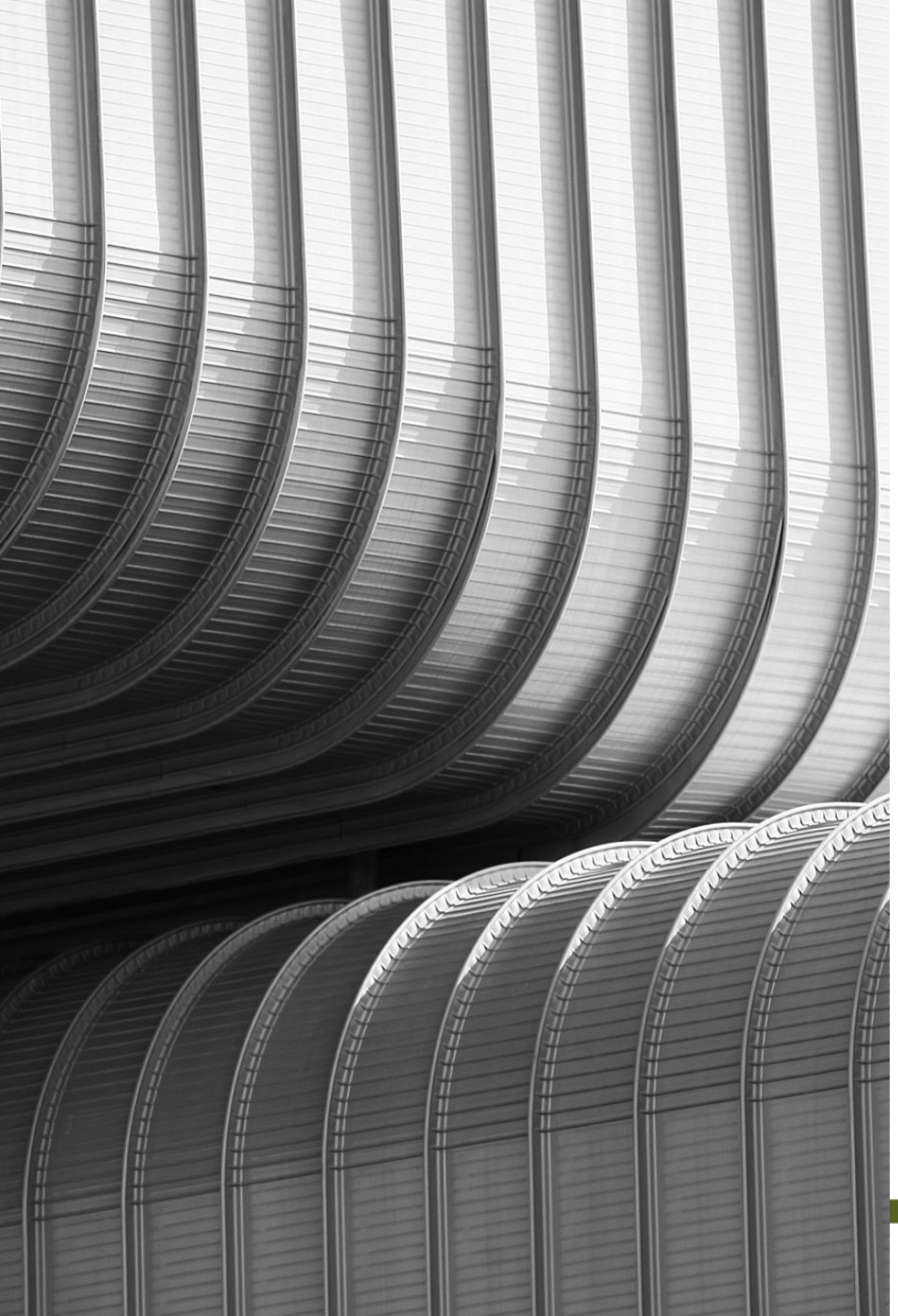
DFARS Clause 252.204-7012 requires contractors/subcontractors to:

1) **Safeguard covered defense information**
2) **Report cyber incidents**
3) **Submit malicious software**
4) **Facilitate damage assessment**

