# NDIA 2018 International Explosives Safety Symposium & Exposition

## Risk Management & Governance Panel
## August 7, 2018

COVINGTON

BEIJING BRUSSELS DUBAI FRANKFURT JOHANNESBURG LONDON LOS ANGELES
NEW YORK SAN FRANCISCO SEOUL SHANGHAI SILICON VALLEY WASHINGTON

www.cov.com

# Reducing Tort Liability Arising Out of Federal Munition/Explosives Contracts: A Matter of Mutual Responsibility for the U.S. and Its Contractors

Presented By:
Ray Biagini, Partner
Covington & Burling, LLP
Rbiagini@cov.com

# A Nightmare Scenario

- U.S. Army contractor, Defense Inc., **designs, manufactures and stores** high-caliber explosive devices and munitions at its sites located nearby to Santa Fe, New Mexico and in military staging areas outside of Syria.
- Defense Inc.'s contracts are **classified** and their explosives and munitions are used by U.S. forces in Syria.
- Defense Inc. developed the **Technical Data Package** (TDP) for its product lines which the Army carefully **reviewed** and **approved**. Defense Inc. also had the Army review and approve its **storage** and **maintenance** procedures, including its perimeter security and access intrusion systems.
- Further, Defense Inc. obtained **SAFETY Act** coverage from DHS for its storage and maintenance security procedures and systems.

- On the 17th anniversary of the September 11 attacks, a small cadre of armed terrorists **breach** Defense Inc.'s perimeter security at the storage facility in Santa Fe and Syria which house multiple explosives and munitions.
- The terrorists **detonate multiple bombs** inside the storage depots, which kill numerous Defense Inc. employees, resident Army personnel, civilian workers and foreign nationals. The explosions are so catastrophic as to cause local Santa Fe businesses to shut down for weeks.
- Numerous **lawsuits** are filed in the U.S. against Defense Inc. and the Army by those injured and killed including foreign nationals, and by the local businesses. The suits seeks compensatory and **punitive** damages, lost revenue and profit in the millions.

# What Best Risk Management and Governance Practices Should The Military Contractor and the U.S. Use to Anticipate and Address Potentially Enterprise-Threatening Tort Liability Scenarios?

# What I Will Address Today

- Plaintiff's Tort Liability Theories
- Why Contractors Are The Target of Plaintiffs' Suits
- How and Why The U.S. and Its Contractors Should Build In A Joint Shield To These Suits
- Key Statutory/Regulatory Indemnity Under Government Contracts
- Specialized Defenses for "Contractors on the Battlefield"
- The SAFETY Act - - The Most Potent Tort Mitigation Tool For Contractors Supplying Anti-Terror Services of Products

# Plaintiffs' Tort Liability Theories

# Product Liability Theories

- The **CORE** allegations in any product liability suit: something about your product or services is **UNSAFE** in its design, manufacture, warning or training, that unsafe condition **caused or contributed** to my injury or death
- Give me the **$$$$!**

- Plaintiffs will seek **COMPENSATORY** damages – lost wages, medical expenses, pain and suffering, etc. and, maybe, **PUNITIVE** damages to punish the corporation
- Plaintiffs will seek such damages under several **LEGAL THEORIES**

- A “product” can include not only the overall system itself but also:
  - material, components and sub-assemblies
  - operating software
  - installation and operating environment
  - training programs
  - product literature, including operating and maintenance instruction and warm-up
  - peripheral equipment which must be utilized with the product for it to operate safely/correctly

# Plaintiffs' Key Liability Theories

- **Negligence** - - was the contractor's **conduct unreasonable**, failing to address **foreseeable** risks
- **Strict Liability** - - was the contractor's **product defective**
- **Failure To Warn** - - did the contractor fail to warn of hazards of which it had **actual knowledge**
- **Continuing Duty To Warn** - - did the contractor continue to **update** its warnings as it learned of new ones

