BNA, INC.

FEDERAL CONTRACTS

BNA Employee-Owned Since 1947

REPORT

The SAFETY Act Interim Regulations: Will They Fulfill the Homeland Security Mission By Stimulating Innovations in Antiterrorism Technology?

BY DAVID Z. BODENHEIMER

On Oct. 16, 2003, the Department of Homeland Security issued interim regulations (68 Fed. Reg. 59684-59704) implementing the SAFETY Act (Pub. L. No. 107-296, §§ 861-65; 116 Stat. 2135) enacted on Nov. 25, 2002. The Department justified the need for these regulations to be immediately effective because further delays in shielding companies from product liability lawsuits could stall the availability of antiterrorism technology ''that will save lives.'' 68 Fed. Reg. 59684. This justification mirrors the legislative purpose underpinning the Act:

> Briefly, the SAFETY Act ensures that U.S. companies will be able to develop and provide vital anti-terrorism technologies to help prevent or respond to terrorist attacks without the threat of crippling lawsuits.

148 Cong. Rec. E2079 (Nov. 15, 2002) (statement of Rep. Armey).

How true are the interim regulations to the SAFETY Act's legislative purpose? While the interim regulations represent a considerable improvement over the proposed regulations issued on July 11 (68 Fed. Reg. 41420), serious shortcomings remain. In short, the interim regulations contain too much red tape, too many disincentives to SAFETY Act protection, and too few assurances of a timely, fair, and cost-effective approval process that will protect companies' rights and highly confidential data. Following are 10 key problem areas and a discussion of each:

(1) Automatic Termination of Rights

(2) Duration of Protection

(3) Confidentiality of Data

(4) Finality of Agency Decision

(5) Insurance Coverage and Data

(6) Application Burden

(7) Certification Requirements

(8) Preamble versus Regulatory Text

(9) Retroactivity

(10) Government Contractor Defense

David Z. Bodenheimer is a partner in the Washington, D.C., office of Crowell & Moring LLP where he specializes in government contracts and homeland security matters, including chemical/biological protection, border security and technology, and the SAFETY Act. He may be reached at (202) 624-2713 or dbodenheimer@crowell.com.

(1) Automatic Termination of Rights

For Sellers that might be tempted to modify antiterrorism technology, the interim regulations introduce great uncertainty and potentially draconian penalties: ''A Designation shall terminate automatically, and have no further force or effect, if the designated qualified anti-terrorism technology is significantly changed or modified.'' 68 Fed. Reg. 59701-02, § 25.5(i). This penalty cannot be squared with the plain language or legislative purpose of the statute or with basic statutory construction. Nowhere does the text of the SAFETY Act itself even suggest the potential for automatic termination of liability protection for Sellers. Furthermore, the very

 ISSN 0014-9063

purpose of the SAFETY Act is to spur the growth of antiterrorism technology, yet the threat of automatically chopping off such rights discourages Sellers from proceeding with technology innovations that may strip away SAFETY Act protection. Finally, automatic termination of rights represents a forfeiture that should not be implied in the statute because forfeitures are judicially disfavored. *See, e.g., Bell Helicopter Textron,* ASBCA No. 21192, 85-3 BCA ¶ 18,415 at 92,429 (''Every reasonable presumption is against a forfeiture''); *Bozied v. Brookings,* 638 N.W. 2d 264 (S.D. Sup. Ct. 2001) (''Forfeitures are considered odious in the law'').

At a minimum, the regulations must recognize fundamental obligations for due process by guaranteeing notice and an opportunity to be heard before a Seller's rights may be terminated. In a similar context, the Federal Acquisition Regulation (FAR) specifically accords procedural due process for contractors' data rights by prohibiting an agency from striking restrictive markings on technical data until after the contractor receives written notice of the agency challenge and a 30-day period to provide ''written justification'' for such markings. FAR § 52.227-14(e). Sellers of antiterrorism technology deserve at least this much procedural protection against termination of rights under the SAFETY Act.