1) To safeguard covered defense information contractors/subcontractors must implement **NIST SP 800-171, Protecting CUI in Nonfederal Information Systems and Organizations**, as soon as practical, but not later than Dec 31, 2017
   - For contracts awarded prior to 1 Oct 2017, contractors/subcontractors shall notify DoD CIO within 30 days of contract award of any NIST SP 800-171 security requirements not implemented at the time of contract award.
   - If the offeror proposes to vary from NIST SP 800-171, they shall submit to the CO a written explanation of why a security requirement is not applicable **OR** how an alternative security measure is used to achieve equivalent protection
2) To report cyber incidents that affect covered defense information or that affect the contractor's ability to perform requirements designated as operationally critical support, the Contractor shall conduct a review for evidence of compromise and rapidly report cyber incidents to DoD at https://dibnet.dod.mil via an incident collection form (ICF).
3) If discovered and isolated in connection with a reported cyber incident, the contractor/ subcontractor shall submit the malicious software to the DoD Cyber Crime Center (DC3).
4) If DoD elects to conduct a damage assessment, the Contracting Officer will be notified by the requiring activity to request media and damage assessment information from the contractor.

Coming: The Cybersecurity Maturity Model Certification (CMMC)





Other and Evolving "Standards"

52.204-21 Basic Safeguarding of Covered Contractor Information Systems (FAR Contract Provision)

EO 14028 "Improving the Nation's Cybersecurity" issued on May 12, 2021

NSM-8 "Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems" issued January 19, 2022

DOJ Civil Cyber-Fraud Initiative

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Wednesday, October 6, 2021

Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative

Deputy Attorney General Lisa O. Monaco announced today the launch of the department's Civil Cyber-Fraud Initiative, which will combine the department'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.

"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," said Deputy Attorney General Monaco. "Well that changes today. We are announcing today that we will use our civil enforcement tools to pursue companies, those who are government contractors who receive federal funds, when they fail to follow required cybersecurity standards — because we know that puts all of us at risk. This is a tool that we have to ensure that taxpayer dollars are used appropriately and guard the public fisc and public trust."

The creation of the Initiative, which will be led by the Civil Division's Commercial Litigation Branch, Fraud Section, is a direct result of the department's ongoing comprehensive cyber review, ordered by Deputy Attorney General Monaco this past May. The review is aimed at developing actionable recommendations to enhance and expand the Justice Department's efforts against cyber threats.

Bucket 1: Knowing Failures to Comply With Cybersecurity Standards

Acting Assistant Attorney General Brian M. Boynton Delivers Remarks at the Cybersecurity and Infrastructure Security Agency (CISA) Fourth Annual National Cybersecurity Summit

Washington, DC ~ Wednesday, October 13, 2021

We have identified at least three common cybersecurity failures that are prime candidates for potential False Claims Act enforcement through this initiative.

First, the False Claims Act is a natural fit to pursue knowing failures to comply with cybersecurity standards. When government agencies acquire cyber products and services, they often require contractors and grantees to meet specific contract terms, which are often based on uniform contracting language or agency-specific requirements. For example, cybersecurity standards may require contractors to take measures to protect government data, to restrict non-U.S. citizen employees from accessing systems or to avoid using components from certain foreign countries. The knowing failure to meet these cybersecurity standards deprives the government of what it bargained for.

Bucket 1: Knowing Failure to Comply

E.g., *United States ex rel. Glenn v. Cisco Systems, Inc.*, Case No. 11-cv-400 (W.D.N.Y. 2011)

Settlement of $8.6 million paid to federal and state governments, including $2.6 million to resolve FCA claims, based on relator's allegations that Cisco knew the video monitoring technology it sold to the Government had serious cybersecurity flaws

Bucket 1: Knowing Failure to Comply

Cisco Systems (cont'd)

Interestingly, Cisco was predicated on a traditional "worthless product" theory, rather than a failure to comply with cybersecurity-specific requirements.

The complaint alleged that the flaws were so egregious that the government was not getting what it purchased: a functional video monitoring system.