- Under certain circumstances, all of these claims can be made in U.S. courts not just by U.S. citizens but by injured foreign nationals under the **Alien Tort Claims Act**

# Why Contractors are the "Tempting Deep Pockets"

# GovCon vs. USG Exposure

- Case Law Isolates Contractors as the **Tortious Targets**
- The Feres, Stencel and Hercules Decisions
  - Military personnel cannot sue the United States for tort damages arising out of **incidents related to military service**. *Feres v. United States* (1950)
  - Contractors cannot sue the United States in tort for **contribution** liabilities arising out of a military accident. *Stencel Aero Eng'g v. U.S*. (1977)
  - **Civilian government personnel** cannot sue the United States for tort damages arising out of the performance of a federal contract because of the Federal Employees Compensation Act bar.
  - Contractors cannot sue the United States for breach of **implied warranties** of design specifications. *Hercules v. United States* (1996).

# GovCon vs. USG Exposure

- Moreover, DOD's acquisition reform policies have often resulted in a "**historic shift**" of **discretionary** decision-making from government to industry, such as **striking balance** between safety, efficacy and costs through use of **performance-based** contracts and **commercialization** techniques in military procurements
- Although the U.S. can be sued under the **Federal Tort Claims Act**, U.S. enjoys powerful tort protection even when its own negligence caused the accident
  - Discretionary Function Exception
  - Combatant Activity Exception
  - In Country Exception
- All of this means that the contractor must know how to successfully assert **key defenses** in tort suits filed against it

# Proactively Building Key "Bookend" Defenses Into Contracts Benefitting U.S. and Contractor

- Why should the U.S. be interested in a **"partnered solution"** with its contractors to mitigate 3rd party tort liabilities?
  - If contractors **lose** tort cases, the U.S. loses too because of **"pass through"** of costs to U.S. for payment, higher contract prices and higher insurance premiums

- How can this partnered solution be implemented?

- In Boyle v. United Technologies, The **U.S. Supreme Court** Established The **Government Contractor Defense** for Contractors and Based It On The Government's **Discretionary Function Defense**

- A Government Contractor Can Eliminate Tort Claims Against It Under the Government Contractor Defense If:
  - The Government **Meaningfully Reviewed** and **Approved** Reasonable Precise Specifications for the Product or Service At Issue
  - The Product or Service **Confirmed** to the Approved Specifications
  - The Contractor **Warned** the Government of Hazards Actually Known to the Contractor But Not Known by the Government

- By Building the Government Contractor Defense Into Contract Activities, **Both** the Government's and Contractor's Ability to Defense Themselves From Tort Suits is Greatly **Enhanced**

- **Why?**

- The Government's Key Defense And the Contractor's Main Defense Enjoy a **"Common DNA."**

- When the Government Gets Sued In Tort For a Product It Procured, Its Main Defense Is to Prove It Exercised **"Meaningful Judgment"** Over the Key **Design** and **Safety** Features of the Product.  If it Can Prove That, It Walks

- This is Known As the Government's **"Discretionary Function"** Defense

- When A Contractor Is Sued In Tort For An Alleged Defective Product It Sold to the Government, Its Main Defense Is to Prove the Government **Meaningfully Reviewed** and **Approved**, i.e., Exercised Government **Discretion**, Over The Key Design/Safety Decisions and Features
- This Is the **Hallmark** of the Government Contractor's Defense

# How To Build In The Bookend Defenses

- At the Outset of the Contract Activity, the Contractor and Government Should Identify **"High Risk"** Design and Safety Issues
- Agree Through **Special H Clauses** That Such Areas Will Be Subjected to **Meaningful** Detailed Review and Consideration by the Government and the Contractor and Ultimately **Approved** By the Government

- Ensure **All Known Hazards** Are Identified to the Government, and Addressed and **Resolved** by the Government In Writing

- **Real Life Success Stories** - - TSA Contract To Reconfigure All U.S. Airports After 9/11 Terrorist Attacks; U.S. Navy Surface Warfare Center

