

# Research & Development Partnerships Group

Working with You to Serve the Homeland  
Security Enterprise

December 2010



Homeland  
Security

Science and Technology

Editor:

Thomas A. Cellucci, Ph.D., MBA  
Research & Development Partnerships Group  
Science & Technology Directorate  
U.S. Department of Homeland Security



### **Working Together to Create High Impact Results**

The Research & Development (R&D) Partnerships Group serves as the primary collaborative group for the Department of Homeland Security Science & Technology Directorate (DHS S&T). It aims to support, enhance, enable and efficiently expedite the fielding of advanced homeland security capabilities through interactions with potential domestic and international partners found in the private sector, university communities, national labs, government agencies and elsewhere to leverage our collective expertise, resources and knowledge to efficiently and effectively develop capabilities aligned to the mission-critical needs of the Homeland Security Enterprise (HSE).

This book serves as a resource and illustrates the various areas of expertise found within the R&D Partnerships Group and how -- through cooperation and collaborative teamwork -- we progress to successfully and effectively foster mutually beneficial partnerships that save time, taxpayer money and government resources and contribute to the execution of DHS S&T's mission of strengthening America's security and resilience by providing innovative science and technology solutions for the HSE.

Much effort has gone into the publication of this book. I would like to specifically thank Dr. Matthew Clark, Mr. James Johnson, Ms. Lilia Ramirez, Mr. Randy Zeller, Ms. Marlene Owens, Mr. W. Adrian Groth, Ms. Elissa Sobolewski, Mr. Bruce Davidson, Mr. Stephen Hancock, Mr. Mark Protacio and Ms. Caroline Greenwood.

Thomas A. Cellucci, Ph.D., MBA  
Director (Acting)  
Research & Development Partnerships Group  
Science & Technology Directorate  
U.S. Department of Homeland Security  
[SandT\\_RDPartnerships@dhs.gov](mailto:SandT_RDPartnerships@dhs.gov)

## Table of Contents

Overview: Mission and Vision of the R&D Partnerships Team.....	4
It’s a Simple Equation: Easy to Understand but Hard to Live Day by Day.....	6
The Critical Role of Requirements .....	7
If You Can’t Measure It, You Can’t Manage It.....	21
Meet the R&D Partnerships Group: A Focused Team Approach.....	23
Office of National Labs .....	24
Technology Transfer.....	29
Office of University Programs.....	31
International Cooperative Programs Office .....	36
Interagency Division.....	38
Office of SAFETY Act Implementation.....	44
Public-Private Partnerships Office.....	43
Small Business Innovation Research .....	51
Long Range Broad Agency Announcement .....	55
Commercialization Office.....	56
DHS S&T Research Council .....	63
Keep it Simple and Make it Easy.....	64
Help Us to Help You.....	64
Summary .....	67
Appendix A: R&D Partnerships Group Opportunities Guide	

## Introduction

The U.S. Department of Homeland Security was established in January, 2003 to serve as an organization comprised of operating components, directorates and offices working toward the unified goal of keeping America safe. The Department leverages its close relationships with federal, state, and local governments to create an integrated force focused on protecting our citizens. This coordinated effort creates a national security strategy that truly encompasses all aspects necessary to securing the homeland.

The Science & Technology Directorate (DHS S&T) serves as the primary research and development entity for the Department. DHS S&T's mission is to improve homeland security by providing our partners the state-of-the-art technology that helps them achieve their missions. DHS S&T's main partners include the seven operating components of the Department, along with state, local, tribal and territorial emergency responders and officials. DHS S&T is structured to put its partners first and foster relationships with those on the front lines to gather critical information about the challenges that they face on a daily basis in service to our country.

DHS S&T is organized into four main groups: Homeland Security Enterprise and First Responders, Homeland Security Advanced Research Projects Agency (HSARPA), Acquisition Support and Operations Analysis, and Research & Development Partnerships. These groups work together to engage and support the DHS operating components and other members of the Homeland Security Enterprise (HSE) to fulfill their missions. Figure 1 shows the current organization of DHS S&T.

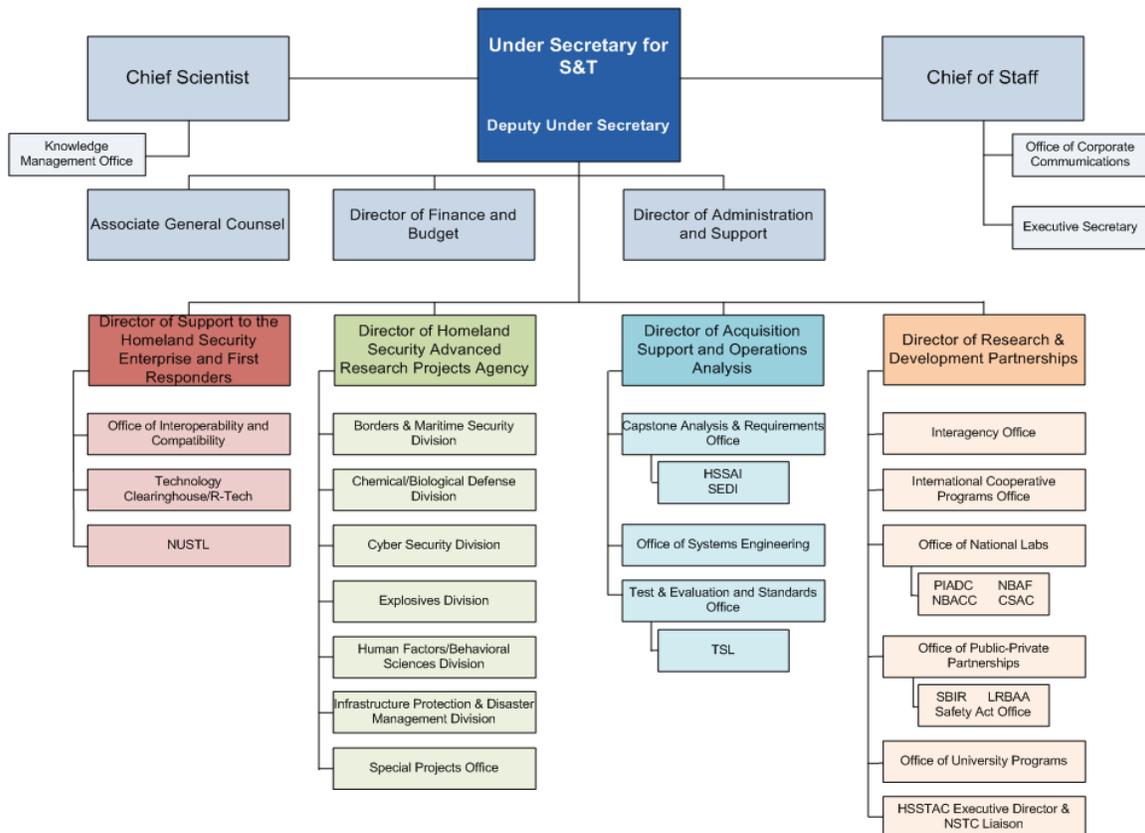


Figure 1 The DHS Science & Technology Directorate

## Overview: Mission and Vision of the R&D Partnerships Group

The Research and Development Partnerships Group is the primary external interface for the U.S. Department of Homeland Security, Science & Technology Directorate. The R&D Partnerships Group works with partners across government, internationally and in the private sector to leverage mutually beneficial investments, activities and technology development efforts that facilitate the fielding of high impact capabilities for members of the Homeland Security Enterprise. The R&D Partnerships Group is comprised of a powerful and well-resourced collection of offices that focus on several aspects of research, innovation and the development of technology and products for use in the HSE. This collaborative model will enhance DHS S&T's outreach and engagement with the many entities that are actively involved with efforts that can bring greater security to the HSE. See Figure 2 for a graphical description of the various members that comprise the S&T Enterprise.

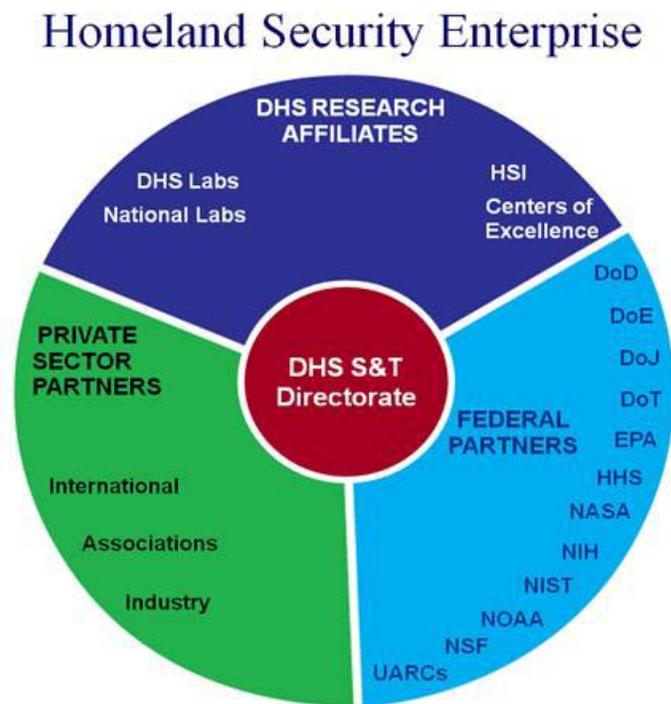


Figure 2 The Homeland Security Enterprise brings contributions to S&T from many entities.

Bringing together the full scope, expertise and shared knowledge of the HSE, the R&D Partnerships Group seeks to promulgate and serve as a catalyst for improved interaction and cooperative engagement between its members. The R&D Partnerships Group has a staff that brings years of experience in the homeland security field with diverse backgrounds and expertise that allow for a stronger connection between the HSE and DHS S&T.

The increased emphasis on partnerships is part of the recognition that sharing the work of addressing the needs of the HSE is a key factor in increasing the efficiency and timeliness for delivering needed capabilities. Nowhere is speed-of-execution more important than in defending the people, property and resources of the United States. There are tremendous amounts of work taking place in many different sectors of the HSE and it is the goal of the R&D Partnerships Group to create the opportunities that will

allow useful and impactful connections to be made to advance the development of capabilities in a unified and coordinated manner.

Mission:

The mission of the R&D Partnerships Team is to interact with potential domestic and international partners found in the private sector, university communities, national labs, government agencies and elsewhere to leverage our collective expertise, resources and knowledge to efficiently and effectively develop capabilities aligned to the mission-critical needs of the Homeland Security Enterprise.

Vision:

The vision of the R&D Partnerships Team is to support, enhance, enable and efficiently expedite the fielding of mission-critical capabilities for the Homeland Security Enterprise through interactions with potential partners that foster mutually beneficial partnerships that save time, taxpayer money and government resources.

### **It's a Simple Equation: Easy to Understand -- but Hard to Live Day by Day**

History has demonstrated, time and time again that the most elegant solutions in science and technology are normally simple to understand. For example,  $E=mc^2$  is a rather simple equation for mass-energy equivalence that would be considered an elegant solution to a complex problem. The same is true in describing organizational performance:

$$P = S \times I$$

Where 'P' is Performance; 'S' is Strategy; and 'I' is Implementation.
---

To say it simply: Performance is obtained when an organization combines strategic vision with the discipline “to get things done” (a phrase describing execution or “implementation”). It is certainly easy to understand – but alas, very difficult to accomplish on a day-in and day-out basis. Adherence to this simple equation requires a deep, focused and prioritized list of strategic requirements; requirements that eventually must be delineated in detailed operational requirements to be shared internally and externally when it is determined that partners can/should be engaged to assist DHS. This information must be distilled from a platform of good ideas, wants and needs articulated in the Homeland Security Enterprise (HSE). But having the ‘S’ is not enough. A famous Chinese proverb states that “vision without action is a daydream.” In order to make a strategy actionable and impactful, it is crucial (that is why Strategy and Implementation are multiplicative rather than additive) that there exist reliable tools, resources, models, etc. to implement (‘I’) or execute the strategy. To determine how well we progress against our strategic goals, we developed easy-to-understand performance metrics to constantly monitor how we are doing.

In summary, this book is a “living document” in which we will regularly update our strategic goals and objective and utilize field-tested tools, methods and world-class personnel to execute them. We always welcome your feedback and comments on how we can improve our implementation pathways.

## The Critical Role of Requirements

In today's dynamic homeland security environment, delivering cost-effective products and services that meet well thought-out detailed requirements is a critical objective for DHS. DHS is composed of many organizational elements with an overriding goal: to enable, support and expedite the mission-critical objectives of DHS' seven operating components – Transportation Security Administration (TSA); U.S. Customs and Border Protection (CBP); U.S. Secret Service, (USSS); U.S. Citizenship and Immigration Service (USCIS); U.S. Immigration and Customs Enforcement (ICE); Federal Emergency Management Agency (FEMA); and the U.S. Coast Guard (USCG). These seven operating components work closely with, support and are supported by a large network of first responders at the state, local and tribal levels. Additionally, the nation's critical infrastructure and key resources (CIKR) owners and operators also have direct connects to DHS. DHS must coordinate, drive and prioritize the detailed needs of this diverse group of operating components and supporting elements, whose missions address a wide variety of terrorist and natural threats to our homeland, in order to maximize the effective use of DHS' resources. Ever changing threat dynamics often require new, innovative- technology based solutions in order to prevent or mitigate the potential effects of current and future dangers. The DHS Science and Technology Directorate (DHS S&T), works diligently to understand, document and offer solutions to current and anticipated threats faced by our "customers" (DHS operating components and field agents) and our "customers' customers" (first responders and the eighteen infrastructure industrial sectors such as banking, chemicals and communications, etc.).

DHS S&T has several strategic efforts and programs that are driven to generate several outputs that guide the development and fielding of products, services and systems for the operating components. DHS S&T regularly conducts strategic needs analysis to determine and prioritize the mission needs and capability gaps that exist within a particular functional area. Capability gaps are broad descriptions of department level identified mission needs that are not met given current products and/or standards. Capability gaps briefly catalog opportunities for enhanced mission effectiveness or address deficiencies in national capability.

DHS S&T interacts regularly with our customer(s) to determine capability gaps. These capability gaps, in many ways, are just the beginning. From a product development standpoint, a capability gap is one of the initial steps in the requirements hierarchy scheme. Additional detailed requirements must be developed to enable the development of a technology or product. The R&D Partnerships Group will expand these efforts across the HSE. DHS S&T realizes that we must work with our customers to produce a detailed set of requirements in order to communicate with other operating components and frequently to various solutions development partners to field solutions aligned to stated requirements.