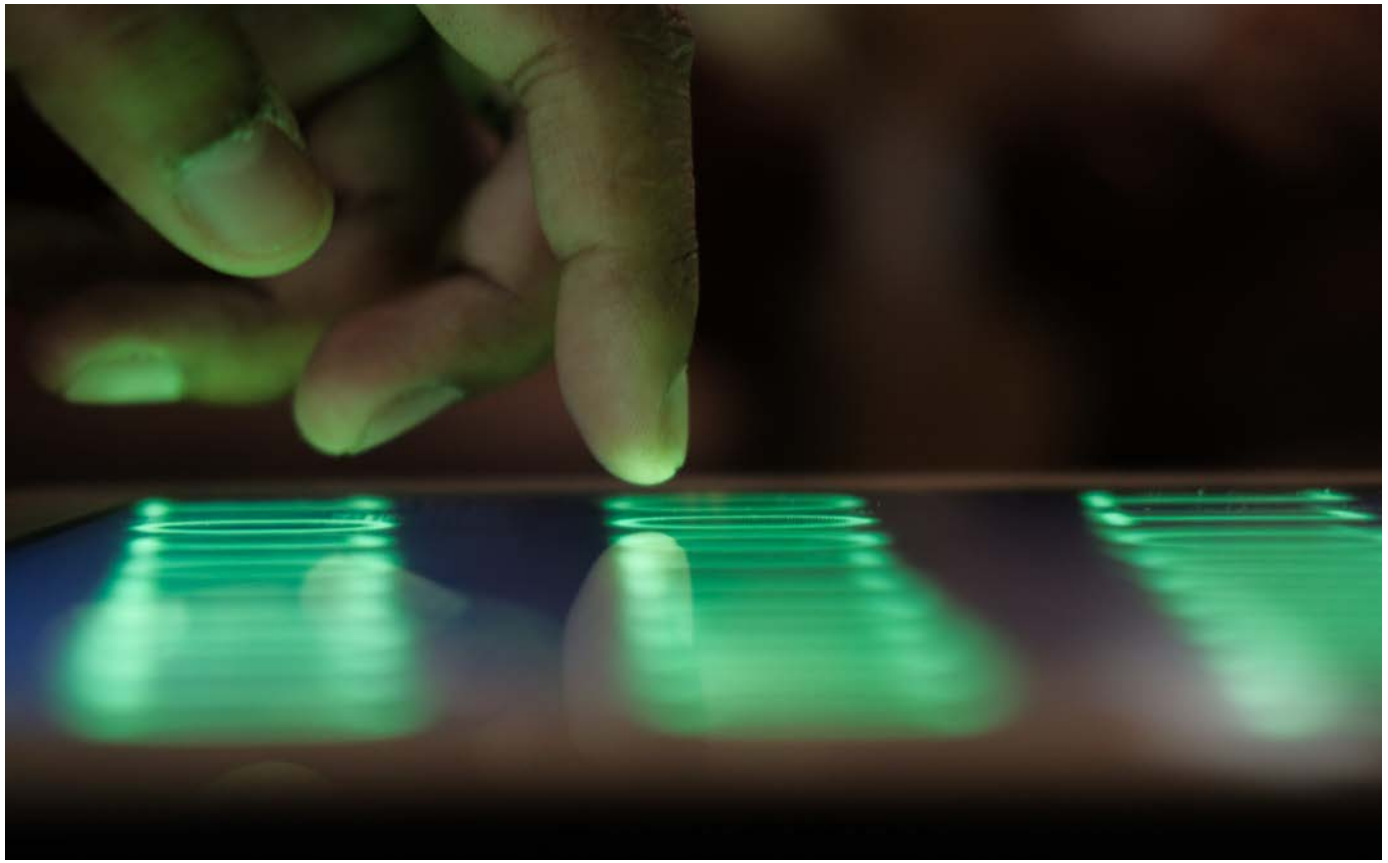
Demonstrates that classic FCA approaches are robust in the cybersecurity realm

Bucket 1: Knowing Failure to Comply

***But see United States ex rel. Adams v. Dell Computer Corp.*, 496 F. Supp. 3d 91, 100 (D.D.C. 2020)**

- "Mr. Adams does not allege that Dell was required to comply with any of the federal technology policies or that the contracts specified such compliance."
- "[E]ven if those requirements were passed along to Dell, the technology policies referenced by Mr. Adams do not require defect-free products, merely that the agencies limit the vulnerabilities and attempt to remedy them if located."
- "[T]he existence of a single vulnerability . . . would not necessarily be material to the agencies' acceptance of the computer systems and payment under the contracts."

Bucket 2: Knowing Misrepresentation of Security Controls and Practices



Acting Assistant Attorney General Brian M. Boynton Delivers Remarks at the Cybersecurity and Infrastructure Security Agency (CISA) Fourth Annual National Cybersecurity Summit

Washington, DC ~ Wednesday, October 13, 2021

Second, False Claims Act liability may be based on the knowing misrepresentation of security controls and practices. In seeking a government contract, or performing under it, companies often make representations to the government about their products, services, and cybersecurity practices. These representations may be about a system security plan detailing the security controls it has in place, the company's practices for monitoring its systems for breaches, or password and access requirements. Misreporting about these practices may cause the government to choose a contractor who should not have received the contract in the first place. Or it could cause the government to structure a contract differently than it otherwise would have. Knowing misrepresentations of this kind also deprive the government of what it paid for and violate the False Claims Act.

Bucket 2: Knowing Misrepresentation: Security Controls/Practices

In seeking a government contract, or performing under it, companies often make representations to the government about their products, services, and cybersecurity practices.

