FCA AND CYBERSECURITY

Mike Beckwith
Partner
Internal Investigations
Former DOJ

DICKINSON WRIGHT

TRENDS

More of the False Claims Act (FCA) in 2026

1. ***More Money***: 2025 was the highest recovery year in the history of the FCA. Cybersecurity-related FCA actions recovered over $52 million.
2. ***More Settlements***: Cybersecurity-related FCA recoveries more than tripled.
3. ***More Whistleblowers***: 1,297 whistleblower lawsuits filed—the most ever (979 and 713 before).
4. ***More Investigations***: 401 new government investigations, reflecting a year-over-year trend. The DOJ initiating its own investigations independent of whistleblowers.
5. ***More CCFI***: The Civil Cyber-Fraud Imitative is no longer a "novel theory." The FCA is viewed as a "powerful weapon" against fraud.

DICKINSON WRIGHT

CAUTIONARY TAILS

Recent Cybersecurity FCA Settlements (2025–2026)

1. ***Hill ASC Inc. ($14.75 million)***: The largest cybersecurity-related settlement of the fiscal year.
2. ***Health Net Federal Services (Centene) ($11.2 million)***: Settled allegations of falsely certifying compliance with cybersecurity requirements in a contract for military health benefits.
3. ***Illumina Inc. ($9.8 million)***: Resolved a whistleblower action alleging the company sold gene sequencing systems with known cybersecurity vulnerabilities to feds.
4. ***Raytheon (RTX Corporation) ($8.5 million)***: Settled over allegations of failing to implement required security plans (NIST SP 800-171). The settlement included Nightwing Group as a "successor in liability."
5. ***MORSECORP ($4.6 million)***: A whistleblower-initiated settlement regarding cybersecurity noncompliance.

DICKINSON WRIGHT

NUTS AND BOLTS

Be Careful in 2026

1. ***Expansion Confirmed.*** 2025 enforcement results confirm the expansion of FCA liability into cybersecurity.
2. ***Cybersecurity as a fraud issue.*** Settlements reflect the emergence of cybersecurity misrepresentations as an FCA theory affecting the defense, aerospace, and space industries.
3. ***CMMC and NIST Compliance:*** The CMMC affirmation trap; and targeting "knowing" failures to implement the 110 specific security controls for handling Controlled Unclassified Information (CUI).
4. ***FedRAMP***: Investigations also target cloud service providers for misrepresenting their FedRAMP authorization status.
5. ***No Data Breach Required***: DOJ can and does pursue cases based solely on the false certification of security protocols.

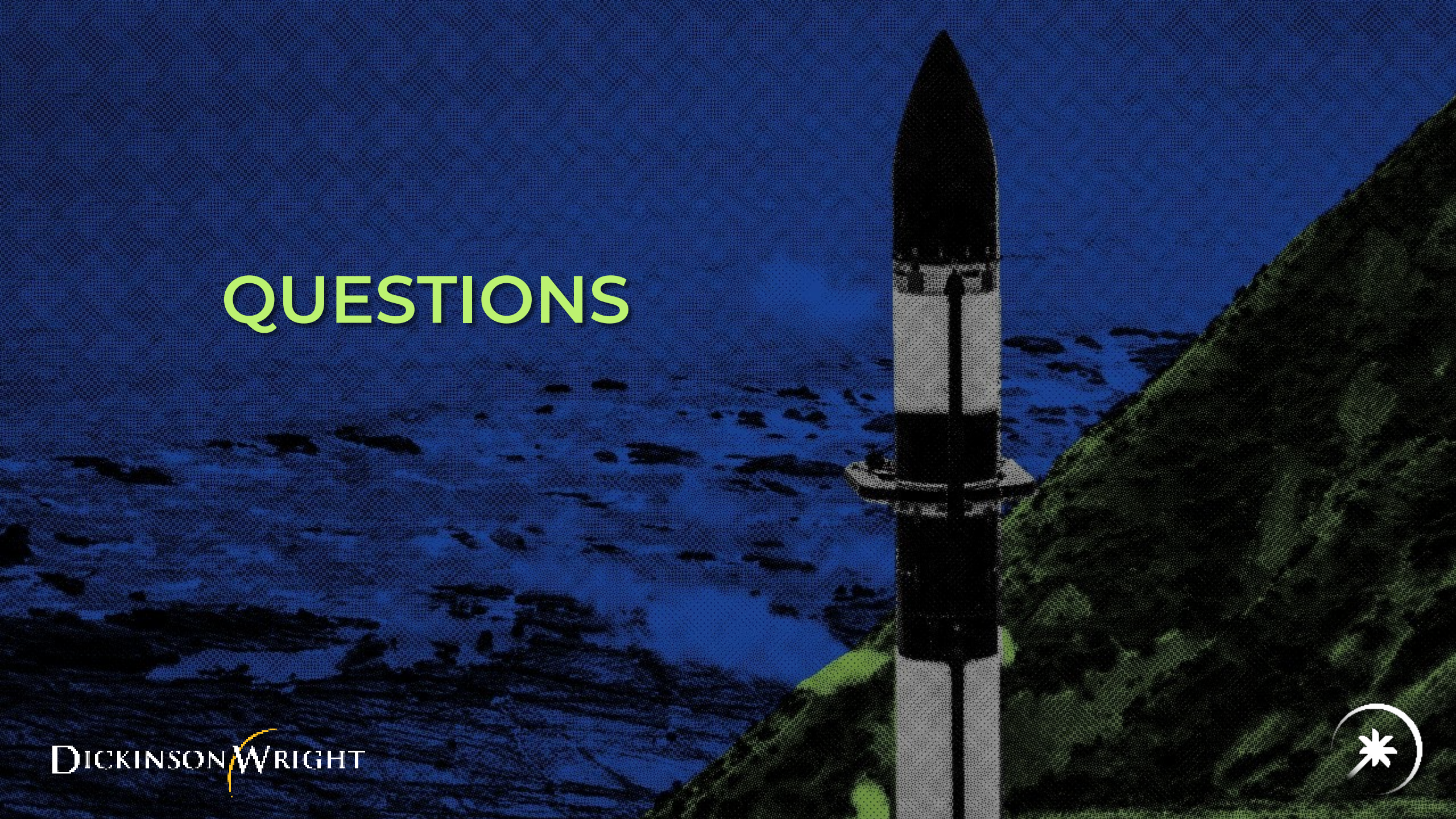
DICKINSON WRIGHT

TAKE AWAYS

"<u>Hear me now. Listen to me later</u>."

1. ***Enhance cybersecurity compliance.*** Conduct privileged "attestation dry runs," inventory vendor access, and align with CMMC and NIST standards.
2. ***Prepare for litigation.*** Design and implement a unified compliance program and preserve contemporaneous records showing compliant intent in real time.
3. ***DOJ is Lurking.*** 2025 FCA results confirm the focus on cybersecurity fraud is more aggressive. DAG Todd Blanche: DOJ will continue to "aggressively deploy" the FCA in the "key area" of government procurement.
4. ***Invest in Compliance.*** Compliance—particularly around cybersecurity—will position a company to withstand increased scrutiny, differentiating itself from others.

DICKINSON WRIGHT


QUESTIONS
DICKINSON WRIGHT