(2) Duration of Protection

Without stating any legal or factual justification, the interim regulations limit the duration of SAFETY Act protection: ''A Designation shall be valid and effective for a term of five to eight years (as determined by the Under Secretary based upon the technology) commencing upon the date of issuance.'' 68 Fed. Reg. 59701, § 25.5(f). As a legal matter, this limitation of ''five to eight years'' violates the express language of the SAFETY Act. For example, the SAFETY Act establishes unconditional, unlimited protection against punitive damages and pre-judgment interest: ''No punitive damages . . . may be awarded, nor shall any party be liable for interest prior to the judgment.'' Pub. L. No. 107-296, § 863(b)(1). If Congress intended to impose a limited shelf life upon such protection, the Act would have stated: ''No punitive damages may be awarded *for five to eight years*.'' *See, e.g., Harris v. Commissioner of Internal Revenue,* 178 F.2d 861, 864 (2nd Cir. 1949) (''dangerous business'' to add words to a statute). Furthermore, this artificial limitation undercuts the Act's purpose of creating incentives for spurring and spreading antiterrorism technology by saddling Sellers with the cost and uncertainty of seeking renewals not contemplated by the Act.

As a factual matter, the Department asserts – with no reference to any agency findings or evidence – that ''five to eight years provides a fair balancing of public and private interests.'' 68 Fed. Reg. 59686. The interim regulations leave us to guess about what has been ''balanced'' or how ''five to eight years'' could be fair. A typical drug takes 10 years to hit the market (Barbaro, ''Biodefense Plan Greeted With Caution,'' *Washington Post*, p. E1 (May 2, 2003)), meaning that SAFETY Act protection could come and go before a biodefense company could make its first sale. Similarly, a trade association representing over 400 corporate members recently explained during congressional hearings that ''a minimum of 10 years – if not substantially longer – . . . is more consistent with the effective dates of long-term services agreements'' and ''the length of time to develop and implement complex systems and services.'' *Implementing the SAFETY Act: Advancing New Technologies for Homeland Security: Hearings Before the House Government Reform Comm.,* 108th Cong., 1st Sess. (Oct. 17, 2003) (statement of Information Technology Association of America President Harris Miller) (hereinafter ''*House SAFETY Act Implementation Hearings*''). If the SAFETY Act did allow the Department to impose a limited period of protection, the public record already establishes that five to eight years is much too short.

(3) Confidentiality of Data

The interim regulations contemplate ''electronic submission'' of information, such as SAFETY Act applications. 68 Fed. Reg. 59696. Indeed, the Application Kit (www.safetyact.gov) states that ''electronic submissions are strongly encouraged to expedite the application process.'' At the same time, the Application Kit requires submission of extraordinarily sensitive technical and financial data regarding the Seller's business plan, technology costs, sales projections, and ''unique technology attributes.'' In response to industry concerns about confidentiality of such key trade secrets and proprietary information, the Department listed various legal protections, including the Trade Secrets Act, but offered no special plan or measures to protect such data. 68 Fed. Reg. 59687.

Electronic security breaches – such as hacking – represent a skyrocketing threat, as the General Accounting Office (GAO) has found a tenfold increase since 1998. GAO, ''Information Security: Further Efforts Needed to Fully Implement Statutory Requirements in DOD,'' p. 7 (July 24, 2003) (GAO-03-1037T). In one instance, a single British computer administrator ''used his home computer and automated software available on the Internet to scan tens of thousands of computers on U.S. military networks.'' *Id.* at 9. Not surprisingly, electronic security arose as a crucial – and unresolved – problem during the recent SAFETY Act hearings:

> [T]he Internet is still an open system and vulnerable to breaches. We are concerned that there is no mention of a comprehensive management plan to secure the systems over which data will be transmitted, policies and procedures applicable to DHS personnel operating and having access to the system, or details on the technological approaches the Department will take to secure the data provided by applicants.

House SAFETY Act Implementation Hearings (statement of ITAA President Miller). The Department cannot serve the SAFETY Act's basic purpose of promoting antiterrorism technology if Sellers are discouraged from submitting applications by uncertain or insufficient assurances of electronic security for confidential data.