### Product Realization beyond Capability Gaps

If you think about it, there are numerous examples in our professional and private lives where the lack of communication or unclear terminology has created misunderstandings, problems and a myriad of other issues. As in any worthwhile pursuit, effective communication is critical in the cost-effective and efficient interactions between various parties seeking a mutually beneficial relationship or partnership.

At every step of product development, it is critical to understand and meet user needs. Product development is not a trivial effort; but with proper planning, tracking and communication, successful

product development can yield measurable positive results and provide DHS operating components with resources necessary to carry out their mission-critical objectives to protect our country.

The initial phase of product realization is a mission needs assessment. This assessment should be conducted relative to the overall mission for a given organization. This exercise identifies capabilities needed to perform required functions, highlights deficiencies in a functional capability and documents the results of the analysis. Some of these capabilities may already be addressed with existing products, systems or services currently accessible by an organization. Additionally, a mission needs assessment serves to identify deficiencies in current and projected capabilities. In the event that current products are not able to address a particular capability; a capability gap exists. Briefly, capability gaps are defined by the difference between current operational capabilities and those necessary capabilities needed to perform mission-critical objectives that remain unsatisfied. Capability gaps must be listed in terms of an overall need to perform a specific task and should avoid explaining how that task should be achieved.

For example, faced with the problem of potential intruders to a sensitive facility, we might define the requirement as “build a wall” whereas the real requirement is “detect, thwart, and capture intruders.” Our wall might “thwart” intruders (or might not, if they’re adept at tunneling), but it would not detect them or facilitate their capture. In short, the solution would not solve the problem.



The robust capability gap to “detect, thwart, and capture intruders” includes no preconceived solutions and prompts us to analyze alternative conceptual solutions and choose the best.

One way to ensure that we are defining a problem, rather than a solution is to begin the statement of the requirement with the phrase “we need the capability to ...” It’s nearly impossible to complete this sentence with a solution (“a wall”), and much easier to complete the sentence with a problem (“capability to detect intruders”). Capability gaps and requirements should address what a system should do, rather than how to do it. This approach is sometimes called capability-based planning. It is a very simple, yet powerful concept.

Properly defining clear and concise capability gaps is a necessary first step in product realization. This high-level understanding of a problem is a key part in the communication of needs. One may find that capability gaps are oftentimes common across multiple cross-sections of DHS operating components and supporting elements such as the first responder community and private sector critical infrastructure owner/operators. Discovering these commonalities is a fundamental aspect of the DHS S&T Capstone IPT Process, which seeks to reduce duplication of efforts and expedite product transition. See Appendix B for further information.

## Why Requirements?

A *requirement* is an attribute of a product, service or system necessary to produce an outcome(s) that satisfies the needs of a person, group or organization. Requirements therefore define “the problem.” In contrast, “the solution” is defined by technical *specifications*.

Defining requirements is the process of determining what to make before making it. Requirements definition creates a method in which appropriate decisions about product or system functionality and performance can be made before investing the time and money to develop it. Understanding requirements early removes a great deal of guesswork in the planning stages and helps to ensure that the end-users and product developers are “on the same page.”

Requirements provide criteria against which solutions can be tested and evaluated. They offer detailed metrics that can be used to objectively measure a possible solution’s effectiveness, ensuring informed purchasing decisions on products, systems or services that achieve the stated operational goals. A detailed requirements analysis can uncover hidden requirements as well as discover common problems across programs and various DHS operating components. Detailed operational requirements will guide product development so that solutions specifications actively solve the stated problems.

We could save ourselves a lot of work if we jump straight to “the solution” without defining “the problem.” Why don’t we do that? Because if we take that shortcut we are likely to find that our solution may not be the best choice among possible alternatives or, even worse we’re likely to find that our “solution” doesn’t even solve the problem!

Defining requirements and adhering to developing solutions to address those needs is often referred to as “requirements-pull.” In this situation, user requirements drive product development and guide the path forward as the requirements dictate. This is a powerful circumstance in which fulfilling requirements becomes the central focus of product development and no possible solution is disregarded given it facilitates

At the other extreme from the “requirements-pull”, approach is its opposite: “technology push.” Here we start with a solution (perhaps a new technology) and see what problems it might enable us to solve. The danger in this approach is to become enamored of “the solution” and neglect to ensure that it actually solves a problem. With technology push, it is likely that actual user requirements may be modified, or even ignored in order to “force-fit” the desired solution. A historical example was the product known as Picture Phone introduced (and discontinued) in the 1960s when the advance of telecommunications technology first made possible the transmission and display of video as well as voice. Picture Phone, which allowed telephone users to see each other during a call, was a technological success but a market disaster. It turned out that callers generally didn’t want to be seen, as a bit of unbiased market analysis would have disclosed. Clearly, this aversion has changed in modern times with the advent of video-conferencing and web chatting capabilities. The Picture Phone example still shows that technology must be accepted by a potential user community to establish a need and allow for the development of markets willing to purchase and use new technology.

Technology push should not be ignored, but if the goal is successful transition to the field with acceptable risk, the technology being pushed must be compared with alternative solutions against a real set of user requirements.

Aside from assuring that the “solution” actually solves the “problem,” requirements-driven design has a further advantage in that the requirements provide criteria against which a product’s successful development can be measured. Specifically, if the product was developed to address a set of quantified operational requirements, then its success is measured by Operational Test and Evaluation (OT&E) to validate that an end-user can use the product and achieve the stated operational goals.

Prior to OT&E, it is common practice to subject products to Developmental Test and Evaluation (DT&E). The purpose of DT&E is to verify that the product meets its technical specifications, which are the engineers’ interpretation of the operational requirements. Such DT&E does not obviate the need for OT&E, which validates that the engineers’ solution is not only technically successfully but also represents a successful interpretation of the end users’ needs, satisfying the original operational requirements (not just the technical specifications) when operated by representative users.

Often requirements are stated in terms of “threshold values” and “objective values,” where the “objective value” is the desired performance and the “threshold value” is the minimum acceptable performance. This formalism is useful in allowing stretch goals to be asserted without saddling the system development with unacceptable risk.

### **The Requirements Hierarchy and Traceability**

To reiterate the definitions above, the documents that govern product realization include requirements, which define the problem, and specifications, which define the solution. Nevertheless, the hierarchy of requirements and specifications is more complex than that simple dichotomy, as depicted in Figure 3.

The hierarchy is divided into two domains, operational requirements and technical requirements, highlighted in yellow and blue in the figure, representing the “problem space” and the “solution space” respectively. The DHS Operating Component, representing the end users in the field (the operators), is responsible for all operational requirements, from the top-level mission requirements to the detailed system-level operational requirements. A system developer is responsible for translating the operational requirements into a system solution, documented in a hierarchy of technical specifications.

# Requirements Hierarchy

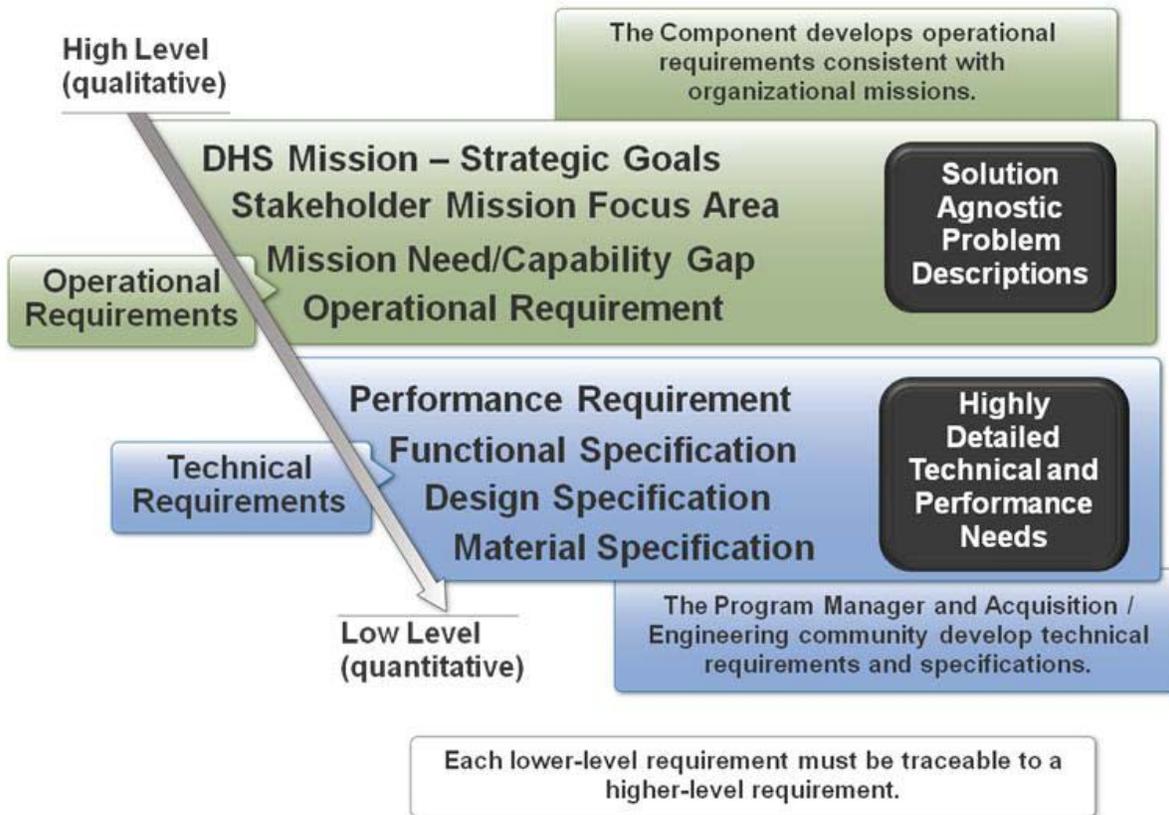


Figure 3 The Requirements Hierarchy

The highest-level type of technical “specification” is actually called a performance “requirement.” A performance requirement actually represents a bridge from operational requirements to the engineering interpretation of those requirements. Put another way, in the course of developing a new system it is necessary to transform the system operational requirements, which are stated from a given Operating Component’s perspective as required outcomes of system action, into a set of system performance requirements, which are stated in terms of engineering characteristics.

Working through the requirements hierarchy, requirements development is the process of decomposing the problems broadly outlined in the capability gaps gleaned from the mission needs assessment.

The requirements and specifications are described below, first those that define the problem and then those that define the solution:

- **Problem Definition**

- **Mission Needs Statement (MNS)** is required by the DHS *Acquisition Review Process* (Management Directive 102-01, Interim) and is developed by the DHS sponsor (S&T's customer) who represents the end users. The MNS provides a high-level description of the mission need (or, equivalently, capability gap), and is used to justify the initiation of an Acquisition program.
- **5W** is a template that outlines general problem descriptions that answer the "Who, What, When, Where, and Why" questions. The 5W begins to explore potential users and establishes initial timelines for when a capability is needed.
- **Detailed Capability Gap** expands on the MNS and describes specific needs-based evaluations for necessary capabilities aligned to a stakeholder mission focus. Includes general CONOPS and target performance.
- **Operational Requirements Document (ORD)** is also required by the DHS *Acquisition Review Process* and, like the MNS, is developed by the DHS sponsor. The ORD specifies operational requirements and a concept of operations (CONOPS), written from the point of view of the end user. The ORD is independent of any particular implementation, should not refer to any specific technologies and does not commit the developers to a design.

- **Solution Definition**

- **Performance Requirements** represent a bridge between the operationally oriented view of the system defined in the ORD and an engineering-oriented view required to define the solution. Performance requirements are an interpretation, not a replacement of operational requirements. Performance requirements define the functions that the system *and its subsystems* must perform to achieve the operational objectives and define the performance parameters for each function. These definitions are in engineering rather than operational terms.
- **Functional Specifications** define the system solution functionally, though not physically. Sometimes called the "system specification" or "A-Spec," these specifications define functions at the system, subsystem, *and component level* including:
  - Configuration, organization, and interfaces between system elements
  - Performance characteristics and compatibility requirements
  - Human engineering
  - Security and safety
  - Reliability, maintainability and availability
  - Support requirements such as shipping, handling, storage, training and special facilities
- **Design Specifications** convert the functional specifications of *what* the system is to do into a specification of *how* the required functions are to be implemented in hardware and software. The design specifications therefore govern the materialization of the system components.
- **Material Specifications** are an example of lower-level supporting specifications that support the higher-level specifications. Material specifications define the required properties of materials and parts used to fabricate the system. Other supporting

specifications include **Process Specifications** (defining required properties of fabrication processes such as soldering and welding) and **Product Specifications** (defining required properties of non-developmental items to be procured commercially).

Building on the concept of the Requirements Hierarchy is the understanding that greater detail of information is necessary to bring increased clarity and definition for each lower-level/higher-resolution requirement. The Requirements Hierarchy can be thought of as a series of lenses that focus energy like a laser and bring increasingly actionable knowledge through each phase. The enhanced understanding gained from each lower-level requirement also improves the potential quality of output given this greater insight. The quality of output is directly related to the detail of input. Figure 4 demonstrates simply that the greater breadth and depth of information can yield improved output through actionable knowledge.