These representations may be about a system security plan detailing the security controls it has in place, the company's practices for monitoring its systems for breaches, or password and access requirements.

Misreporting about these practices may cause the government to choose a contractor who should not have received the contract in the first place. Or it could cause the government to structure a contract differently than it otherwise would have.

Knowing misrepresentations of this kind also deprive the government of what it paid for and violate the False Claims Act.

Bucket 2: Knowing Misrepresentation: Security Controls/Practices

What are the "misrepresentations," when were they made, and how were the relevant to contract award and/or claims payment?

Causation: Did the misrepresentations fraudulently induce the government to award the contract?

"False Claim": Do the claims misrepresent the goods and services at issue/for which the government is being charged?

Materiality: Did the misrepresentation affect the government's decision to pay claims?

Damages: Did the government suffer any actual damage?

Bucket 2: Knowing Misrepresentation: Security Controls/Practices

Nov. 2020: Interim DFARS re: NIST SP 800-171 DoD Assessment Requirements	*To be considered for award,* contractor must have a current assessment of "each covered contractor information system that is relevant"	Assessment posted in the Supplier Performance Risk System (SPRS)	These provisions implemented as part of CMMC rollout
• 252.204-7019 (notice provision) • 252.204-7020 (contract clause)		• "Basic" assessments = self assessment • Medium and High assessments = government assessment	

Bucket 2: Knowing Misrepresentation: Security Controls/Practices

- Nov. 2021: CMMC 2.0
  - Response to comments and implementation issues around CMMC 1.0
  - Attempts to simplify
  - Allows contractors at lowest tiers to self-assess and certify
- Bottom line: to participate in certain DoD contracts, companies will need to report their self-assessment = opportunities for misrepresentations that could lead to arguments regarding eligibility

Bucket 2: Knowing Misrepresentation: Security Controls/Practices

United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc., Case No. 2:15-cv-2245 WBS-AC (E.D. Cal.)

On Summary Judgment, Defendant argued that Relator's fraudulent inducement theory fails because no evidence of causation (i.e., no causal link between Aerojet's "representations regarding the extent of its noncompliance with the Cybersecurity Clauses" and the government's decision to contract – or pay claims).

On Summary Judgment, Defendant argued that Relator's fraudulent inducement theory fails because no evidence of causation (i.e., no causal link between Aerojet's "representations regarding the extent of its noncompliance with the Cybersecurity Clauses" and the government's decision to contract – or pay claims).
On Summary Judgment, Defendant argued that Relator's fraudulent inducement theory fails because no evidence of causation (i.e., no causal link between Aerojet's "representations regarding the extent of its noncompliance with the Cybersecurity Clauses" and the government's decision to contract – or pay claims).

Bucket 2: Knowing Misrepresentations of Security Controls or Practices

***E.g., United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, Case No. 2:15-cv-2245 WBS-AC (E.D. Cal.)**

29. Defendants have entered multiple contracts with the federal government, and as subcontractors on contracts with the federal government, which required that defendants meet the cyber security standards set forth in the DFARS Clause 252.704-7012 and NASA FARS Clause 1852.204-76 even though defendants knew their information systems did not meet these cyber security requirements.

Bucket 2: Knowing Misrepresentations of Security Controls or Practices

***Aerojet Rocketdyne*, 381 F. Supp. 3d 1240, 1246 (E.D. Cal. 2019)**

> First, defendants argue that AR disclosed to its government customers that it was not compliant with relevant DoD and NASA regulations and therefore it is impossible for relator to satisfy the materiality prong. The Supreme Court did observe in Escobar that "if the Government pays a particular claim in full despite its actual knowledge that certain requirements were violated, that is very strong evidence that those requirements are not material." Id. Here, however, relator properly alleges with sufficient particularity that defendants did not fully disclose the extent of AR's noncompliance with relevant regulations. See id. at 2000 ("[H]alf-truths--representations that state the truth only so far as it goes, while omitting critical qualifying information--can be actionable misrepresentations."). For instance, relator alleges that AR

Bucket 2: Knowing Misrepresentations: of Security Controls or Practices

Aerojet Rocketdyne, 381 F. Supp. 3d 1240, 1249 (E.D. Cal. 2019)

1020 (9th Cir. 2018). Defendants contend that the DoD never expected full technical compliance because it constantly amended its acquisition regulations and promogulated guidances that attempted to ease the burdens on the industry. This observation is not dispositive. Even if the government never expected full technical compliance, relator properly pleads that the extent to which a company was technically complaint still mattered to the government's decision to enter into a contract. (See SAC ¶¶ 66-72.) Defendants have not put forth any judicially noticeable