(4) Finality of Agency Decision

In an effort to preempt external scrutiny, the interim regulations state that the Department's ''decision shall be final and not subject to review'' because ''second-guessing of the Secretary's discretionary judgment'' would be ''inappropriate.'' 68 Fed. Reg. 59701, 59688. The Department's position is half right. A legislative rationale exists for barring third-party challenges alleging that the Department improperly *approved* a SAFETY Act application. Such third-party protests would undermine the certainty of SAFETY Act protection and increase the Seller's risk of exposure to liability lawsuits, thereby striking at the Act's core purpose of encourag-

  FCR ISSN 0014-9063

ing companies to bring out more antiterrorism technology.

In contrast, improper rejections of Sellers' applications warrant external scrutiny. The SAFETY Act's history reflects a legislative intent favoring liberal approval, not rejection, of liability protection for antiterrorism technology: ''it is Congress' hope and intent that the Secretary will use the necessary latitude to make this list as broad and inclusive as possible, so as to insure that the maximum amount of protective technology and services become available.'' 148 Cong. Rec. E2080 (Nov. 15, 2002) (statement of Rep. Armey). Furthermore, the Department's discretion should not shield improper rejections from review by a neutral forum because disappointed SAFETY Act applicants deserve to have their applications considered fairly, just as the Court of Claims recognized a disappointed bidder's right to judicial review when an agency breached its implied duty ''to give fair and impartial consideration'' to bids nearly 50 years ago. *Heyer Prods. Co. v. United States*, 135 Ct. Cl. 63, 69 (1956). Finally, a recent incident underscores the need for external review. A Homeland Security official recently announced that the SAFETY Act did not cover existing technology: ''This is not for technologies already out there being used.'' Hasson, ''DHS teaches lawsuit protection,'' *Federal Computer Week* (Sept. 12, 2003). Although the Department has since backtracked from this unjustifiable position, disappointed applicants need a neutral forum, such as a court or administrative board, to ensure that SAFETY Act protection is not unfairly denied for critical antiterrorism technology.

(5) Insurance Coverage and Data

Perhaps no part of the interim regulations raises more questions – and provides less insight – than the insurance requirements. Two of the more troubling questions center upon the amount of required insurance and the type of information to be submitted by Sellers.

The Amount of Insurance

The interim regulations require Sellers to ''obtain liability insurance.'' 68 Fed. Reg. 59699, § 25.4(a). How much insurance is enough? These regulations largely mirror the inscrutable words of the Act: ''the maximum amount of liability insurance reasonably available from private sources on the world market at prices and terms that will not unreasonably distort the sales price of the Seller's anti-terrorism technology.'' *Id.*, § 25.4(b). Like a minotaur's maze, the proposed regulations leave sellers and Department personnel alike begging for direction:

- ''Unreasonably distort the sales price.'' From whose perspective? The Seller's? A competitor's? A federal agency's? An affected member of the private sector?
- ''Available from private sources.'' Of what sort? Thinly capitalized sources? Captive insurers?
- ''Terms.'' Of what sort? Package insurance deals? Equity stakes in the technology?

Seller's Submission of Data

The seller must submit information about the required insurance. Much of the information (insurer's name, policy description, deductibles, and exclusions) is garden variety, but some information requires a crystal ball, such as:

> The price for such insurance, if available, and the per-unit amount or percentage of such price directly related to liability coverage for the Seller's qualified anti-terrorism technology deployed in defense against, or response to, or recovery from an act of terror.

68 Fed. Reg. 59700, § 25.4(g)(6). To know the ''per unit amount or percentage of such price,'' the seller must guess the sales volume at variable prices spread over federal, state, local, and private buyers for technology that may have no sales or claims history. In addition, the interim regulations acknowledge that the ''insurance market appears to be in disequilibrium'' and ''little market information exists'' (68 Fed. Reg. 59695), thus raising a question about the realism and propriety of such demands for insurance information from Sellers. Finally, industry warned the Department that insurance information and prices could not be traced directly to a specific antiterrorism technology because ''most liability insurance is not purchased product-by-product.'' 68 Fed. Reg. 59687. The Department acknowledged ''the difficulties,'' but inexplicably failed to relieve applicants of these unreasonable burdens for insurance information.