- Through Careful Implementation, The Government and Industry Can Act Now to Proactively and Discriminately Create A **Joint Shield** to Future Tort Liability

# Key Statutory/Regulatory Indemnification Provisions That Can Reduce Tort Liabilities

- Pursue Statutory **Indemnity** from U.S. Where Appropriate
  - **10 U.S.C. §2354** – The Secretary of DOD is authorized to indemnify R&D contractors for 3rd party tort liabilities, including litigation and settlement expenses, for bodily injury or death from a risk the contract identifies as **"unusually hazardous"** and for which the contractor's insurance is not responding. DOD can pay such liabilities from (1) funds obligated for the performance of the contract or from funds available for R&D, not otherwise obligated; or (2) funds appropriated for those payments.

- **P.L. 85-804** – Certain federal agencies, including DOD, can provide **"extraordinary contractual relief"** to their contractors, including indemnification for 3rd party tort liabilities, where the Secretary of the agency determines to do so would **"facilitate the national defense."** To the extent the contractor's insurance is not responding to 3rd party liabilities, the federal agency that granted P.L. 85-804 indemnity must indemnify the contractor for such litigation expenses, settlements, etc. to the extent they arise out of a risk the contract defines as **"unusually hazardous."** The federal agency's requirement to indemnify for 3rd party liabilities is **not** limited to the availability of appropriate funds and applies even if the contractor acted with **wilful misconduct**.

- **FAR 52.228-7**, **Insurance-Liability to Third Persons –** for most cost-type federal contracts, the DOD and civilian agencies must reimburse a contractor for liabilities, including litigation and settlement expenses, to the extent NOT compensated by the contractor's insurance and subject to the availability of appropriated funds at the time the contingency occurs. This reimbursement occurs even if the contractor acted negligent but is not applicable if the contractor's directors, officers or managers acted with **wilful misconduct** or **lack of good faith**

# Specialized Defenses For "Contractors On The Battlefield"

# States Secrets Privilege

- This privilege "is a common law evidentiary rule that protects information from discovery when disclosure would be **inimical to the national security**." The United States may claim a privilege against the discovery of military and state secrets through a Declaration "lodged by the head of the department which has control over the matter, after actual personal consideration by that officer."
  - *U.S. v. Reynolds*, 345 U.S. 1 (1953). *Bentzlin v. Hughes Aircraft Co.,* 853 F. Supp. 1486 (C.D. Cal 1993); *White v. Raytheon*, 2008 WL 5273290 (D.Ma. 2008)

# Political Question Doctrine

- The political question doctrine ("PQD") bars any tort suit that would require the court to **second-guess** policy decisions that are constitutionally committed to the "political branches" of Government (i.e., Executive and Legislative branches). *See Baker v. Carr*, 369 U.S. 186 (1962). If a government contractor is "**under the military's control**" and its conduct is governed by military decisions that are "closely intertwined" with "national defense interests," then tort claims based on the contractor's conduct must be dismissed under the PQD.
  - *See Taylor v. Kellogg Brown & Root Services, Inc.*, 658 F.3d 402, 411 (4th Cir. 2011). *Carmichael v. Kellogg Brown & Root Servs., Inc.*, 572 F.3d 1271 (11th Cir. 2009)

# Combatant Activities Exception of the FTCA

- Tort claims against government contractors are **preempted** by the combatant activities exception ("CAE") of the FTCA where the application of state tort law conflicts with "**the military's battlefield conduct and decisions**." *Saleh v. Titan Corp.*, 580 F.3d 1, 4–5 (D.C. Cir. 2009). If a contractor is "**integrated**" with the military, and its alleged conduct "stem[s] from military commands," then the CEA will bar any tort claim challenging such conduct.
  - *In re KBR, Inc., Burn Pit Litig.*, 744 F.3d 326, 351 (4th Cir. 2014).