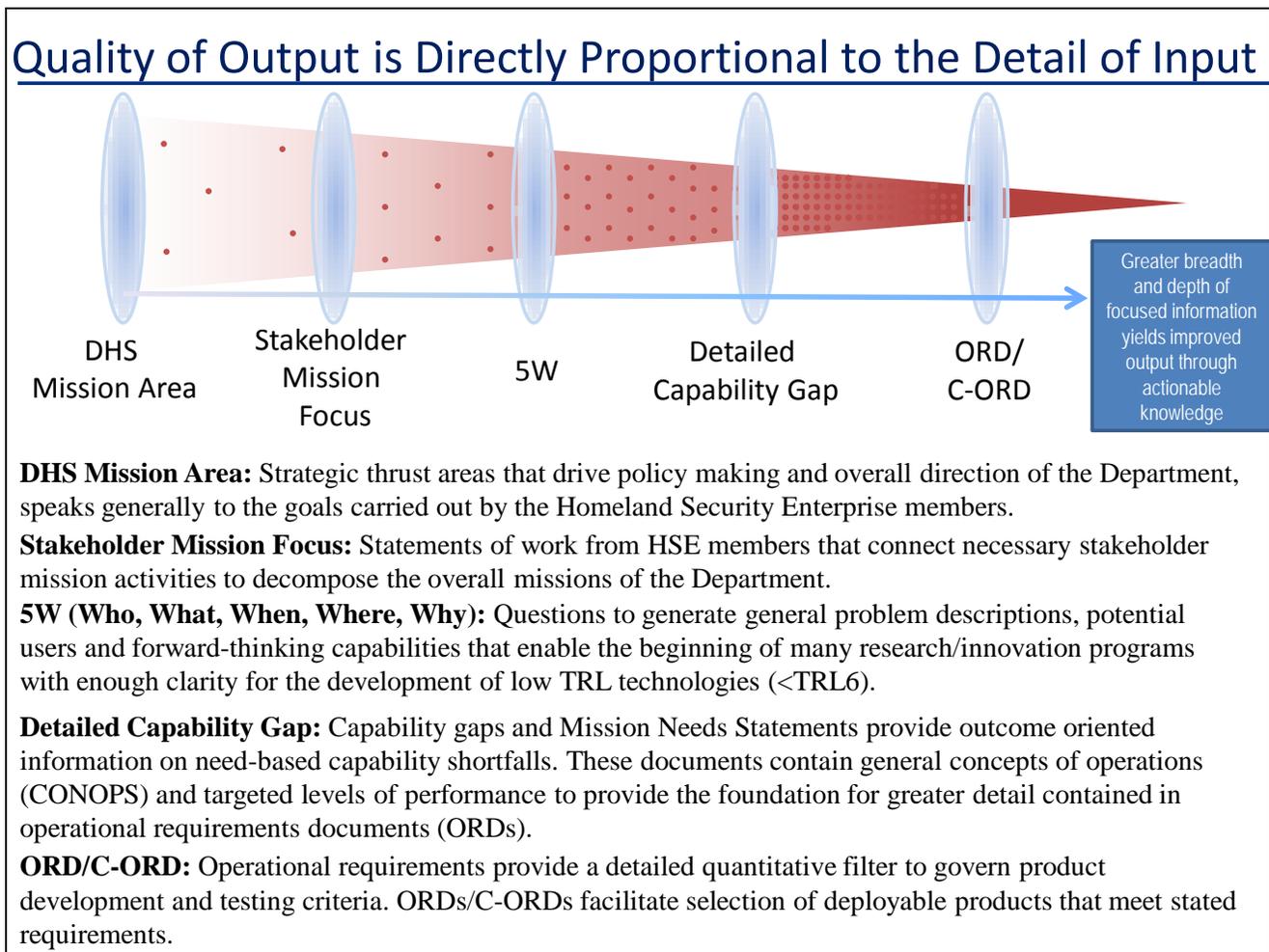


Figure 4 Requirements documentation “lenses” focus efforts and increase the quality outputs.

## Characteristics of Good Requirements

Requirements engineering is difficult and time-consuming, but must be done well if the final product or system is to be judged by the end users as successful. From the International Council of Systems Engineers (INCOSE) Requirements Working Group<sup>1</sup>, here are eight attributes of good requirements:

- Necessary: Can the system meet prioritized, real needs without it? If yes, the requirement isn't necessary.
- Verifiable: Can one ensure that the requirement is met in the system? If not, the requirement should be removed or revised.
- Unambiguous: Can the requirement be interpreted in more than one way? If yes, the requirement should be clarified or removed. Ambiguous or poorly worded requirements can lead to serious misunderstandings and needless rework.
- Complete: Are all conditions under which the requirement applies stated? In addition, does the specification include all known requirements?
- Consistent: Can the requirement be met without conflicting with any other requirement? If not, the requirement should be revised or removed.
- Traceable: Is the origin (source) of the requirement known, and is there a clear path from the requirement back to its origin?
- Concise: Is the requirement stated simply and clearly?
- Standard constructs: Requirements are stated as imperative needs using "shall." Statements indicating "goals" or using the words "will" or "should" are not imperatives.

## Developing Operational Requirements (ORDs): Customer Input

So far, we've discussed operational requirements but have not provided any insight into how to develop them. In an effort to provide a basic framework for the articulation and documentation of operational requirements, the Operational Requirements Document (ORD) was created. ORDs provide a clear definition and articulation of a given problem, providing several layers of information that comprise the overall problem. Using resources such as this book and the accompanying template, we have tried to simplify and streamline the process of communicating requirements. ORDs can be used in Acquisition, Procurement, Commercialization and Outreach Programs –any situation that dictates detailed requirements (e.g. RFQ, BAA, RFP, RFI, etc.). It's clear to see that it's cost-effective and efficient for both DHS and all of its stakeholders to communicate needs clearly and effectively.

---

<sup>1</sup> Kar, Pradip and Bailey, Michelle. Characteristics of Good Requirements. International Council of Systems Engineers, Requirements Working Group. INCOSE Symposium, 1996. Found online: <http://www.afis.fr/nav/gt/ie/doc/Articles/CHARACTE.HTM>.

Let's first look at the contents of a typical Operational Requirements Document (ORD) shown in Figure 5.

***OPERATIONAL REQUIREMENTS DOCUMENT***

- 1.0 General Description of Operational Capability
  - 1.1. Capability Gap
  - 1.2. Overall Mission Area Description
  - 1.3. Description of the Proposed System
  - 1.4. Supporting Analysis
  - 1.5. Mission the Proposed System Will Accomplish
  - 1.6. Operational and Support Concept
    - 1.6.1. Concept of Operations
    - 1.6.2. Support Concept
- 2.0 Threat
- 3.0 Existing System Shortfalls
- 4.0 Capabilities Required
  - 4.1 Operational Performance Parameters
  - 4.2 Key Performance Parameters (KPPs)
  - 4.3 System Performance
    - 4.3.1 Mission Scenarios
    - 4.3.2 System Performance Parameters
    - 4.3.3 Interoperability
    - 4.3.4 Human Interface Requirements
    - 4.3.5 Logistics and Readiness
    - 4.3.6 Other System Characteristics
- 5.0 System Support
  - 5.1 Maintenance
  - 5.2 Supply
  - 5.3 Support Equipment
  - 5.4 Training
  - 5.5 Transportation and Facilities
- 6.0 Force Structure
- 7.0 Schedule
- 8.0 System Affordability
- Appendixes
- Glossary

**Figure 5. The contents of an Operational Requirements Document**

The complexity of the intended system and its operational context will govern the required level of detail in the ORD. The most difficult sections to develop are probably Section 4.0, which describes the

capabilities required of the system to be developed, and Section 1.6, which describes the operational and support concepts.

There is no “silver bullet” to solve the potential challenges in developing an ORD, but since the issues are universal, there is a wealth of literature that offers approaches to requirements development. As an example, here are nine requirements-elicitation techniques described in the *Business Analyst Body of Knowledge* (from the International Institute of Business Analysis)<sup>2</sup>.

1. Brainstorming
  - Purpose
    - An excellent way of eliciting many creative ideas for an area of interest. Structured brainstorming produces numerous creative ideas.
  - Strengths
    - Able to elicit many ideas in a short time period.
    - Non-judgmental environment enables outside-the-box thinking.
  - Weaknesses
    - Dependent on participants’ creativity.
2. Document Analysis
  - Purpose
    - Used if the objective is to gather details of the “As Is” environment such as existing standard procedures or attributes that need to be included in a new system.
  - Strengths
    - Not starting from a blank page.
    - Leveraging existing materials to discover and/or confirm requirements.
    - A means to crosscheck requirements from other elicitation techniques such as interviews, job shadowing, surveys or focus groups.
  - Weaknesses
    - Limited to “as-is” perspective.
    - Existing documentation may not be up-to-date or valid.
    - Can be a time-consuming and even tedious process to locate the relevant information.
3. Focus Group
  - Purpose
    - A means to elicit ideas and attitudes about a specific product, service or opportunity in an interactive group environment. The participants share their impressions, preferences and needs, guided by a moderator.
  - Strengths
    - Ability to elicit data from a group of people in a single session saves time and costs as compared to conducting individual interviews with the same number of people.
    - Effective for learning people’s attitudes, experiences and desires.

---

<sup>2</sup> International Institute of Business Analysis. *A Guide to the Business Analyst Body of Knowledge*, Release 1.6. 2006. Found online: [http://www.theiiba.org/Content/NavigationMenu/Learning/BodyofKnowledge/Version16/BOKV1\\_6.pdf](http://www.theiiba.org/Content/NavigationMenu/Learning/BodyofKnowledge/Version16/BOKV1_6.pdf).

- Active discussion and the ability to ask others questions creates an environment where participants can consider their personal view in relation to other perspectives.
- Weaknesses
  - In the group setting, participants may be concerned about issues of trust, or may be unwilling to discuss sensitive or personal topics.
  - Data collected (what people say) may not be consistent with how people actually behave.
  - If the group is too homogenous, the group's responses may not represent the complete set of requirements.
  - A skilled moderator is needed to manage the group interactions and discussions.
  - It may be difficult to schedule the group for the same date and time.
- 4. Interface Analysis
  - Purpose
    - An interface is a connection between two components. Most systems require one or more interfaces with external parties, systems or devices. Interface analysis is initiated by project managers and analysts to reach agreement with the stakeholders on what interfaces are needed. Subsequent analysis uncovers the detailed requirements for each interface.
  - Strengths
    - The elicitation of the interfaces' functional requirements early in the system life cycle provides valuable details for project management:
      - Impact on delivery date. Knowing what interfaces are needed, their complexity and testing needs enables more accurate project planning and potential savings in time and cost.
      - Collaboration with other systems or projects. If the interface to an existing system, product or device and the interface already exist, it may not be easily changed. If the interface is new, then the ownership, development and testing of the interface needs to be addressed and coordinated in both projects' plan. In either case, eliciting the interface requirements will require negotiation and cooperation between the owning systems.
  - Weaknesses
    - Does not provide an understanding of the total system or operational concept since this technique only exposes the inputs, outputs and key data elements related to the interfaces.
- 5. Interview
  - Purpose
    - A systematic approach to elicit information from a person or group of people in an informal or formal setting by asking relevant questions and documenting the responses.
  - Strengths
    - Encourages participation and establishes rapport with the stakeholder.
    - Simple, direct technique that can be used in varying situations.
    - Allows the interviewer and participant to have full discussions and explanations of the questions and answers.
    - Enables observations of non-verbal behavior.

- The interviewer can ask follow-up and probing questions to confirm own understanding.
- Maintain focus using clear objectives for the interview that are agreed upon by all participants and can be met in the time allotted.
- Weaknesses
  - Interviews are not an ideal means of reaching consensus across a group of stakeholders.
  - Requires considerable commitment and involvement of the participants.
  - Training is required to conduct good interviews. Unstructured interviews, especially, require special skills. Facilitation/virtual facilitation and active listening are a few of them.
  - Depth of follow-on questions may be dependent on the interviewer's knowledge of the operational domain.
  - Transcription and analysis of interview data can be complex and expensive.
  - Resulting documentation is subject to interviewer's interpretation.
- 6. Observation
  - Purpose
    - A means to elicit requirements by assessing the operational environment. This technique is appropriate when documenting details about current operations or if the project intends to enhance or change a current operational concept.
  - Strengths
    - Provides a realistic and practical insight into field operations by getting a hands-on feel for current operations.
    - Elicits details of informal communication and ways people actually work around the system that may not be documented anywhere.
  - Weaknesses
    - Only possible for existing operations.
    - Could be time-consuming.
    - May be disruptive to the person being shadowed.
    - Unusual exceptions and critical situations that happen infrequently may not occur during the observation.
    - May not well work if current operations involve a lot of intellectual work or other work that is not easily observable.
- 7. Prototyping
  - Purpose
    - Prototyping, when used as an elicitation technique, aims to uncover and visualize user requirements before the system is designed or developed.
  - Strengths
    - Supports users who are more comfortable and effective at articulating their needs by using pictures or hands-on prototypes, as prototyping lets them "see" the future system's interface.
    - A prototype allows for early user interaction and feedback.

- A throwaway prototype is an inexpensive means to quickly uncover and confirm user interface requirements.
  - A revolutionary prototype can demonstrate what is feasible with existing technology, and where there may be technical gaps.
  - An evolutionary prototype provides a vehicle for designers and developers to learn about the users' interface needs and to evolve system requirements.
  - Weaknesses
    - Depending on the complexity of the target system, using prototyping to elicit requirements can take considerable time if the process is bogged down by the "how's" rather than "what's".
    - Assumptions about the underlying technology may need to be made in order to present a starting prototype.
    - A prototype may lead users to set unrealistic expectations of the delivered system's performance, reliability and usability characteristics.
8. Requirements Workshop
- Purpose
    - A requirements workshop is a structured way to capture requirements. A workshop may be used to scope, discover, define, prioritize and reach closure on requirements for the target system. Well-run workshops are considered one of the most effective ways to deliver high quality requirements quickly. They promote trust, mutual understanding, and strong communications among the project stakeholders and project team, produce deliverables that structure, and guide future analysis.
  - Strengths
    - A workshop can be a means to elicit detailed requirements in a relatively short period of time.
    - A workshop provides a means for stakeholders to collaborate, make decisions and gain a mutual understanding of the requirements.
    - Workshop costs are often lower than the cost of performing multiple interviews.
    - A requirements workshop enables the participants to work together to reach consensus which is typically a cheaper and faster approach than doing serial interviews as interviews may yield conflicting requirements and the effort needed to resolve those conflicts across all interviewees can be very costly.
    - Feedback is immediate, if the facilitator's interpretation of requirements is fed back immediately to the stakeholders and confirmed.
  - Weaknesses
    - Due to stakeholders availability it may be difficult to schedule the workshop.
    - The success of the workshop is highly dependent on the expertise of the facilitator and knowledge of the participants.
    - Requirements workshops that involve too many participants can slow down the workshop process thus negatively affecting the schedule. Conversely, collecting input from too few participants can lead to overlooking requirements that are important to users, or to specifying requirements that do not represent the needs of the majority of the users.