(6) Application Burden

The Department underestimated the interim regulation's burden on applicants by an order of magnitude. The interim regulations estimate ''36 to 180 hours per application'' and presume a ''relatively low estimated burden of applying for this technology program.'' 68 Fed. Reg. 59696, 59694. During the recent hearings on October 17, 2003, a major industry association concluded – based upon actual responses from industry members – that the application would consume an average of 1,000 hours. *House SAFETY Act Implementation Hearings* (testimony of ITAA President Miller).

A typical drug takes 10 years to hit the market, meaning that SAFETY Act protection could come and go before a biodefense company could make its first sale.

The 35-page ''SAFETY Act Application Kit'' (www.safetyact.gov) represents classic information overkill that should be slashed under the Paperwork Reduction Act requirements. This Application Kit demands massive amounts of sensitive management and financial data, such as business plans, past and future customer lists, profitability analyses, sales history and revenue projections, and detailed cost data and estimates. For the many commercial technology companies that refused to do business with the government until the Federal Acquisition Streamlining Act relieved many of the burdensome Truth in Negotiations Act requirements for submitting mountains of cost data, this Application Kit creates a huge hurdle that will discourage some of the best technology companies from even considering a SAFETY Act application. Ironically, the Department's request for a tsunami of sensitive and expansive financial information may overwhelm not only many small technology companies, but even the Homeland Security Department reviewers, as it could take months for government economists to wade through the submissions

of financial data. *House SAFETY Act Implementation Hearings* (testimony of ITAA President Miller).

(7) Certification Requirements

The interim regulations specify annual certifications that ''the Seller has maintained the insurance required'' by the Under Secretary. 68 Fed. Reg. 59700, § 25.4(i). While this provision imposes a requirement not mentioned in the statute itself, the more pernicious certification requirement surfaces in the Application Kit that requires the applicant ''under penalty of perjury'' to declare that ''all statements made and information provided in this application and any accompanying documents are true, correct, and complete.'' By extending this certification ''under penalty of perjury'' to ''all statements and information'' in the application, the Department has created a certification of unprecedented breadth and unmatched burden. Hardly any functional unit in any company (Finance, Engineering, Testing, Program Management, Risk Management, *etc.*) can readily escape the staggering burden of assuring the accuracy and completeness of ''all statements and information'' in the application, including:

- *Financial Information:* ''Sales revenues,'' ''Technology Costs,'' ''Gross Profit,'' and ''annual production volume,'' both historically and prospectively
- *Engineering Details:* ''scientific principles and unique technology attributes distinguishing the ATT [antiterrorism technology] from alternatives''
- *Risk Assessments:* ''studies and reports supporting assessments of the magnitude of risk exposure to the public''
- *Testing Information:* ''*measures* for evaluating the expected operational performance of the technology''
- *Safety Data:* ''all known or suspected *current hazards* and safety issues associated with the ATT''

Even more troubling, the ''Application Kit'' certification covers not only verifiable facts, but also a bundle of estimates, judgments, and pure speculation, such as ''Symbolic Damage,'' ''Mass Disruption,'' and ''psychological impacts.'' Not even the Truth in Negotiations Act (10 U.S.C. § 2306a(h)(1)) mandates a certification of such ''judgmental information.'' Rather than fulfilling the SAFETY Act's purpose, the Department's Application Kit certification creates a powerful disincentive to seeking liability protection – and developing life saving antiterrorism technology – due to the demand that companies certify the uncertifiable.

(8) Preamble Versus Regulatory Text

For reasons not explained, the Department relegated much of the SAFETY Act implementation to the preamble or other introductory comments, rather than incorporating the statements into the text of the interim regulation itself. For example, the introductory comments capture the purpose of the SAFETY Act with crystal clarity:

> The purpose of the Act is to ensure that the threat of liability does not deter potential manufacturers or Sellers of antiterrorism technologies from developing and commercializing technologies that could save lives.