# Derivative Sovereign & Qualified Immunity

- Government contractors possess derivative and/or qualified immunity from suit for actions taken pursuant to a contract with the United States, provided that the contractor does not violate any **clearly established requirements** of federal law or the Government's "explicit [contractual] instructions."
  - *See Campbell-Ewald v. Gomez*, 136 S. Ct. 663 (2016); *Yearsley v. W.A. Ross Construction Co.*, 487 U.S. 500 (1988).

# The SAFETY Act - - Most Potent Tort Mitigation Technique For Contractors Supplying Anti-Terror Products or Services

# The Perfect Storm Led to the Enactment of the SAFETY Act in 2002

- **Post 9/11 Realities:**
  - Because of **liability** concerns, key homeland security providers were not going to sell their anti-terror technology into the marketplace
  - Federal courts were now finding that terrorist attacks were **foreseeable**
  - Insurance companies **stopped** writing terror coverage
  - **Pro-tort reform** White House and Congress
- The Safety Act is **landmark** legislation, **eliminating** or minimizing tort liability for **sellers** of or **facilities that deploy** anti-terror technology ("ATT") approved by the U.S. Department of Homeland Security (DHS) should suits arise in the U.S. after an act of terrorism
- The **Secretary of DHS** will determine on a case-by-case basis whether an attack is covered under the SAFETY Act

- **Act of Terrorism** is defined as an **unlawful** act **causing** harm to a person, property or entity in the U.S., **using** or **attempting to use** instrumentalities, weapons or **other methods** designed or intended to cause mass destruction, injury **or other loss** to citizens or instrumentalities of the U.S.
- The SAFETY Act defines "**loss**" as death, injury, or property damage, to third parties, including **business interruption loss**

# Protections Of The SAFETY Act

- **CERTIFICATION** – The Highest Form of Protection
  - Presumption that seller/deployer of ATT is **immediately dismissed** from the suit unless **clear and convincing** evidence that seller/deployer acted **fraudulently** or with **wilful misconduct** in submitting data to DHS during application process; **no punitives**; suit can be filed only in federal court; any liability **capped** at agreed upon limit, usually your **terror insurance** coverage limits

- **DESIGNATION** – Includes All of the Above **Except** Presumption of Immediate Dismissal
  - Developmental, Testing and Evaluation Designation
- These Certification and Designation protections also apply to seller/deployer's **subs, vendors, distributors** and **customers**, commercial or governmental, contributing to or utilizing SAFETY Act approved technologies

- Importantly, DHS clarified in 2006 that the protections can apply to entities implementing their **anti-terror security plans** to protect their **own facilities** and assets — crucial for soft targets like health care and entertainment venues
- Protections will apply even if the act of terror occurs **outside the United States** so long as the **"harm," including financial harm**, is to persons, property or entities in the United States. This is the **"extraterritorial"** feature of the SAFETY Act

- The definition of **"anti-terror technologies"** (ATT) is **broadly** applied by DHS, to cover technologies deployed in **defense against** or **response** or **recovery** from a terror attack
  - **Security Practices:**
    - Threat and vulnerability assessment protocol
    - Event day vs. non-event day security procedures
    - Emergency evacuation plans
    - Vendor selection
    - Hiring, vetting, and training of security personnel
    - Coordination response/recovery procedures with governmental entities
  - **Deployed physical security systems:**
    - Perimeter security, including guards and canines
    - Access intrusion detection systems, including CCTV, magnetometers, and metal detectors
    - Command and control centers
    - Delivery screening and public address systems
  - **Deployed cybersecurity systems:**
    - Recovery, restoration, and credentialing technologies

# Obtaining SAFETY Act Coverage – You Must Apply For It!

- Applicants Must Complete and Submit the SAFETY Act **Application Kit** to DHS
  - **Technical** section that emphasizes **written** evidence of **efficacy** of the ATT; readiness for deployment; existence of substantial third party risks; safety/hazards analyses; established **and documented** anti-terror decision-making processes. Demonstrate that your security planning processes are **written, repeatable,** and **enduring**
  - **Financial** section that requests (only for the ATT at issue) revenues or security expenditures for the current year and projection of revenues/security expenditures for the next two years