Bucket 3: Knowing Failure to Timely Report Suspected Breaches

Acting Assistant Attorney General Brian M. Boynton Delivers Remarks at the Cybersecurity and Infrastructure Security Agency (CISA) Fourth Annual National Cybersecurity Summit

Washington, DC ~ Wednesday, October 13, 2021

Finally, the knowing failure to timely report suspected breaches is another way a company may run afoul of the Act. Government contracts for cyber products, as well as for other goods and services, often require the timely reporting of cyber incidents that could threaten the security of agency information and systems. Prompt reporting by contractors often is crucial for agencies to respond to a breach, remediate the vulnerability and limit the resulting harm.

Breach: FCA Liability

- Not the breach, but the response
  - A breach alone is not fraud
  - Covering it up can be

- Failure to report is a violation of a contractual/regulatory requirement
  - Gives rise to subsequent false claims and/or false certifications
  - Strongest in DoD space because of DFARS
  - But present in many gov't contracts

Breach: DoD Requirements

- Three of the four DFARS 252.204-7012 requirements are implicated in breaches:
  - Reporting of cyber incidents
  - Submitting malicious software
  - Facilitating damage assessment

Breach: DoD Requirements

DFARS 252.204-7012(c)(1) -- Cyber incident reporting requirement.

- Triggered when Contractor discovers a cyber incident that
  - Affects a covered contractor information system **OR**
  - The covered defense information residing therein, **OR**
  - That affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support

Breach: DoD Requirements

DFARS 252.204-7012(c)(1) -- Cyber incident reporting requirement (cont'd)

- Two required steps
- When triggered, the contractor must
  - Conduct a review
  - Rapidly report

Breach: DoD Requirements

DFARS 252.204-7012(c)(1) –

Cyber incident reporting requirement (cont'd)

- The contractor must review for evidence of compromise of covered defense information:
  - Identify compromised computers, servers, specific data, and user accounts.
  - Analyze system(s) that were part of the cyber incident
  - Analyze any other systems on the network(s) that may have been accessed to identify compromised covered defense information
  - Analyze any other systems that affect the Contractor's ability to provide operationally critical support

Breach: DoD Requirements

DFARS 252.204-7012(c) -- Filing a cyber incident report

- Within 72 hours of discovery
- DFARS incorporates requirements set out at https://dibnet.dod.mil, including:
    1. Impact to Covered Defense Information
    2. Ability to provide operationally critical support
    3. DoD programs, platforms or systems involved
    4. Type of compromise (unauthorized access, unauthorized release (includes inadvertent release), unknown, not applicable)
    5. Description of technique or method used in cyber incident
    6. Incident outcome (successful compromise, failed attempt, unknown)
    7. Incident/Compromise narrative

Breach: FCA Liability

- Strong argument that a knowing failure to report a breach is material
  - DoD focus/DFARS
  - DOJ Initiative demonstrates government interest
- Scienter is critical
  - Can be hard to establish
    - Unless inferred from a cover-up
  - Whistleblowers will be key
- But where are the cases?

Breach: The Big Qs

How do you evaluate damages?

Where are the cases?

- So far, they're at the SEC and CFTC:
  - At least 12 actions since 2015
  - Fines ranging from $75K to $100M (Facebook)

Breach: The Big Qs (cont'd)

- What about the flipside?
- Is a breach required for an FCA claim?
  - No. Two prior theories are viable without a breach.
- But a breach can be useful evidence of the relevance of failures to comply with or misrepresentations about cybersecurity protocols.
  - Hard to argue willful ignorance of the failings if you've been hacked
  - Breach can be a proof of concept of the materiality of a cybersecurity failing

Breach: The Big Q's (con't)

- What makes the claim for payment "false" in these cases?
- Is a failure to report a breach tied to a claim for payment?

Other Thoughts

DoD is far ahead on these issues (in a three steps forward, two steps back way), but the Administration has made clear that it wants cybersecurity standards across government.

Likely leaders in civilian space are DHS and GSA.

Healthcare providers are a frequent target of cyberattacks. 45 CFR §§ 164.400-414 is the HIPAA Breach Notification Rule; requires reporting of certain incidents to HHS (they are posted on a website and investigated).

"Vendors of Personal Health Records" must report breaches to the FTC under the HITECH Act. *See* 16 CFR Part 318. A failure to report can be enforced by the FTC as an unfair or deceptive trade practice.

Question: The FCA is a powerful tool, but is it the right tool for enforcement in cybersecurity issues?