## 9. Survey/Questionnaire

- Purpose
  - A means of eliciting information from many people, anonymously, in a relatively short time. A survey can collect information about customers, products, operational practices and attitudes. A survey is often referred to as a questionnaire.
- Strengths
  - When using ‘closed-ended’ questions, effective in obtaining quantitative data for use in statistical analysis.
  - When using open-ended questions, the survey results may yield insights and opinions not easily obtainable through other elicitation techniques.
  - Does not typically require significant time from the responders.
  - Effective and efficient when stakeholders are not located at one place.
  - May result in large number of responses.
  - Quick and relatively inexpensive to administer.
- Weaknesses
  - Use of open-ended questions requires more analysis.
  - To achieve unbiased-results, specialized skills in statistical sampling methods are needed when the decision has been made to survey a sample subset.
  - Some questions may be left unanswered or answered incorrectly due to their ambiguous nature.
  - May require follow up questions or more survey iterations depending on the answers provided.
  - Not well suited for collecting information on actual behaviors.

### Addressing Requirements versus Proposing Solutions

When employing efforts to elicit and explain requirements using any of these methods, it is imperative to steadfastly avoid requirements that define potential solutions or otherwise restrict the potential solution space. While it is necessary and useful to understand the current state-of-the-art within a given technology space and knowledge about potential solutions that may already be in development, requirements are meant to simply define problems. Properly drafted requirements allow for a variety of solutions, each with their own advantages and disadvantages, to be considered as potential ways to address a problem. Solution-agnostic requirements prevent limiting and defining the outcome of product realization. Within the context of the Operational Requirements Document Template described in detail below, the solution definition aspect of the Requirements Hierarchy is purposefully not addressed.

This is useful given that an open and honest review of one’s needs might show that a preconceived notion about a desired solution may turn out not to be the best solution, or that modifications to existing products or services may be necessary and useful to end users.

## If You Can't Measure It, You Can't Manage It

Requirements provide additional benefits for the execution of programs and projects in an accurate and quantifiable manner. Requirements definition establishes the performance parameters necessary to evaluate the effectiveness of a given solution. The formation of metrics based on developed requirements to measure achievement is critical in establishing the viability of a potential solution and determining the ability for a potential solution to satisfy a capability need. Requirements create the foundation for developing critical evaluation tools and documents such as detailed test plans for both laboratory and operational environments. Detailed test plans greatly enhance the evaluation process and ensure that a common testing protocol is followed making the review of test and evaluation data straightforward and coherent. It certainly takes a collaborative effort between users, developers and evaluators throughout the entire requirements and testing development process to bring everyone onto the same page, but the benefits of efficient and effective product development and evaluation will pay off greatly in the long run.

Beyond their benefit to measure effective product development, the use of metrics in an organization is equally important. Strategically, an organization can use metrics for planning and measuring progress against goals. There are several ways to define metrics that can be used in an organization and varying levels of detail, much the same way that requirements can gain additional clarity moving from a capability gap to a detailed operational requirement. *Performance objectives* are general statements of the desired achievement, and a *performance goal* is a specific statement of the desired level of achievement. Performance objectives are broad statements, such as “improve communication with the private sector,” whereas performance goals are specific and measurable, such as “increase applications received from small businesses by 15% over the previous year.”

The SMART test is frequently used to provide a quick reference to determine the quality of a particular performance metric:

**S = Specific:** clear and focused to avoid misinterpretation. Should include measure assumptions and definitions and be easily interpreted.

**M = Measurable:** can be quantified and compared to other data. It should allow for meaningful statistical analysis. Avoid "yes/no" measures except in limited cases, such as start-up or systems-in-place situations.

**A = Attainable:** achievable, reasonable, and credible under conditions expected.

**R = Realistic:** fits into the organization's constraints and is cost-effective.

**T = Timely:** doable within the time frame given.

Establishing performance goals enables the use of management tools for planning and evaluation about the effectiveness of a team and its subcomponents through defined Objectives, Strategies and Tactics or OST. An OST is a simple and effective way to capture on one page the functions and activities that will guide an organization to achieve its mission.

## It All Starts with a Plan... Objectives, Strategies and Tactics

<p><u>Objectives</u></p> <ol style="list-style-type: none"> <li>1.</li> <li>2.</li> <li>3.</li> </ol>	<p><u>Strategies</u></p> <ol style="list-style-type: none"> <li>1.</li> <li>2.</li> <li>3.</li> <li>4.</li> <li>5.</li> </ol>
<p><u>Tactical Elements</u></p> <ol style="list-style-type: none"> <li>1.</li> <li>2.</li> <li>3.</li> <li>4.</li> <li>5.</li> <li>6.</li> <li>7.</li> <li>8.</li> <li>9.</li> <li>10.</li> </ol>	

**Figure 6** The Objectives, Strategies and Tactics tool is an effective means to plan, track and communicate the direction and activities necessary to achieve mission success.

### **Objectives**

In the OST model, an organization outlines its three to four major objectives. There should be typically no more than 4 objectives for any organization and all objectives shall keep in mind the SMART test so that objectives are measurable and contain a due date or deadline. These objectives may contain both short-term and long-term goals for an organization. Defined objectives should keep in mind overarching mission goals and maintain alignment to the overall direction for the organization as a whole and how individual components work together and support each other.

### **Strategies**

In order to breakdown the major activities necessary to meet objectives, a series of strategies are laid out for the stated objectives. There is not necessarily a 1:1 correlation between strategies and objectives, and oftentimes strategies can support multiple objectives to create cohesiveness between all activities that collectively support the overall mission. Strategies do not necessarily need to pass the SMART test but it is important to maintain traceability to the objectives.

### **Tactics/Tactical Elements**

Having established what an organization intends to accomplish in its objectives and strategies, defining the tactics addresses the individual actions taken to achieve a larger purpose. There will be several tactics used to achieve the objectives and strategies. These tactics will focus on the daily operations and plan how each activity will advance the accomplishment of organizational objectives.

The OST tool is used extensively throughout the R&D Partnerships Group for many reasons. First and foremost, OSTs are useful in ensuring that all offices within the group have clearly defined missions and a plan to go about executing those missions. Additionally, OSTs serve as a communications tool to share between offices and improve the understanding and awareness that offices have of their counterparts to break down barriers and create opportunities for teamwork and cooperation. Lastly, the OSTs provide management with an easy-to-use format for monitoring activities, planning mission execution and measuring the contributions of each office to overall mission success.

## Meet the R&D Partnerships Group: A Focused Team Approach

We know what you're thinking – “team approach” in the federal government? Your experience has likely been that “the left hand doesn't know what the right hand is doing” or you hear “my group, my organization, etc.” You'll be pleasantly surprised to learn that the R&D Partnerships Team is a real team where “us, we, our, together and join” are more common vocabulary. Everything we do is done with the knowledge of what others are doing in a given area or field. We communicate regularly with members to understand what we're all working on. We develop our models, methods, surveys, etc. as a team to give everyone the opportunity to share their ideas and voice their opinions. We make consensus-based decisions in a timely manner knowing that the speed-of-execution is just as important as the execution itself.

Resources are focused where they should be – at the “front line” interface serving our potential partners. You depend on us to provide accurate information and we depend on you to use your resources to genuinely assist us in solving problems – working together to deploy products, services, systems and/or technologies to keep our homeland safe. It is our goal to dedicate the resources and time to those who work most closely with our Homeland Security Enterprise partners and equip them with the knowledge and tools that will create effective and clear communication that will help the R&D Partnerships Group solve real world problems with a speed-of-execution and quality of output that makes a high impact in securing our nation. Appendix A contains the R&D Partnerships Opportunities Guide which describes the various ways that each office within the group is “open for business.”



Figure 7 Pushing resources to the "front lines" increases interaction with our HSE partners and ensures that energies are spent where they can provide the most good to as many partners as possible.

## Office of National Labs

The Office of National Labs (ONL) supports the development of fundamental scientific knowledge to meet future homeland security challenges. ONL interacts with partners across the nation in an effort to harness shared expertise, resources and knowledge while conducting and supporting scientific discoveries and inventions relevant to existing and emerging homeland security needs.

Title III of *The Homeland Security Act* (2002) establishes the Office of National Laboratories (ONL) within the Science and Technology Directorate. ONL meets this responsibility through the coordination and utilization of the Department of Energy National Laboratories and other scientific research sites. ONL coordinates with DHS components and laboratories to successfully identify and transfer homeland security technologies and capabilities to state, local and tribal governments and the private sector. In addition, the Office of National Labs has the responsibility to provide the operations and facility funding for the Department of Homeland Security S&T laboratories where scientists perform mission-critical research on biological and agricultural safety, chemical analysis, and post-event biological and chemical forensics. ONL is organized into three branches which together ensure effective construction, stewardship, and utilization of current S&T labs as well as pursuing development of enduring infrastructures dedicated to the homeland security mission.

The Director of the Office of National Laboratories is Mr. James Johnson.

### **Construction Branch**

This branch oversees the planning, budgeting, and management of DHS S&T's laboratory construction and infrastructure upgrade projects. The team performs environmental impact studies, risk assessments and other applicable site-specific evaluations. Infrastructure in this context refers to the physical buildings and facilities that house laboratory research, development, test, and evaluation work that supports the broader goals of the Department of Homeland Security Science and Technology Directorate. Construction projects provide space for and maintain research and development (R&D) capabilities to support the missions of the S&T Directorate, the Department, and other government agencies that have interrelated homeland security missions such as the Department of Agriculture (USDA), Department of Health and Human Services (HHS), and Department of Defense (DoD). The Office of National Labs' construction investments include the construction of future assets, where a current capability does not exist, and upgrades to extend the life or expand capabilities of present laboratory facilities.

The branch uses leading edge management practices and focuses on providing superior oversight of strategic agency and program goals in the context of project objectives and key performance parameters. The branch has developed a Project Management Manual which is used by project managers and their teams to run all infrastructure projects. The Lead for the Infrastructure Branch is Ms. Julie Brewer (Acting).

## **Operations Branch**

The Operations Branch within the Office of National Labs is the operations point of contact for six S&T field labs. The operations function ensures that the labs have the resources they need for safe, secure, and compliant management and operations under federal, state, and local laws/regulations and DHS policies and Management Directives, while still maintaining the mission needs. The operations resources span areas such as the availability of proper space, maintenance and operations of physical structures, required staffing to maintain the facilities and conduct the core research, business execution and budget planning, health and safety safeguards, physical security, and IT systems and security. The Operations Branch also works with other government agencies to ensure infrastructure support needs are maintained for S&T labs that require such assistance.

The laboratory buildings must be maintained and operated efficiently to meet the current missions. As DHS' and the S&T Labs' missions evolve to meet new threats and emerging requests, the Operations Branch builds new requirements into the five year Federal budget process in order to plan and prioritize any necessary physical changes or upgrades to facilities, buildings and internal systems. Changing requirements can mean adding to or upgrading existing facilities, altering staffing levels and also closing a facility according to all legal and environmental requirements.

The purpose of the DHS S&T Labs is to combat the hazards that threaten security in the homeland and to provide direct engineering and scientific support (e.g., forensics) to the DHS Operational Components and other Federal Agencies. Much of this mission requires that the Labs maintain 24x7 operations. The ONL Operations Branch is responsible for ensuring the continuity of operations for the labs under all circumstances.

## **Biosafety and Biosecurity (Biosurety)**

DHS owns and operates two biocontainment laboratories, the Plum Island Animal Disease Center (PIADC) and the National Biodefense Analysis and Countermeasures Center (NBACC). Both PIADC and NBACC have developed facility-wide policies and operating procedures pertaining to biosafety, biosecurity, agent accountability, and personnel reliability. Biosurety requirements ensure compliance with the Select Agents regulations; create an operational environment where work with biological select agent and toxins (BSAT) is conducted in a safe, secure and reliable manner; and identify roles and responsibilities of all individuals in establishing safe management practices and biosurety standards for the protection of BSAT.

The DHS Science and Technology (S&T) Directorate is responsible for ensuring Department-wide compliance with DHS policies for Biosafety and Select Agents and Toxin Security, and for overseeing the management and operation of PIADC and NBACC. The DHS Regulatory and Compliance Office (RCO) supports S&T and the Office of National Labs in providing guidance for policy implementation and compliance at DHS biocontainment facilities and institutions conducting DHS-sponsored biological R&D activities. The RCO also conducts biosafety and biosecurity reviews of these facilities and activities under the direction of the S&T Office of General Counsel (OGC)

As part of the biosurety program, DHS has implemented departmental policies and assigned responsibilities for DHS-sponsored biological R&D activities. The policies adopt and require DHS-sponsored activities involving biological agents to comply with current federal regulations, guidelines,

and policies including the Select Agent Regulations (7 CFR 331, 9 CFR 121, 42 CFR 72 &73), the most current edition of the *Biosafety in Microbiological and Biomedical Laboratories* (BMBL) and the *NIH Guidelines for Research Involving Recombinant DNA Molecules* (NIH Guidelines) as appropriate. The Instruction Handbook for DHS Personnel Suitability (121-01-007) serves a general role in personnel reliability across the Department by establishing screening requirements and processes for all individuals who require unescorted access to DHS-owned facilities, or commercial facilities operating on behalf of DHS.

DHS S&T, including ONL and other DHS components (Office of Health Affairs, Policy, and the Office of Infrastructure Protection in the National Protection and Programs Directorate), have actively participated in interagency deliberations regarding laboratory biosafety, biosecurity, and biosurety over the last two years, and are engaged in ongoing biosurety policy development processes.

The Lead for the Operations Branch is Mr. Jim Helt.

S&T Laboratory	Reports To	Operations and Management (Including Resources) by
National Biodefense Analysis and Countermeasures Center (NBACC)	Director, Office of National Labs	ONL
Plum Island Animal Disease Center (PIADC)	Director, Office of National Labs	ONL
National Bio and Agro-Defense Facility (NBAF)	Director, Office of National Labs	ONL
Chemical Security Analysis Center (CSAC)	Director, Chemical and Biological Division	ONL
Transportation Security Laboratory (TSL)	Director, Test and Evaluation Standards Office	ONL
National Urban Security Technology Laboratory (NUSTL)	Director, Support to the Homeland Security Enterprise and First Responders	ONL

Figure 8 Alignment of the Six S&T Labs

### C. Utilization Branch

Laboratory Utilization and R&D Coordination focuses on the effective use of Department of Energy National Laboratories and S&T in-house laboratories for research, technology transition, and test and evaluation activities to meet homeland security challenges. At the same time, the Utilization Branch identifies research programs at DOE for potential applications that will meet and accelerate DHS required technology and future transition.

#### - Managing S&T’s Strategic Partnerships with National Labs

The Utilization team develops program and policies for the effective use of National Laboratories by DHS and for their performance of specific-assigned DHS work. These policies and strategies address how DHS uses labs as Federally Funded Research and Development Centers (FFRDCs) and takes advantage of their core capabilities. At the same time, Utilization is critically involved in helping to set the National Labs’ research agendas, assuring the continuity of critical laboratory capabilities, and involving the Labs in DHS strategic deliberations.