68 Fed. Reg. 59690. The Department should include this statement in the text of the regulation (§ 25.1 ''Purpose'') so that long after the *Federal Register* notice has disappeared into mists of time, the regulation itself will remind both agency officials and technology Sellers of why Congress enacted the SAFETY Act. Such an express statement of purpose would reduce the risk of unduly restrictive interpretations that could choke off critical liability protection to antiterrorism technology Sellers.

Federal preemption represents a second critical topic that the Department should move from the introductory remarks (68 Fed. Reg. 59693) to the regulatory text itself. For many companies, a litigation nightmare begins with being hauled into a plaintiff-friendly local court in another state to defend against a mass-tort lawsuit. The Department's introductory remarks squarely address this concern with a well-stated agency position that the SAFETY Act creates a federal cause of action that preempts a state lawsuit against the Seller arising out of an act of terrorism. 68 Fed. Reg. 59693. Because such preemption offers essential protection to antiterrorism technology Sellers against high-risk state court liability lawsuits, the Department should set forth its position in the text of the final regulations.

(9) Retroactivity

Regarding SAFETY Act coverage for antiterrorism technology already in the marketplace, the Department stated that ''it would be inappropriate to apply SAFETY Act protections retroactively to deployments of a qualified anti-terrorism technology that occurred prior to the effective date of the Designation issued for such technology.'' 68 Fed. Reg. 59686. The Department then draws a strained distinction between technology that has been deployed versus sold. *Id.* In plain language, the Department's interpretation would recognize SAFETY Act coverage for a bomb detector being transported to the installation site (sold, *but not* deployed), but deny coverage to an identical bomb detector already installed (sold *and* deployed) prior to the effective date of designation. The Act does not draw such a distinction, and neither should the Department. So long as no terrorist incident has occurred, the SAFETY Act coverage should extend to *all* ''qualified anti-terrorism technologies'' (Pub. L. No. 107-296, § 863), not just undeployed ''qualified anti-terrorism technologies.'' *See House SAFETY Act Implementation Hearings* (statement of Professional Services Council President Stan Soloway). The artificial distinction not only penalizes existing technologies, but creates a substantial disincentive to rapid deployment of life-saving antiterrorism technologies.

(10) The Government Contractor Defense

The government contractor defense stands as the crown jewel of liability protection under the SAFETY Act and interim regulations: ''The government contractor defense is an affirmative defense that immunizes Sellers from liability for certain claims brought under Section 863(a) of the Act.'' 68 Fed. Reg. 59691. While acknowledging that the courts have also recognized a government contractor defense, the Department correctly states that the SAFETY Act's ''express terms supplant many of the requirements in the case law for application of the defense'' and that ''these express provisions of the Act, rather than by the judicially-developed criteria'' determine the applicability of the government contractor defense. *Id.*

After drawing this bright line between the statutory and judicial versions of the government contractor de-

  FCR ISSN 0014-9063

fense, the Department then confuses the issue by suggesting a linkage between the two versions of the defense:

> The Department believes that Congress incorporated the Supreme Court's *Boyle* line of cases as it existed on the date of enactment of the SAFETY Act, rather than incorporating future developments of the government contractor defense in the courts.

Id. The only common thread between the SAFETY Act and the judicial government contractor defense is that both offer the contractor immunity from tort suits. To prevent future misunderstandings that might creep from the Department's comments into a plaintiff tort lawyer's brief, the final regulations should omit this confusing statement in order to ensure that antiterrorism technology receives the full benefit of the SAFETY Act's robust government contractor defense.

Conclusion

In the midst of a massive reorganization, the Homeland Security Department has accomplished much. However, the interim regulations and ''Application Kit'' threaten to negate much of the initial promise of the SAFETY Act due to restrictive interpretations, inordinate paperwork burdens, and inadequate protection of the rights and needs of the companies that must bring antiterrorism technology to the front lines. In making the necessary revisions to the final regulations, the Department must return to the core purpose of the SAFETY Act – fostering antiterrorism technology by eliminating the threat of crippling liability litigation. Only then will the public interest be served by expediting the development and deployment of life-saving antiterrorism technology.