Countering Terrorism One Technology at a Time

Laura Itle

The Problem

In 2003, the Department of Homeland Security (DHS) needed a repeatable methodology for the evaluation of anti-terrorism products and services. IDA's resulting peer-review model looks for measures of operational performance and long-term reliability, as well as the implementation of sound business practices and strong personnel training programs.

IDA developed a flexible, repeatable methodology for assessing the technical capability and operational effectiveness of anti-terrorism products and services.

Dates and hashtags tend to mark the ongoing threat of global terrorism: the early morning of June 12, 2016; the night of May 22, 2017; the sunny afternoons of April 15, 2013, December 2, 2015, November 13, 2015, March 22, 2016, and July 14, 2016; #JeSuisCharlie; #JeSuisParis; #JeSuisOrlando; #PrayforNice; and #PorteOuverte. The events and images are often overwhelming, so much so that it seems that no progress has been made to prevent or detect future acts or protect the public from the harm that these attacks cause. Then, there are the attacks that didn't happen—ones that don't make the news. Someone picks up the phone and calls law enforcement. Thousands of hours of intelligence gathering stops attackers before they strike. Dollars are invested to buy technology and to train responders. That last element, dollars invested in technology and personnel readiness, calls to mind another date: November 25, 2002, the date the Homeland Security Act of 2002 was enacted.

Tucked into the 187 pages of statutory language that created the DHS is Subtitle G (Section 861-865), the Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act. A relatively small section, four-and-a-half pages total, the SAFETY Act was intended to provide industry incentives to invest in the development and deployment of anti-terrorism technologies by establishing a system of risk and liability management protections (see Figure 1). The Act and the DHS Implementing Regulations outline eleven criteria (see Figure 2) that, broadly speaking, ask DHS to determine the technical efficacy of a product and service while, at the same time, determining an insurance liability cap.

- The SAFETY Act is part of the Homeland Security Act of 2002 passed by Congress.
- It provides legal liability protections for manufacturers and sellers of qualified anti-terrorism technologies (ATTs) that could save lives in the event of a terrorist attack.
- Its protections apply only to claims arising out of, relating to, or resulting from an Act of Terrorism when SAFETY Act-covered technologies have been deployed.
- It comprises two broad classes of protection:
  - *Designation,* which provides a liability cap, exclusive action in Federal court, no joint and severable liability for non-economic damages, and no punitive damages or prejudgment interest
  - *Certification,* which provides all benefits of Designation, plus the rebuttable presumption of the Government Contractor Defense and placement on the Approved Products List for Homeland Security

Figure 1. SAFETY Act Quick Facts

The SAFETY Act and DHS Implementing Regulations outline eight general criteria for Designation and three Certification conditions that are discretionarily applied by DHS.

SAFETY Act Designation Criteria

1. Prior U. S. Government use or demonstrated substantial utility and effectiveness
2. Availability of the anti-terrorism technology (ATT) for immediate deployment in public and private settings
3. Existence of extraordinarily large or extraordinarily unquantifiable potential third-party risk exposure to the Seller or other provider of such ATT
4. Substantial likelihood that such ATT will not be deployed or will have less than optimal deployment unless SAFETY Act protections are extended
5. Magnitude of risk exposure to the public if such ATT is not deployed
6. Evaluation of all scientific studies that can be feasibly conducted to assess the capability of the technology to substantially reduce risks of harm
7. ATT that would be effective in facilitating the defense against acts of terrorism, including technologies that prevent, defeat, or respond to such acts
8. A determination by Federal, State, or local officials that the technology is appropriate for preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise case

SAFETY Act Certification Conditions

The technology

1. Will perform as intended
2. Conforms to the Seller's specifications
3. Is safe for use as intended

Figure 2. Statutory SAFETY Act Criteria

In May 2003, DHS asked IDA to help develop a method to assess the operational effectiveness of new technologies and determine the proper level of liability insurance that each company should carry. Within 5 months, DHS was able to accept SAFETY Act applications for evaluation. DHS subsequently asked IDA to refine and implement the initial evaluation methodologies using the combined operational test and evaluation and cost analyses experience of IDA's Operational Evaluation Division and Cost Analysis and Research Division. In 14 years, IDA, in support of the DHS Office of SAFETY Act Implementation (OSAI), has reviewed thousands of technologies: metal detectors, chemical, biological, radiological, nuclear, and explosive (CBRNE) sensors; mass notification systems; integrated security programs for sports stadiums; cybersecurity platforms; first responder gear; medical countermeasures; and others. Each technology represents the willingness of the private sector to invest in the development of anti-terrorism measures to protect the general population through the deployment of one technology at a time.