## - **Providing Strategy and Guidance**

The Utilization team assists the Director of ONL and other S&T and DHS principals in strategic planning. Once research priorities are set, the Utilization team coordinates the process for selecting the appropriate laboratory to perform the work, and oversees strategic alignment and engagement of DOE labs with the technical divisions within S&T. Utilization also conducts annual laboratory performance assessments for internal S&T and external labs that conduct work for S&T and DHS. The Utilization Lead also represents S&T/ONL on technology and science interagency working groups.

The Lead for the Utilization Branch is Mr. Don Kirkley.

## **Overview of DHS S&T Laboratories**

### **A. National Biodefense Analysis and Countermeasures Center (NBACC)**

The National Biodefense Analysis and Countermeasures Center (NBACC) applies science to challenges critical to defending the nation against bioterrorism. The first laboratory built specifically for DHS, it is a resource for understanding the risks posed by biological threats and their transformation into bioterrorism or biocrime events. Located in Maryland, the NBACC comprises two centers: The National Bioforensic Analysis Center (NBFAC), which conducts technical forensic analyses following an attack, and the Biological Threat Characterization Center (BTCC), which conducts experiments and studies to learn more about current and future biological events. The laboratory is managed by the Battelle National Biodefense Institution in support of DHS. Total staff is approximately 125 FTE.

### **B. Plum Island Animal Disease Center (PIADC)**

For more than a half century, the Plum Island Animal Disease Center (PIADC) has served as the front line of the nation's defense against diseases that could devastate markets for livestock, meat, and other animal products. Located off the tip of Long Island, the lab's mission crosses three areas: diagnostics, research and development, and education. PIADC is capable of diagnosing foreign animal diseases. Its research programs include developing new diagnostic tools and preventatives (such as vaccines and antivirals) for foot-and-mouth and other foreign animal diseases. Since 1971, it has provided training to veterinarians on how to recognize foreign animal diseases. PIADC is currently undergoing upgrades to maintain safety and security, and to provide additional near-term capacity for research. Total staff is approximately 300 FTE.

### **C. National Bio and Agro-Defense Facility (NBAF)**

The National Bio and Agro-Defense Facility (NBAF) will provide an integrated facility to study foreign animal, emerging and zoonotic (transmitted from animals to humans) diseases that affect large livestock. The NBAF will be equipped with modern, integrated high-security, biosafety level (BSL) 3 and 4 facilities to safely and effectively address the accidental or intentional introduction of animal diseases of high consequence into the United States, such as foot-and-mouth disease (FMD). The facility will conduct research for the specific purposes of improving diagnostic tests, developing effective vaccines and other countermeasures, and enhancing rapid response capacity. The NBAF will be located in Manhattan, Kansas, and will serve as a replacement for the facilities at the Plum Island Animal Disease Center (PIADC). Total planned staff is approximately 350 FTE.

### **D. Chemical Security Analysis Center (CSAC)**

The Chemical Security Analysis Center (CSAC) provides a scientific basis for the awareness of chemical threats and the attribution of their use. From its facility in Maryland, CSAC draws upon expertise in chemical defense, chemical agents, and toxic industrial chemicals. The Center analyzes chemical threat characterization data, including toxic industrial chemicals and chemical warfare agents, and integrates science-based risk assessments using physical, chemical, and toxicological information. In an emergency, CSAC can support other agencies and organizations with expert analysis. Total staff is approximately 22 FTE.

**E. Transportation Security Laboratory (TSL)**

The Transportation Security Laboratory (TSL) protects our nation's transportation systems through research, development, testing and validation of explosives technology detection systems. Based in New Jersey, TSL develops products in the areas of personnel inspection, checked baggage and small parcel inspection, containerized cargo inspection, conveyance protection, and infrastructure protection. The laboratory has a long history of success and is internationally recognized for its role in the development of standards, protocols and test articles necessary for detection technology assessments. Based on increased requirements to do explosives testing, an Infrastructure Investment Plan has been completed to provide a long-term capability for explosives testing and evaluation. Total staff is approximately 120 FTE.

**F. National Urban Security Technology Laboratory (NUSTL)**

The National Urban Security Technology Laboratory (NUSTL) advances the science and technology required for preventing and responding to homeland security threats, especially in the areas of radiological and nuclear threats. NUSTL seeks to improve the understanding of these threats through research, development, testing and evaluation. The NUSTL team provides these capabilities for Department-developed technologies and systems. The lab's central Manhattan, NY location and relationships with the Tri-State region's homeland security community complement NUSTL's test and evaluation capability by enabling the use of the New York metropolitan area as an urban test bed in support of the first responders. Total staff is approximately 31 FTE.

## Technology Transfer

The Office of National Labs also oversees the DHS Technology Transfer Program which serves as the focal point for technology transfer activities at the Department. Currently, the Department operates from one centralized Office of Research and Technology Applications (ORTA) to manage technology transfer at each of its laboratories and throughout the Department. The Technology Transfer Program promotes the transfer and/or exchange of technology with industry, state and local governments, academia, and other Federal agencies. The technologies developed and evaluated within the Department can have tremendous potential for commercial applications throughout the nation and dramatically enhance the competitiveness of individual small businesses as well as expanding areas of exploration and cooperation for all non-federal partners.

To accomplish its mission, the Technology Transfer Program promotes research and partnerships, evaluates, protects, markets, licenses, monitors, and manages Department inventions and other intellectual property as mandated by the Federal Technology Transfer Act of 1986.

To accomplish its mission, the Technology Transfer Program Office:

- Serves as the focal point for the Department on technology transfer policy
- Assists Laboratories in conducting R&D for technology that can be transferred in support of DHS mission
- Establishes partnerships to transfer cutting-edge technology to the nation's marketplace
- Prepares assessments for selected R&D projects that may have commercial applications
- Provides and disseminate information of federally owned or originated products, processes, and services having potential application to state and local government and to private industry
- Cooperates with and assists the National Technical Information Service, the Federal Laboratory Consortium for Technology Transfer, and other organizations which link the R&D resources of that laboratory and Federal government as a whole to potential users in State and local government and private industry
- Provides technical assistance to State and local government officials
- Participates in regional, State, and local programs designed to facilitate or stimulate the transfer of technology for the benefit of the region, State, and local jurisdiction of DHS laboratories
- Works closely with each laboratory on technology transfer matters through the Technology Transfer Program Manager (T2PM).

## Technology Transfer Mechanisms

**Cooperative Research And Development Agreements (CRADA)** – The CRADA is probably the most commonly used technology transfer mechanism. CRADAs are instruments that may be used in all aspects of a product and/or system life cycle where research, development, test and evaluation (RDT&E) activities occur. The federal parties may provide personnel, services, facilities, equipment, intellectual property or other resources with or without reimbursement (but not funds to the non-federal parties). The non-federal parties may provide funds, personnel, services, facilities, equipment, intellectual property, or other resources toward the conduct of specified research and development efforts that are consistent with

the missions of the Component or Laboratory. Please contact Tech Transfer for more information about a CRADA agreement.

**Licensing Agreement** – A contract between the owner or lawful user of Intellectual Property and another party (licensee) that permits the licensee to use the IP in accordance with the terms of the contract. Please contact Tech Transfer for more information about a licensing agreement.

**Memorandum of Understanding (MOU)** – An MOU provides the framework for cooperation and coordination with other agencies. The agreement helps to ensure smooth operations with shared resources or workflow. It creates a clear understanding of each party's commitment/purpose.

**Partnership Intermediary Agreement (PIA)** – An agreement between DHS and the agency of a state or local government or a nonprofit entity to allow the Partnership Intermediary to:

1. Identify new technologies in the private sector that can be utilized by DHS
2. Facilitate joint projects between DHS and private companies, as well as between agencies and academic institutions, to accelerate delivery of technological capabilities to the nation
3. Help existing companies identify DHS technologies that can be licensed and commercialized

## Office of University Programs

The Office of University Programs supports critical homeland security-related research and education at U.S. colleges and universities to address high-priority DHS-related issues and to enhance homeland security capabilities over the long term. The Office of University Programs is charged with maximizing DHS' return on investment in university research and education with the goal of creating a permanent and coordinated network of universities conducting research, supporting science and engineering education and careers, and providing capabilities for DHS to access at any time.

Our guiding principles are:

Effective – Do the right work [quality products]

Efficient – Do the work right [lowest cost]

Enduring – Recoup the investment [returning customers]

Equal Opportunity – Reflect America to protect America [build customer base for the future]

The program brings together scientists, mathematicians, and engineers from many academic disciplines and institutions. These researchers are investigating research questions important to DHS and developing new technologies and approaches to solve complex and challenging homeland security problems. The program focuses on building homeland security expertise in the academic community, creating strategic partnerships among universities and public agencies, and developing a new scientific workforce of homeland security experts. The primary customers for the Office of University Programs are the DHS S&T Directorate's divisions, the DHS component agencies, and federal, state, and local government agencies.

Investments in university basic research and support for students in relevant fields are critical to preserving the U.S.'s strategic and economic security as well as supporting all five Quadrennial Homeland Security Review (QHSR) Mission Areas:

- Preventing Terrorism and Enhancing Security
- Securing and Managing Our Borders
- Safeguarding and Securing Cyberspace
- Ensuring Resilience to Disasters, and
- Enforcing and Administering our Immigration Laws.

The Office of University Programs carries out its activities through three thrust areas: 1) the DHS University Centers of Excellence (COEs), 2) the DHS S&T Directorate's Educational Programs, and 3) the Minority Serving Institutions.

The Director of the Office of University Programs is Dr. Matthew Clark.

## Centers of Excellence

The 12 current COEs engage approximately 200 colleges and universities to conduct multidisciplinary research in priority DHS mission areas (see Figure 9). The COEs align to the S&T Directorate's divisions and their customers. COEs improve understanding of the causes, elements, and consequences of a range of threats from terrorists and natural disasters. They also support countermeasure, mitigation, prevention, and resilience approaches based on both technologies and human behavior.

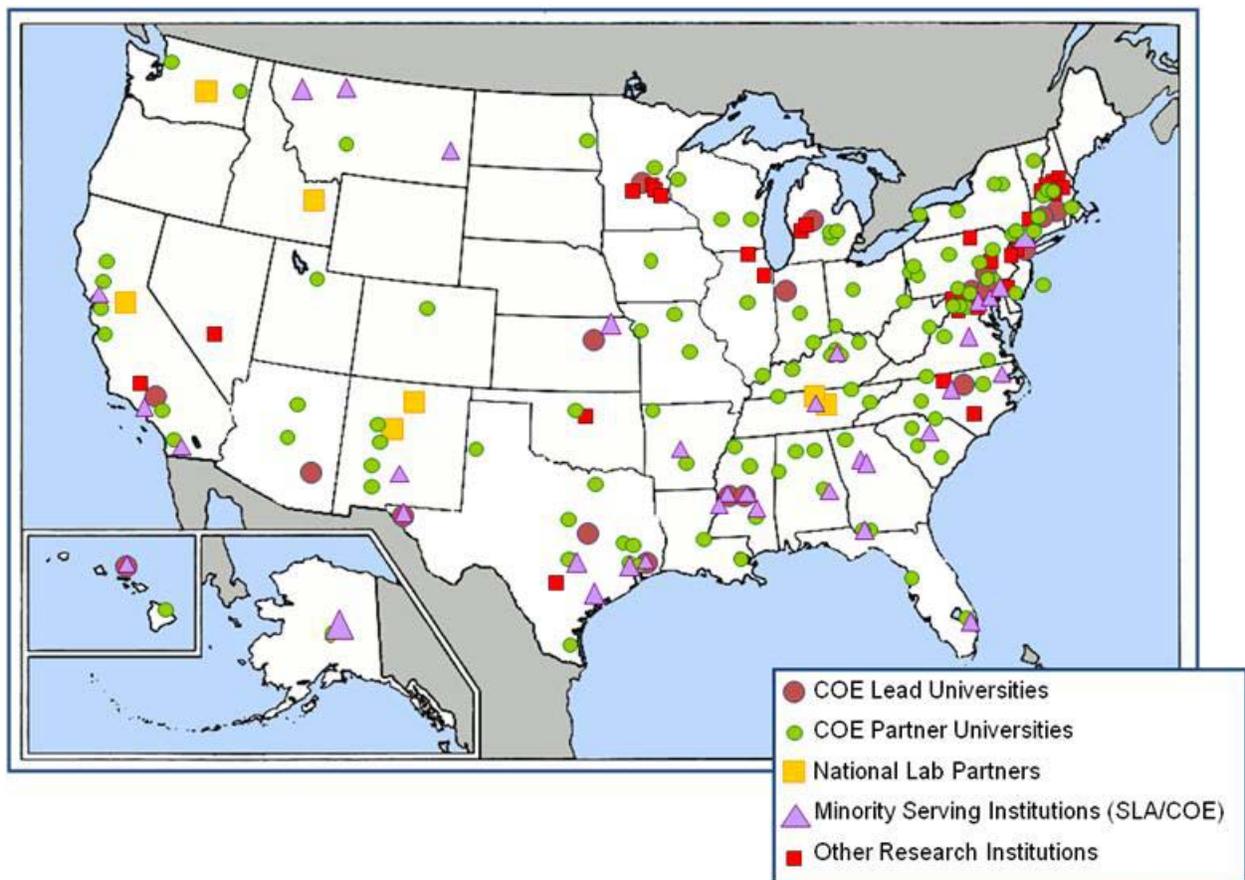


Figure 9 The DHS University Network

The COEs work with and through the S&T Directorate's divisions and complement other DHS research and development programs including those of federal laboratories and federally funded research and development centers (FFRDCs). They take advantage of other relevant Federal agency-sponsored research and provide outcomes useful to federal, state, and local government, private sector, and international partners. The selection process for the COEs is highly competitive, rigorously peer-reviewed, and merit-based.

The COEs are primarily funded through research grants and cooperative agreements. They are building expertise and reach-back capabilities in multi-disciplinary topical areas important to homeland security.