- **Insurance** section that requests information on applicant's **terror insurance** policies available to satisfy third-party claims arising out of an act of terror involving the ATT at issue, including information on exclusions, limits, deductibles and self-retentions. Your terror insurance limits (or lower amounts negotiated with DHS) usually become your SAFETY Act **cap** on liability

- Regarding **Confidentiality**, DHS Is Committed To **Vigorous Protection** of Applicant's SAFETY Act Data
  - Those conducting the review will enter into **non-disclosure** agreements and be subjected to a **conflicts-of-interest** evaluation
- SAFETY Act data is protected by the **Trade Secrets Act**; Exemption 1 (**"national security"**) and Exemption 4 ("privileged or confidential information") of FOIA; and under the **Critical Infrastructure Information Act** as a voluntary submission
- Unauthorized disclosure is subject to **criminal** penalties
- DHS agrees to **not** share data outside of DHS without **express permission** of applicant

- The DHS **Review** and **Approval** Process Takes About **120** days - - DHS has **200+** Experts From Academia, Federal Government, National Labs and FFRDC's To Review Applications
- Coverage usually awarded for **5 years** from date of decision. However, DHS has also awarded SAFETY Act protections to apply **retroactively** to **past deployments** of substantially equivalent ATT
- To obtain these tort protections, it is **CRUCIAL** that you demonstrate to DHS the **"PROVEN EFFECTIVENESS"** of your ATT, e.g., through your own internal testing/QC and third party assessments and evaluations, use of established vendor selection criteria and processes, etc.

# As The Foregoing Demonstrates, Obtaining SAFETY Act Coverage Is A Matter of Corporate Responsibility And Competitive Edge

- Given substantial risk mitigation benefits, those that sell or deploy Anti-Terror Technologies and services should pursue SAFETY Act Coverage as a matter of **Corporate Responsibility and Competitive Edge**
  - **Corporate Responsibility** – companies must take all reasonable steps to mitigate risks
  - **Competitive Edge –** because **customers** and **users** enjoy immunity from tort suits arising out of act of terror **only if** they buy and deploy **SAFETY Act approved** technology and services, customers have **incentive** to purchase SAFETY Act approved technology over non-SAFETY Act approved technology

# Representative SAFETY Act Awards

# Facility Awards

- **Dow Chemical's Facility Security Plan**, including vulnerability assessments; protection of chemical plants and storage; and cyber security emergency preparedness and response procedures
- **Cincinnati/Northern Kentucky Airport's Security Management Plan,** including electronic security tools; emergency operations center; selection, integration and maintenance of technical security systems; and operation and training procedures for its airport police, rescue and firefighter personnel

- **Port Authority of New York/New Jersey's New Freedom Tower of the World Trade Center**, including for its security assessments and designs and architectural/engineering services that incorporated security-related design features at Freedom Tower and WTC
- **General Growth Properties**, including its Shopping Mall Security Management Services; its tracking and monitoring procedures for outside perimeters and on-site parking; its emergency response program; and its selection criteria used for security vendors
- **Numerous sports stadiums and arenas**, including their physical and cyber security deployments

# Product Awards

- **Michael Stapleton Associates**' X-Ray screening; bomb/hazardous materials detection equipment; and training regimen for bomb sniffing dogs
- **Rapiscan's** Conventional X-Ray detection systems for airports
- **Raytheon's** perimeter intrusion detection system
- **Wachenhut's** physical security guard services
- **URS'** threat and vulnerability services
- **SAIC's** cargo inspection system used at ports of entry

# Key Takeaways

- Federal contractors involved in **unusually hazardous** work like manufacture, storage, and handling of explosives and munitions should proactively pursue a **layered** risk mitigation strategy and a **"partnered solution"** with its U.S. customer.
- It is in both parties to reduce or eliminate 3rd party liabilities and to create a **"joint shield"** that protects and benefits the U.S. and its contractors