IDA developed a flexible, repeatable methodology for assessing the technical capability and operational effectiveness of anti-terrorism products and services.

Establishing a Review Process

Central to IDA's support of OSAI is a repeatable process staffed with the right mix of people to assess the diverse range of potential technologies that can seek SAFETY Act protections. The evaluation process is subject to the following conditions:

- Any application should be processed in 120 business days, including a 30-day completeness phase and a 90-day evaluation phase.
- Applications should be reviewed using consistent measures, irrespective of the type of technology or the size of the business entity seeking protections.
- Applications should be assessed against the statutory criteria and subject to a liability cap analysis.

Under these constraints, we constructed a peer-review process (see Figure 3) that uses independent technical experts and IDA core staff.

Note: Using a peer-review model with specific process milestones, IDA for the last 8 years has helped DHS achieve its congressionally required 120-day average processing timeline while maintaining analytical rigor and adherence to evaluation guidelines.

Figure 3. General Process Flow

The process begins with IDA and DHS reviewing applicant data to determine whether sufficient background, operational, and financial data exist to conduct a full review (completeness phase). Initially, to characterize the type of data needed, we bifurcated the evaluation methodology into two categories: products and services. We then compare to the SAFETY Act statutory criteria to develop guidance on measures and metrics against which each technology could be reviewed and the type of data to be submitted by industry (see Figure 4).

The evaluation of products follows a traditional research and developmental model. Applicants are asked to provide manufacturing information, developmental and operational testing, and instructional manuals. Service applications rely on a process-based methodology that takes into account the 4Ps:

- **Processes** for developing a service-based technology
- **Procedures** for deploying a technology consistently across varied deployments
- The backgrounds and qualifications of the **People** who provide a technology
- Methods for documenting and the results of service **Performance** in the field.

IDA's methodologies for the evaluation of products and services also capture the human element and adaptations that occur because of specific deployment locations. They also allow us to look at how

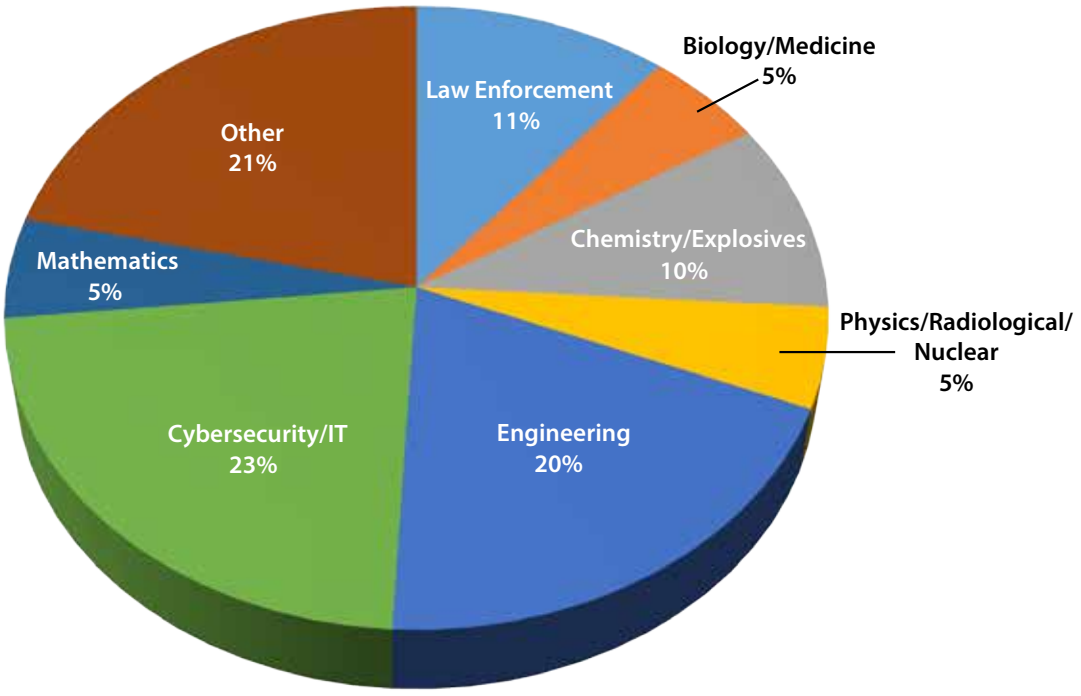
Measures and Metrics	Capability (Designation Criteria 2 and 6)	Effectiveness (Designation Criterion 7)	Long Performance (Certification Condition 1)	Safety (Certification Condition 3)
Products	Engineering design, laboratory tests, applicable standards	Evidence of performance metrics, deployment performance, customer feedback	Reliability, maintainability, suitability, usability, long time course performance data	Certifications, user manuals, mitigation techniques
Services	People, process, policies and procedures	Suitable performance of past deployments documented, internal/external audits favorable, customer feedback favorable	Quality assurance plans documented, range of feedback, performance in simulated events	Training programs, OSHA compliance, worker claims, mitigation techniques, licensures