The current COEs are:

1. Center for Risk & Economic Analysis of Terrorism Events (CREATE)
  - Lead: University of Southern California
2. National Center for Zoonotic & Animal Disease Defense (ZADD)
  - Lead: Kansas State University
  - Lead: Texas A&M University
3. National Center for Food Protection & Defense (NCFPD)
  - Lead: University of Minnesota
4. National Consortium for the Study of Terrorism & Responses to Terrorism (START)
  - Lead: University of Maryland
5. Center for Advancing Microbial Risk Assessment (CAMRA)
  - Lead: Michigan State University, in Partnership with U.S. EPA
6. National Center for the Study of Preparedness & Catastrophic Event Response (PACER)
  - Lead: Johns Hopkins University
7. The Center for Awareness and Location of Explosives-Related Threats (ALERT)
  - Research Co-Lead: Northeastern University
  - Education Co-Lead : University of Rhode Island
8. The National Center for Border Security and Immigration (NCBSI)
  - Research Co-Lead: University of Arizona
  - Education Co-Lead: University of Texas at El Paso
9. The Center for Maritime, Island and Remote and Extreme Environment Security (MIREES)
  - Maritime and Islands Co-Lead: University of Hawaii (CIMES)
  - Port Security Co-Lead: Stevens Institute of Technology (CSR)
10. Natural Disasters, Coastal Infrastructure and Emergency Management (NDCIEM)
  - Research Co-Lead: University of North Carolina at Chapel Hill (DIEM)
  - Education Co-Lead: Jackson State University (NDCIEM)
11. National Transportation Security COE (NTSCOE) – Required by HR-1
  - Research Co-Lead: University of Connecticut
  - Education & Training Co-Lead: Tougaloo College
  - Petro-Chemical Transportation Co-Lead: Texas Southern University
12. Command Control and Interoperability (C2I)
  - Co-Lead: Purdue University
  - Co-Lead: Rutgers University

## **Education Program**

OUP administers several programs and initiatives that assist in increasing the Homeland Security (HS)-STEM workforce. Collectively, these programs and initiatives are intended to inspire, engage, educate and ultimately direct academically high performing individuals toward choosing HS-STEM related careers. The programs support institutions as well as high-performing science and engineering students or professionals in the United States to develop the next generation of homeland security science

and technology leaders. OUP funds students, scholars, and faculty drawn from postsecondary, graduate, and professional levels of science and engineering disciplines. Activities include individual student scholarships and internships; Homeland Security related Science, Technology Engineering and Mathematical (HS-STEM) Career Development Grants to academic institutions; and post graduate professional fellowships.

**National HS-STEM Scholarship and Fellowship Program** – The DHS Scholars program competitively awards scholarships to individual science, mathematics, and engineering undergraduate and graduate students throughout the U.S. In addition to a monthly stipend, tuition, books and fees are paid for up to three years. A one year post completion service commitment is required.

**National HS-STEM Summer Internship Program** – Internships are provided to rising juniors and seniors for up to ten weeks during the summer. Participants are provided a stipend and conduct research in DHS mission-relevant research areas at federal research facilities and DHS Centers of Excellence (COE).

**Career Development Grants Program** – Grants are competitively awarded to accredited universities, including the COEs, which have made a commitment to develop HS STEM related curricula and courses of study. The recipients recruit and mentor participants to assure their success and direct them to HS-STEM related careers.

**Professional Fellowships** – The Office of University Programs (OUP) supports initiatives and opportunities for individuals with advanced degrees and highly specialized Homeland Security expertise to assist with special projects within DHS S&T or the National Laboratories, as needed.

**DHS Employee Professional Development** – As needed, OUP supports initiatives and opportunities for current DHS professionals to obtain advanced training and education in order to maximize use of current human capital.

### **Minority Serving Institutions (MSIs)**

The primary goal of the OUP Minority Serving Institutions (MSI) programs is to develop a homeland security-related science, technology, engineering and mathematics (HS-STEM) workforce that reflects the diversity of the Nation as efficiently as possible. Programs in this area include the Scientific Leadership Award (SLA) grant program and the Summer Research Team (SRT) program. Both are intended to improve the capabilities of MSIs to conduct research, education, and training in areas critical to homeland security and to develop a new generation of scientists capable of advancing homeland security goals. OUP is leveraging the existing science and engineering capabilities of MSIs through the following awards and programs:

**MSI Scientific Leadership Awards (SLA)** – Institutional awards to support the development of HS-STEM teaching initiatives, curriculum development and scholarships in HS-STEM fields. The

SLA program provides three to five years of institutional support for students and early career faculty.

**Summer Research Team Program** – Early career faculty and up to two students from Minority Serving Institutions (MSI) are selected as teams to participate in the program. The team conducts research at one of the twelve DHS Centers of Excellence and their partners for 10 weeks during the summer. The program is designed to provide research opportunities to increase and enhance the scientific leadership at MSIs in research areas that support the mission and goals of DHS.

## **International Cooperative Programs Office**

The International Cooperative Programs Office provides the strategic framework to establish, facilitate, and sustain effective international partnerships that support homeland security research, development, test and evaluation. The Office catalyzes the Science and Technology (S&T) Directorate's connectivity among the international science and technology community, Department of Homeland Security operational components, and the homeland security research enterprise.

### **Objectives**

The International Cooperative Programs Office works to match U.S. entities engaged in homeland security research with foreign counterparts so that they may partner in cooperative research activities. Specifically:

- Coordinating with partner nations, the Department, and other agencies to identify viable areas for cooperation and partnering opportunities.
- Engaging international partners to participate in the Department Centers of Excellence program and encouraging U.S. institutions to partner with academic institutions abroad.
- Conducting an international research grant program that requires recipients to include at least one U.S. and foreign institution.
- Developing strategic priorities with the Department Office of International Affairs and other federal agencies in support of the homeland security mission.

### **Leadership**

The International Cooperative Programs Office is headed by the ICPO Director. The Director keeps the Under Secretary, Deputy Under Secretary, Chief of Staff, Chief Scientist, Director of Support to the Homeland Security Enterprise and First Responders, Director of Homeland Security Advanced Research Projects Agency, Director of Acquisition Support and Operations Analysis, Director of Research & Development Partnerships, Associate General Counsel, Director of Finance and Budget, and Director of Administration informed of significant international developments and potential areas of collaboration with international partners. The Director of ICPO is Ms. Lilia Ramirez.

### **Organization**

The International Cooperative Programs Office was established in accordance with Title 6 U.S. Code Section 195c ("Promoting antiterrorism through international cooperation"). The International Cooperative Programs Office facilitates the planning, development, and implementation of international cooperative activity to address the strategic priorities the Under Secretary considers appropriate, including grants, cooperative agreements, or contracts to or with foreign public or private entities, governmental organizations, businesses, federally funded research and development centers, and universities.

### **Grants**

The Department of Homeland Security Science and Technology Directorate solicits applications for international research projects aligned with the mission and requirements of the directorate. These

projects should be designed to augment and complement, through international research and collaboration, the depth and breadth of homeland security science and technology research.

Specifically, the S&T Directorate seeks proposals that will contribute to homeland security science and technology, including but not limited to:

- Evaluation of novel tools or approaches to confronting homeland security challenges.
- Basic research to provide data, understandings, or models that support S&T efforts or policy decisions.
- S&T and operations research evaluations to support revolutionary improvements in the Department's mission and its component agencies' operations.

Information on these grants, including eligibility criteria and how to apply will be made available at [www.grants.gov](http://www.grants.gov). Proposals must be led by an academic institution and must include both U.S. and foreign institutions. For more information, e-mail [S&T-InternationalPrograms@dhs.gov](mailto:S&T-InternationalPrograms@dhs.gov).



Figure 10 Map of ICPO Grant Awardees

## Interagency Division

The R&D Partnerships Group serves as the primary collaborative group for the S&T Directorate. The Interagency Division (IAD) supports the Partnership Group and Directorate by serving as S&T's lead facilitator and systems integrator for helping our internal and external members of the Homeland Security Enterprise (HSE) achieve their respective missions. We conduct outreach with our state and local partners to strengthen collaborative efforts, and to collect input, on their technology gaps. Our partnerships with other agencies of the Federal government are focused on sharing information relative to the research, development, test and evaluation (RDT&E) requirements and capabilities of both the Directorate and its partners.

The Director of the IAD is Mr. Randel Zeller.

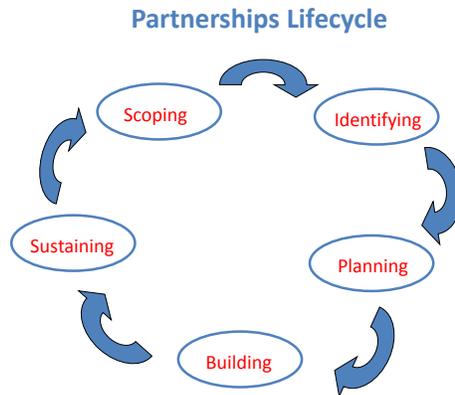
### **Mission**

The IAD establishes and implements policies for the management of interagency programs to enhance cooperative science and technology and RDT&E endeavors with members of the HSE: other Federal agencies, other DHS components, state, local, territorial and tribal governments. It also facilitates S&T's cooperative RDT&E activities across Federal, State, local, territorial and tribal governments, and the private sector, working to leverage fully the capabilities of external organizations to address high priority homeland security requirements.

This endeavor is accomplished by representing the Directorate, and exercising a leadership role, on boards, committees, and other groups pertaining to homeland security science and technology and RDT&E efforts of national scope and interest. The Division encourages and coordinates the exchange of information with other DHS officials and representatives of Federal, State, local, tribal, academic, and private sector organizations; and coordinates with other appropriate executive agencies in developing and carrying out the science and technology agenda of the Department. These mutually beneficial partnerships allow for the identification of potential technology solutions, avoids potential duplication of effort and investments among our internal and external customers, and contributes to the execution of S&T's mission.

## Partnerships and Interagency Collaboration

Key to our mission is cultivating and maintaining successful partnerships. The following figure depicts an example of a Partnerships Lifecycle Process.



**Figure 11** The Interagency Division fosters meaningful relationships through the Partnerships Lifecycle.

These steps of the lifecycle are:

### Scoping

- Establishes boundaries
- Manages expectations
- Ensures a consistent understanding

### Identifying

- To listen
- To accept
- To empathize

### Planning

- A road map to success
- Defines clear responsibilities
- An agreement of work
  - “Fail to plan – plan to fail”

### Building

- A foundation for the future
- The way ahead
- Measureable, tangible and successful

### Sustaining

- To conduct ongoing outreach
- To maintain effective collaboration
- To provide effective, reliable communications

One of the unique aspects of IAD is its construct: a geographically dispersed organization of senior analysts who possess scientific and multi-disciplinary practical education and experience in the mission focus areas of preparedness, response and resilience. The staff’s geographical areas of responsibility align with the FEMA Regional construct so that activities are in accordance with the DHS construct. This is in the interest of our state, local, territorial and tribal customers. Their work is also coordinated with

DHS components, such as the DHS/Office of Intergovernmental Affairs (IGA) as appropriate. Their extensive experience, knowledge of the ‘footprint’ of the respective geographic areas, and daily interactions with our stakeholders make them uniquely poised to cultivate partnerships with our HSE partners, provide expert guidance to the S&T divisions on areas of concerns of our stakeholders as well as potential impediments to successful field demonstrations and testing needed by the Directorate.

Through knowledge of organizational constructs of our HSE customers, alignment and processes at the federal, state and local levels, IAD is able to provide expert guidance in accordance with our DHS policies coordinating the initiatives of the directorate. Their input also provides the directorate with key information when demonstration or testing is being considered to ensure a fair and equitable balance among our interested HSE customers. As piloting and testing is needed by the directorate, IAD is called upon to provide expert guidance and recommendations for engaging with our external customers. They also receive technology requirements and provider information and relay such information to the appropriate Directorate office or division for action.

The Division also serves as the directorate’s IGA and Tribal Liaison - coordinating/facilitating the Directorate’s state, local and tribal activities with IGA - key areas of interest for the Secretary.

### **Communication and Information Sharing**

Another unique aspect of the Division is the ability of its staff to obtain, capture and share information and knowledge with the Directorate in a real-time environment. This can only be achieved through the establishment of their trusted, lasting and sustainable relationships. These vital communication links increase situational awareness and directly support the Department’s mission of enhancing preparedness, resiliency and response.

The extensive interagency coordination conducted by the IAD includes involvement with officials at the Federal, State, local, tribal, and territorial level which meets priorities of the Department. IAD continues to seek opportunities to leverage research and technology development efforts in support of Homeland Security needs; and to cultivate S&T collaboration, partnering, and information sharing opportunities. IAD maintains enduring relationships with key state and local officials, including Adjutant Generals, Homeland Security Advisors/Directors, first responder officials and organizations, as well as federal customers providing valuable information to the S&T Division Directors for their respective initiatives.

### **Strategic Accomplishments**

The IAD has established and continues to maintain valuable relationships among the DoD community. It has served as the S&T lead on the DoD-DHS Capability Development Working Group (CDWG) Senior Steering Committee (SSG) which provided a provided a senior-level forum to explore capability development topics of mutual interest; ensure best use of resources and avoid duplication of effort; promote cooperation; and support/ inform policy, planning, and decision-making activities. It coordinated a Homeland Defense/ Homeland Security (HD/ HS) Forum with DoD to better enable awareness, synchronization of, and interest in finding solutions to HD/HS capability gaps. The Division

also monitors the progress of a number of DoD Joint Capability Technology Demonstration (JCTD) programs. The CDWG continued to serve as the key vehicle for collaboration between DOD and DHS. It is chaired by the DHS/Under Secretary for S&T, DHS/Under Secretary for Management, and the DoD/Under Secretary for Acquisition, Technology, and Logistics (OSD AT&L). Improved collaboration was realized in the areas of Unmanned Aerial Systems (UAS), national airspace surveillance and security, enhancing security of nation's electrical power grid, and joint radiation detection capabilities. The CDWG also coordinated the adoption of a DHS-DOD-EPA Memorandum of Agreement promoting collaboration in the areas of Chemical and Biological Security. The charter for the CDWG was signed by the Deputy Secretary of Defense and Deputy Secretary of Homeland Security in FY 09.

We have expanded our collaborative relationships and outreach with the DOD, DOE, the National Guard, the Joint Staff and appropriate Combatant Commanders to leverage RDT&E efforts and capabilities resulting in savings to the government by avoiding duplication of effort and investments. The IAD has also conducted Regional Homeland Security S&T Summits in the west and south. These symposia enhanced and strengthened partnerships, collaboration and information sharing with and among Federal, State, Local, Tribal, and National Laboratory partners. They also served to better understand and address the technology needs of our customers. The success of these symposia was measured by the expressed desire of our customers for us to further such endeavors. Capability gaps and/or concerns were shared with S&T divisions as appropriate. Future symposia are being planned.