Figure 4. Guidance on Measures and Metrics

technology providers might react to unanticipated future changes in operation (e.g., having to adapt to a future threat), how providers implement quality control measures to support consistent operations or correct problems, and how a provider might ensure that practitioners are hired, trained, and vetted.

If sufficient data exist for review, the evaluation phase begins. First, application materials are shared with subject matter experts (SMEs). Drawing from retired Federal law enforcement communities, the national laboratories, and its own community, IDA maintains a team of more than 100 SAFETY-Act-trained experts who have experience in counter-terrorism operations, the physical sciences, law, medicine, physical security, and training (see Figure 5). Experts score each technology against the statutory criteria, which are then provided to the IDA core team for further analyses.

Next, the core research team, consisting of 20 analysts, including former State and Federal law enforcement agents and industry security experts, PhD-level scientists and engineers, and economists, consolidates expert findings with other research. In addition to taking into account the SME scores, IDA analysts incorporate into a final report the results of customer surveys,



Note: This graph presents a snapshot of IDA's current expert pool. The "Other" category refers to experts in public policy, ports, canine detection, special tactics, forensic science, and counterterrorism and insurgency operations.

Figure 5. IDA SMEs by Discipline

consultations with other government agencies, and independent technical research. This final report also includes the IDA team's analysis of an applicant's insurance policies and liability exposure. Each report works through IDA's quality control process before it is submitted to OSAI. OSAI reviews this report in light of its own analysis and makes a recommendation to the Under Secretary for Science and Technology as to whether a technology should be Designated and Certified, thus completing the process.

Adapting the Review Process

As the need for anti-terrorism products and services grew, industry turned to the SAFETY Act and, in particular, the Approved Products List for Homeland Security to inform purchasing decisions. While purchasing SAFETY Act-approved technologies, venue owners also realized the importance that these protections could have in the development and deployment of integrated security solutions at a specific venue. Starting with the New York Stock Exchange, IDA adapted the base methodology for the evaluation of venue-specific (and campus-specific, in the case of Southern Methodist University) anti-terrorism measures.

We worked to refine methodologies for specific types of venues. For example, IDA, working in collaboration with OSAI and the National Football League (NFL), created a tailored process for the review of stadiums that implement the NFL's practices for stadium security. This method compares the applicability of various NFL-proprietary security measures to the SAFETY Act statutory criteria through a set of tailored technical forms and structured interview guides. These forms and questionnaires are accompanied by a guided elicitation tool for SMEs to focus their reviews solely on the implementation of the NFL Best Practices. To date, IDA has assessed the security programs of seven NFL stadiums (see Figure 6), with a specific focus on anti-terrorism measures such as active shooter prevention and response and measures for minimizing the risks from improvised explosive devices (IEDs).