We work closely with the National Guard and US Northern Command to support interagency efforts to establish a Homeland Defense/ Homeland Security (HD/HS) Capabilities Forum to enable awareness, synchronization of, and interest in finding solutions to HD/HS capability gaps. Participating agencies included: US Northern Command; National Guard; S&T; OSD AT&L; Assistant to the Secretary of Defense for Homeland Defense and America's Security Affairs; Office of the Secretary of Defense/ Director, Defense Research and Engineering; Defense Threat Reduction Agency; Defense Advanced Research Projects Agency; National Nuclear Security Administration; Department of Justice; Combating Terrorism Technical Support Office; Joint Chiefs of Staff; the National and Service Laboratories; the Center for Homeland Defense and Security (Naval Post Graduate School); and the Institute for Defense Analyses.

The IAD assisted with the interagency coordination of the funding and conduct of the first DHS-DOD-DOE interagency "war-game," in partnership with the commercial electric utility industry, which simulated a coordinated (terrorist physical and cyber attack) on the national electric grid. The war-game was hosted by National Defense University (NDU) in July 2009. The war-game identified weaknesses in multi-agency plans, policies and procedures. Those weaknesses will require improvement to make the nation safer against this type of threat. DHS personnel from the offices of Intelligence and Analysis (I&A), National Protection and Programs Division (NPPD), Office of Infrastructure Protection (OIP), National Cyber Security Division (NPPD) and National Operations Center (NOC) also participated. IAD personnel have provided numerous post-war-game briefings to DHS and DOD stakeholders and there is growing high level attention to the need of addressing the vulnerabilities highlighted by the war-game. S&T is working with USNORTHCOM to plan a follow-up regional exercise which will examine grid reliability issues affecting critical infrastructure and DOD installations plus the surrounding civilian areas.

Internally at DHS S&T, we helped establish interagency outreach between the Human Factors and Behavioral Sciences Division (HFD) and US Joint Forces Command (JFCOM) to leverage \$36M of DoD funds. HFD collaborated with JFCOM to enhance Small Unit High Performance in support of the Future

Immersive Training Environment (FITE). Within the DOD RDT&E structure this initiative is classified a Joint Capabilities Technology Demonstration (JCTD). The objective of the JCTD is to demonstrate, assess, and transition capabilities to better prepare small combat units (for DHS this equates to first responders and the variety of field deployed DHS agency units) to perform in high stress, extremist situations, and to allow us to better provide them with the knowledge, skills, and abilities to successfully perform their tasks and detect those cues in the field that signal an unexpected threat.

We regularly exercise a leadership role for the Directorate in conducting an on-site visit to a major disaster event to provide extensive support and assess technology needs. Through the established contacts made with our HSE customers, IAD plans to expand its role in this area serving as the primary linkage for the Directorate.

IAD also maintains the DHS Center of Innovation (COI) at the United States Air Force Academy. The COI has evolved rapidly into a significant public/private collaboration facilitator. Major components from the interagency, particularly, the Intelligence Community, have joined with the COI to collaborate with the private sector. The primary emphasis thus far has been in cyber security and point-to-point collaboration over a non-secure network.

## Public-Private Partnerships Office

The Public-Private Partnerships Office is comprised of DHS S&T's Office of SAFETY Act Implementation (OASI), the Long Range Broad Agency Announcement (LRBAA) procurement vehicle, the Small Business Innovation Research (SBIR) Program Office, and the Commercialization Office. This collection of offices has a common mission of engaging with the private sector in a proactive manner to create opportunities for the private sector to engage with DHS S&T. These offices all possess rigorous evaluation processes to determine the efficacy of private sector offerings to address the mission critical needs of the Homeland Security Enterprise and create easy-to-use vehicles that will advance the fielding of needed capabilities. The Public-Private Partnerships Office is an effective and efficient organization that promotes and facilitates collaborative efforts with the private sector and delivers to the private sector critical information about current and future capability needs and requirements of the Homeland Security Enterprise.

A public-private partnership is an agreement between a public agency and a private sector entity that combines skills and resources to develop a technology, product and/or service that improves the quality of life for the general public. The private sector has been called upon numerous times to use its resources, skills and expertise to perform specific tasks for the public sector. Historically, the public sector has frequently taken an active role in spurring technological advances by directly funding the private sector to fulfill a specialized need that cannot be completed by public sector itself.

Increasingly, users in the public sector are being viewed as stable markets – i.e., a sizeable customer base for the private sector to warrant investments of time and money. A commercialization-based public-private partnership has the same goal as more traditional public-private partnerships, but the method is inspired to leverage positive attributes of the free market system. The introduction of a commercialization-based public-private partnership, developed and implemented at the US Department of Homeland Security (DHS) provides benefits for three constituents of the Homeland Security Enterprise (HSE): the private sector, the public sector and the taxpayer. This is a desirable scenario where there is a “win-win-win” environment created in which all participants are in a position to benefit.

In the free market system, private sector companies and businesses must sell commercial products consumers want to purchase. Commercialization is defined as the process of developing markets and producing and delivering products and/or services to address the needs of those targeted markets. The development and understanding of markets is a critical undertaking for many companies seeking to gain share of a market, with companies directing significant amounts of money and resources to these activities in addition to its product development efforts. Sometimes a company does not understand the correct needs or demand data of a market or market segment and their product(s) does not sell well. The company's investment in designing, manufacturing and advertising the product can, and is in many cases, a waste of time and money if the company “misses the mark.”

## Office of SAFETY Act Implementation

As part of the Homeland Security Act of 2002, Public Law 107-296, Congress enacted the Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act) of 2002. The SAFETY Act provides incentives for the development and deployment of effective anti-terrorism technologies through systems of risk and litigation management. The purpose of the Act is to ensure that the threat of liability does not deter potential manufacturers or sellers of anti-terrorism technologies from developing and commercializing technologies that could save lives. The Act creates certain liability limitations for claims arising out of, relating to, or resulting from an act of terrorism where qualified anti-terrorism technologies have been deployed.

The Secretary of the U.S. Department of Homeland Security (DHS) determines whether an act of terrorism has occurred; this determination is required to employ the protections of the Act. The DHS Under Secretary for Science & Technology or the Under Secretary's designees are the decision officials regarding SAFETY Act applications. The SAFETY Act program is administered by the Office of SAFETY Act Implementation, reporting to the Director, Research & Development Partnerships Group, in the DHS Science & Technology Directorate.

The SAFETY Act applies to a broad range of technologies, including products, services, and software, or combinations thereof, as long as the Under Secretary for Science & Technology or the Under Secretary's designees, as an exercise of discretion and judgment, determines that a technology merits coverage. Examples of some eligible technologies can be seen below:

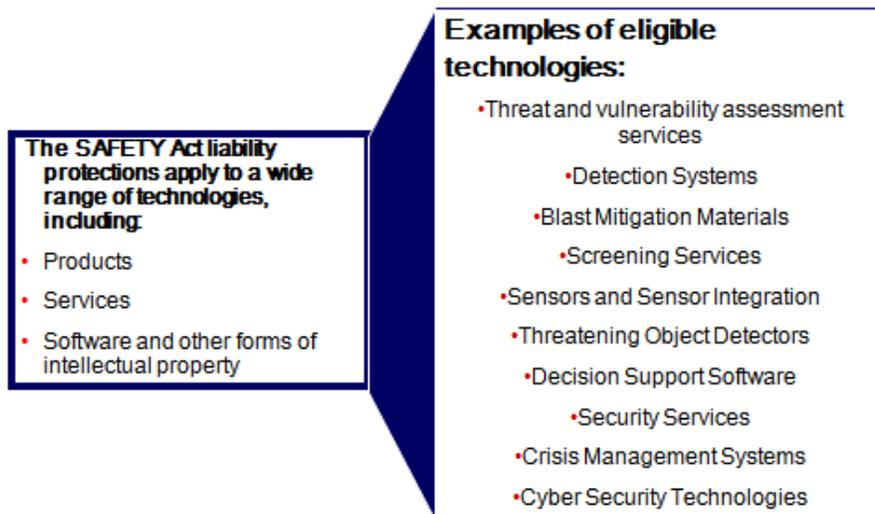


Figure 12 SAFETY Act liability protections cover a wide range of technologies.

The SAFETY Act provides liability protection to both sellers of technologies that are determined to be effective by DHS (these technologies are called “Qualified Anti-Terrorism Technologies” or QATTs) and, very importantly, to their customers. DHS has consistently held the position that SAFETY Act

protections extend to users, since, under the purview of the SAFETY Act, a lawsuit alleging deficiencies with the performance of a QATT may be brought only against the Seller of the QATT and not against the buyers, the buyers' contractors, downstream users of the QATT, the Seller's suppliers or contractors, or any other person or entity. This feature can provide a significant benefit for security service and technology vendors and their customers, which can include commercial facilities, critical infrastructure sites, the transportation industry, and public venues.

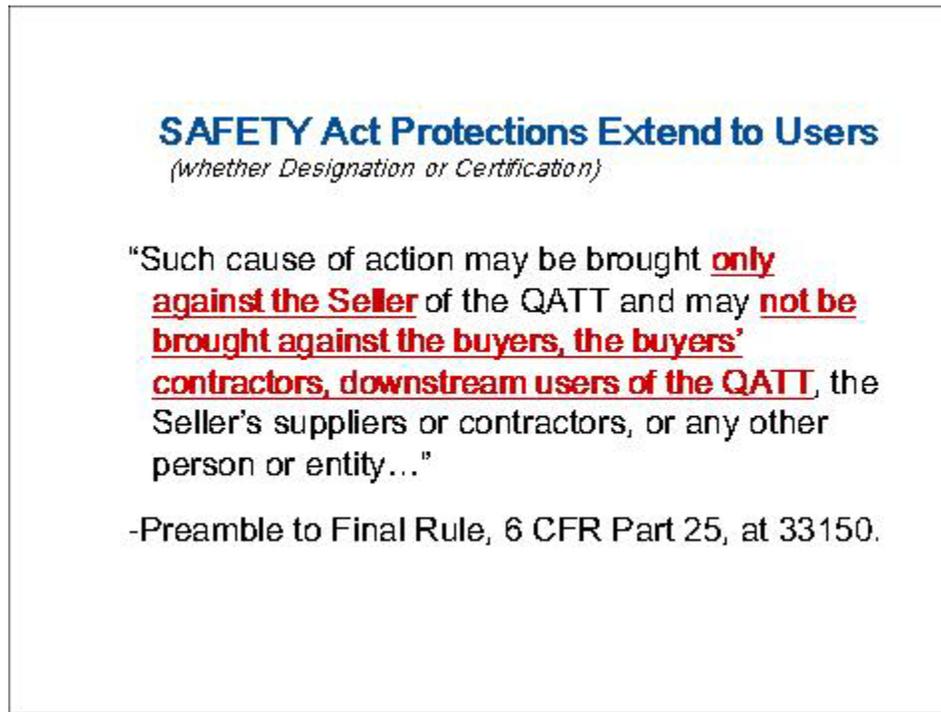


Figure 13 SAFETY Act protections cover the users of QATTs as well as the developers.

*Under the SAFETY Act, there are two principal levels of protection: Designation, and Certification.*

The benefits of SAFETY Act **Designation** include:

- Liability is capped at the amount of liability insurance that DHS requires the Seller to obtain and maintain;
- Sellers are not liable for punitive damages, prejudgment interest, or non-economic damages caused by others;
- All claims are heard in Federal court;
- Users of Designated technologies/services are immune from suit for failures allegedly due to those technologies/services; and
- Special coverage is available for promising technologies during Developmental Testing and Evaluation in a limited number of operational venues.

In addition to these benefits, for **Certification**, the SAFETY Act creates a rebuttable presumption that the government contractor defense applies to those QATTs approved by the Secretary in accordance with certain statutory criteria. The presumption may be overcome only by evidence showing that the Seller acted fraudulently or with willful misconduct in submitting information to the Secretary, DHS, during the

Secretary’s consideration of such technology.<sup>3</sup> The government contractor defense is an affirmative defense that immunizes Sellers from liability for certain claims.

The government contractor defense under the SAFETY Act appears to be somewhat broader than the judicially-created government contractor defense doctrine set forth in *Boyle v. United Technologies Corp.*, 487 U.S. 500, 512 (1988) and subsequent cases. First, the SAFETY Act provides that the Seller of a QATT with SAFETY Act Certification need not be a government contractor to take advantage of this defense; it applies to Sellers who contract with other private sector entities as well. Secondly, Sellers of QATTs with SAFETY Act Certification need not design their technologies to federal government specifications to obtain this defense; for example, commercial off the shelf technology may be employed. An additional benefit of Certification is a listing of the approved technology on the SAFETY Act’s “Approved Product List for Homeland Security” at [www.safetyact.gov](http://www.safetyact.gov). Technologies that are Designated may be listed on the web site under a separate Designations listing.

The criteria considered by DHS in evaluating a technology for Designation and Certification are set forth in the Regulations Implementing the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (the “Final Rule”), 6 CFR Part 25.

The Designation criteria, set forth in greater detail in §25.4 of the Final Rule, can be summarized as follows:

## Criteria for Designation

- Prior United States Government use or demonstrated substantial utility and effectiveness
- Availability of the Technology for immediate deployment in public and private settings
- Existence of extraordinarily large or unquantifiable potential third party liability risk exposure to the Seller or other provider of the technology
- Substantial likelihood that the Technology will not be deployed unless SAFETY Act risk management protections are extended
- Magnitude of risk exposure to the public if the Technology is not deployed
- Evaluation of scientific studies that can be feasibly conducted in order to assess the capability of the Technology to substantially reduce risks of harm
- Whether the Technology is effective in facilitating the defense against Acts of Terrorism
- ATT determination made by Federal, State, or Local officials

Red=Technical criterion  
Blue=Economic criterion

Figure 14 SAFETY Act criteria for designation if contained in §25.4 of the Final Rule.