Similarly, with the increasing prevalence of cyber attacks, IDA is working with DHS to develop tailored methodologies for the assessment of corporate cybersecurity solutions that protect electrical generation and distribution systems. This method ties the SAFETY Act statutory criteria to the National Institute of Standards and Technology (NIST) Cybersecurity Framework and other standards such as NIST Special Publications (SP) 800-53 Revision 4 *(Security and Privacy Controls for Federal Information Systems and Organizations)* and NIST SP 800-82 Revision 2 *(Guide to Industrial Control Systems (ICS) Security).*

These tailored methods for physical and cybersecurity measures retain the fundamental principles of SAFETY Act reviews (the need for developmental and operational test data and for information on processes, procedures, people, and performance) while accounting for specific threat types and industry guidance.

(a) (b)

Note: (a) The author (right) and a DHS-colleague at Lambeau Field (home of the Green Bay Packers) during the development of an NFL-specific methodology for stadium security program evaluations; (b) An IDA analyst, Mr. Gregory Olmstead, on a site visit to the University of Phoenix Stadium (home of the Arizona Cardinals)

Figure 6. Assessing the Security Programs of NFL Stadiums

Evaluation Process

IDA's evaluation process has been successfully implemented to review several thousand applications, resulting in 934 individual SAFETY Act Designations and Certifications in the past 14 years (see Table 1). At the end of July 2017, 75 technologies had received SAFETY Act protections in Fiscal Year (FY) 2017, representing over $3 billion in revenue and over 81,000 employees. Thirty-five percent of these technologies were provided by small businesses. The 2017 SAFETY Act Designations and Certifications include:

- Autonomous aerial reconnaissance and surveillance systems that can

Table 1. Numbers of SAFETY Act Awards Since FY 2012

TYPE	FY12	FY13	FY14	FY15	FY16	FY17
Certification	3	1	2	1	1	4
Designation & Certification	24	14	19	19	26	29
Designation	40	39	35	57	41	46
DT&E Designation	6	6	9	10	8	12
Total	**73**	**60**	**65**	**87**	**76**	**91**

be deployed from land or sea for border surveillance

- Computed-tomography systems for the detection of explosives and other prohibited items in carry-on luggage at airports or other screening checkpoints
- Security personnel who provide access control and crowd management at sporting events, business conventions, and concerts
- The physical security program for Gillette Stadium, home of the New England Patriots.

These technologies, along with hundreds of others, are used by first responders, law enforcement and public safety agencies, and private security providers. They touch all aspects of American life—where we shop, how we travel, where we learn, and where we play. They help us communicate faster in crises and help keep our data secure. Each product or service was painstakingly reviewed to ensure that if a business is granted liability protections to help it succeed, Americans will benefit from technically sound anti-terrorism solutions. For 14 years, IDA's evaluation method has adapted to changing threat environments and industrial innovation and is poised to continue to do so as DHS seeks to respond, deter, and protect against acts of terrorism that might otherwise become simply another date or hashtag.

Acknowledgments

IDA wishes to thank DHS OSAI, particularly Director Bruce Davidson and Deputy Director Rachel Abreu, for its continued sponsorship. The SAFETY Act task at IDA is supported annually by more than 100 analysts across the IDA Systems and Analyses Center's eight divisions and the IDA Science and Technology Policy Institute. The author wishes to thank the core staff of Mr. David Berezansky, Ms. Larysa Murray, Mr. David Greene, Ms. Dina Gregory, Mr. Gregory Olmstead, Mr. John Seidenberg, Mr. Tj O'Connor, Ms. Nancy LeMieux, Mr. Christopher Lawyer, Ms. EunRae Oh, Ms. Amelia DiAngelo, Mr. Scott Bidlack, Mr. Ryan Ellman, Dr. Dennis Kimko, Dr. John Bailey, Dr. Dmitriy Mayorov, and Dr. Thomas Frazier.

Dr. Laura Itle *is a Research Staff Member in IDA's Operational Evaluation Division. She holds a Doctor of Philosophy in chemical engineering from Pennsylvania State University.*