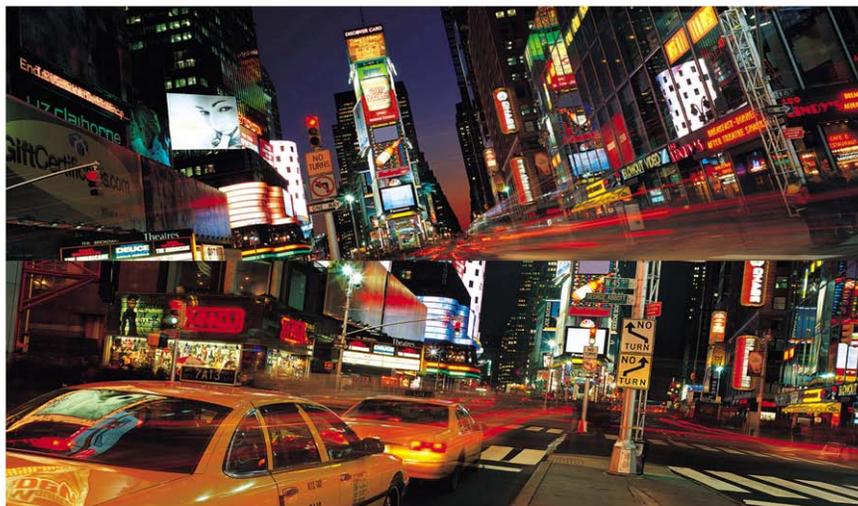
As noted above, the DHS may take into account determinations made by government officials concerning the appropriateness of the technology for anti-terrorism missions, as well as other relevant factors. While the Under Secretary and the Under Secretary’s designees are afforded discretion in applying the evaluation criteria, successful applications normally contain significant evidence of

<sup>3</sup> 6 U.S.C. 442(d)(1).

effectiveness and repeatability in an operational environment. In some cases, this can be demonstrated through the results of operational testing; for others, documentation regarding suitable performance of past deployments, favorable audits, and customer feedback may be appropriate.

For Certification, additional criteria as discussed in §25.8 of the Final Rule, apply: DHS will conduct a more detailed review of the technology and determine whether the technology will perform as intended, conforms to the Seller's specifications, and is safe for use as intended. As the benefits for Certification are higher than for Designation, the application must provide additional evidence of effectiveness beyond that required for Designation. Evidence of high reliability, availability, and consistent positive results (e.g., long-term low failure rates and false alarms) is generally required for Certification.

From the above, it follows that the SAFETY Act can play a significant role in strengthening anti-terrorism readiness for venues, facilities, and various activities (e.g., travel, shipment of goods). The Act can serve as an incentive for Sellers of anti-terrorism technologies and services to deploy them more widely.



### ***The SAFETY Act's Potential Impact: Some Examples***

Deploying an anti-terrorism technology or service in a major commercial facility or commercial center carries significant risk of large financial loss from third party claims and litigation in the event of a successful terrorist attack. Sellers, through obtaining SAFETY Act coverage, will be able to significantly mitigate those risks and thus will be less deterred from undertaking these sales and deployments of anti-terrorism technologies. Sellers will likely devote additional effort and resources to improve the capabilities of their products and services, as they seek Designation, and to qualify for the benefits of SAFETY Act Certification, which requires additional evidence of efficacy. Since SAFETY Act protections generally last for five years, for continued coverage, a renewal application must be filed. Thus, Sellers will have an incentive to monitor the performance of their QATTs, collect relevant data, and make improvements to ensure they can demonstrate continued effectiveness in their renewal applications.

Customers who procure QATTs, whether the QATTs are Designated or Certified, will be able to take advantage of the significant liability protections provided to users of those technologies and services. They will also have added assurance that evidence concerning the engineering and operation of the

QATTs have been reviewed and favorably evaluated by DHS. A listing of SAFETY Act qualified technologies and services can be found on the program web site at [www.safetyact.gov](http://www.safetyact.gov). If the venue owner desires to contract for technologies or services that are not on the listing, consideration should be given to contacting the vendors to acquaint them with the benefits of the SAFETY Act and suggest that they apply for coverage.

The SAFETY Act can also incentivize increased investments in anti-terrorism technologies to protect power grids and water supply systems that deliver these essential services to cities,



to protect transportation infrastructure,



and to enhance security at critical infrastructure sites, by covering technologies such as perimeter security systems, alarm and surveillance systems, cyber security systems, and processes relating to inherently safer technologies.



Some venue owners may wish to deploy an anti-terrorism technology or service that they have developed for their facility, such as integrated security plans or incident response centers. Under appropriate circumstances, they may qualify for SAFETY Act coverage for these efforts. One way to seek further information and guidance from the Office of SAFETY Act Implementation (OSAI) is to take advantage of the Pre-Application process described at [www.safetyact.gov](http://www.safetyact.gov), where applicants can participate in a teleconference with OSAI staff to receive a preliminary assessment of their product or service, its potential eligibility for SAFETY Act protections, and guidance concerning the type of documentation normally expected for a full SAFETY Act application. As shown below, the Pre-Application is an abbreviated process, with applicants normally receiving a response email with information for requesting a teleconference to discuss their technology in approximately 21 days following submission of the pre-application form.

Full applications (for Designation/Certification) are also reviewed in a timely manner. Following receipt, generally within 30 days, a determination is made whether the application is sufficiently complete to permit the commitment of resources required for a full review. The applicant is notified of this determination. If the application is determined to be complete, a final decision is normally made within 120 days of application submission. If the application is determined to be incomplete, a letter is sent to the applicant indicating areas where additional information is required and containing information regarding re-applying.

## Timeline of SAFETY Act Application Review Process

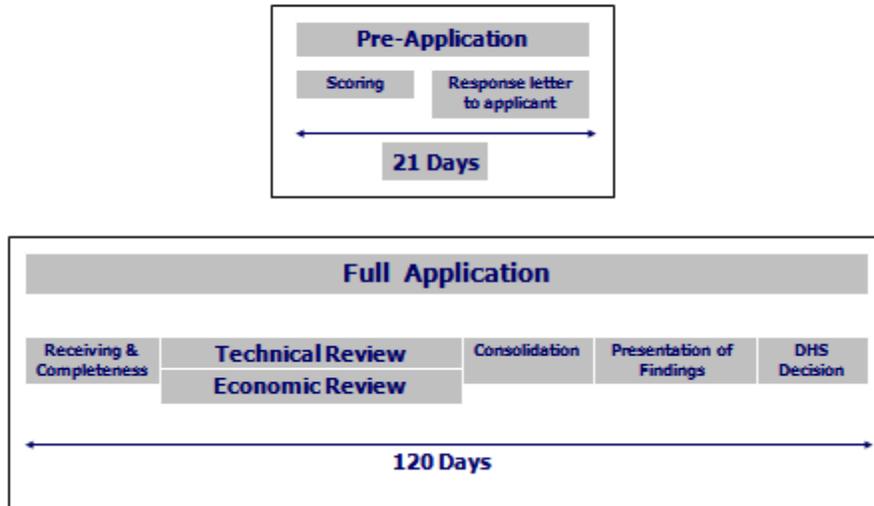


Figure 15 Timeline of SAFETY Act application reviews

The SAFETY Act is an effective and innovative tool for strengthening anti-terrorism capability and security in the United States. As of November 2010, over 400 applicants have successfully earned SAFETY Act protection for their technologies or services. The OSAI is accessible, customer oriented, and open for business. They can be contacted via the Help Desk link on the SAFETY Act website ([www.safetyact.gov](http://www.safetyact.gov)).

## Small Business Innovation Research

In 1982, Congress established the Small Business Innovation Research (SBIR) program with the following objectives: to stimulate technological innovation; to use small business to meet federal research/research and development (R/R&D) needs; to foster and encourage participation by socially and economically disadvantaged small businesses, and women-owned small businesses, in technological innovation; and to increase private sector commercialization of innovations derived from federal R/R&D, thereby increasing competition, productivity and economic growth. The federal SBIR Program is mandated by Public Laws 97-219, 102-564, 106-554, and all public laws that provided temporary extensions of programs under the Small Business Investment Act of 1958, with the most recent extension<sup>4</sup> provided by P.L. 111-251. Each federal agency with an extramural research/research and development (R/R&D) budget in excess of \$100 million must participate in the SBIR program. Each agency must establish an SBIR program by reserving, in each fiscal year, not less than 2.5 percent of its extramural budget for awards to small business concerns for R/R&D. Currently, 11 federal agencies participate in the SBIR program. The Director of the SBIR Program is Ms. Elissa Sobolewski.

The federal SBIR Program is a competitively phased process, uniform throughout the federal government of soliciting proposals, and awarding funding agreements for R/R&D, production, services, or any combination, to meet agency needs or missions. In order to stimulate and foster scientific and technological innovation, including increasing commercialization of federal R/R&D, the program must follow a uniform competitive process of the following three phases:

- Phase I. Phase I involves a solicitation of contract proposals or grant applications (hereinafter referred to as proposals) to conduct feasibility related experimental or theoretical R/R&D related to described agency requirements. These requirements, as defined by agency topics contained in a solicitation, may be general or narrow in scope, depending on the needs of the agency. The object of this phase is to determine the scientific and technical merit and feasibility of the proposed effort and the quality of performance of the SBC with a relatively small agency investment before consideration of further Federal support in Phase II.
- Phase II. The object of Phase II is to continue the R/R&D effort from the completed Phase I. Only SBIR awardees in Phase I are eligible to participate in Phases II and III. This includes those awardees identified via a "novated" or "successor in interest" or similarly-revised funding agreement, or those that have reorganized with the same key staff, regardless of whether they have been assigned a different tax identification number. Agencies may require the original awardee to relinquish its rights and interests in an SBIR project in favor of another applicant as a condition for that applicant's eligibility to participate in the SBIR Program for that project.
- Phase III. SBIR Phase III refers to work that derives from, extends, or logically concludes effort(s) performed under prior SBIR funding agreements, but is funded by sources other than the SBIR Program. Phase III work is typically oriented towards commercialization of SBIR research or technology. Phase III efforts are funding with non-SBIR funds.

The DHS SBIR Program was initiated in 2004. At present, two components with DHS have SBIR programs: the Science and Technology (S&T) Directorate and the Domestic Nuclear Detection Office (DNDO). The goal of the SBIR Program Office is to increase the participation of innovative creative small businesses in federal R/R&D and to challenge industry to bring innovative homeland security solutions to reality for use by the homeland security enterprise. The DHS SBIR Program is focused on

---

<sup>4</sup> Extended to 31 January 2011.

near-term commercialization and delivery of operational prototypes to Federal, state and local emergency responders and managers. The Program's customers are internal DHS entities, and Federal, state, and local emergency responders and managers. The DHS SBIR Program funding has become somewhat stable over the years, with approximately \$15 million set aside in the S&T Directorate and \$6 million set aside in DNDO specifically for small businesses in FY10.

For the DHS SBIR Program, two SBIR solicitations are issued each year, generally in the November and May timeframes. The annual solicitations consist of topics that are relevant to the research areas pursued in the Directorate's divisions: Borders and Maritime Security; Chemical /Biological Defense; Cyber Security; Explosives; Human Factors/Behavioral; Infrastructure Protection and Disaster Management; and Radiological and Nuclear Detection.

All DHS SBIR awards are based on the soundness, technical merit, and innovation of the proposed approach; the qualifications of the proposed principal investigators, supporting staff, and consultants; and the potential for commercial (government or private sector) application and the benefits expected to accrue from this commercialization. Phase I awards are typically up to \$100,000 and six months in duration, with the potential to increase to a total of \$150,000 if a proposed option is exercised. Phase II awards are typically up to \$750,000 and twenty four months in duration, with the potential to increase to \$1,000,000 if a proposed option is exercised. Phase I efforts are awarded as firm fixed price contracts, while Phase II efforts are awarded as either cost reimbursable or firm fixed price contracts.

As of the FY10 competitions, the DHS SBIR Program received 2,608 Phase I proposals from small businesses located in all of the United States (as well as the District of Columbia and Puerto Rico). While program participation occurs throughout the entire United States as shown below, participation from a few states stands out. The states with small business companies receiving the most DHS SBIR awards<sup>5</sup> from 2004 through 2010, in descending order are: California, Massachusetts, Virginia, Maryland, Texas, and New York.

---

<sup>5</sup> More than 100 Phase I proposal submissions.

# DHS SBIR Phase I

## Data from 14 Competitions through FY10.2\*

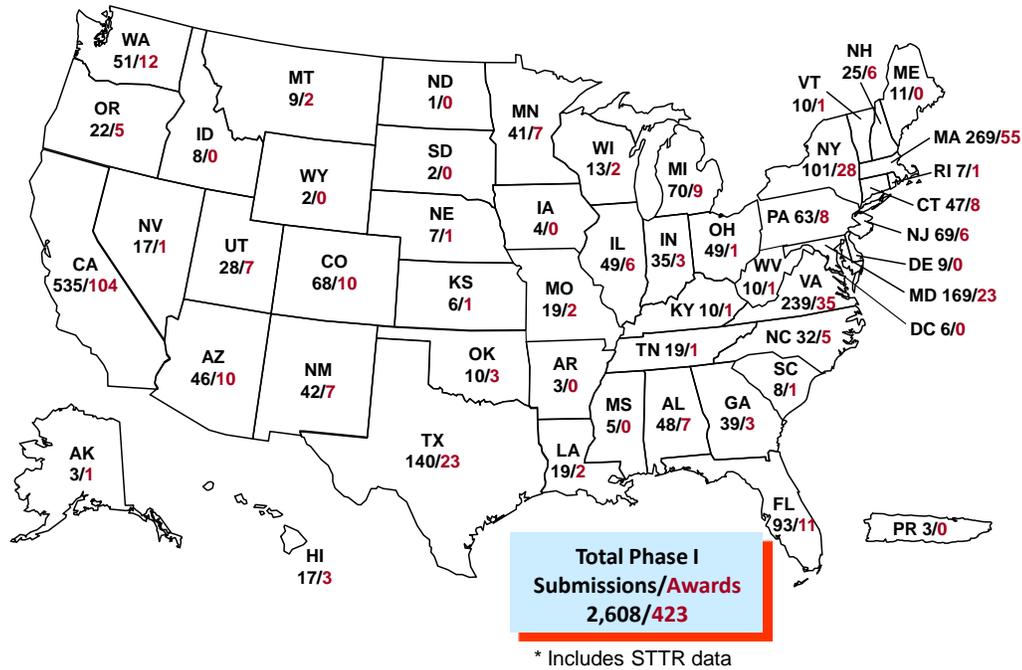


Figure 16 DHS SBIR awardees come from all across the country.

The DHS SBIR Program is quite competitive. From the 2,608 Phase I proposal submissions, 423 Phase I awards, about 16 percent or approximately one in six, were made to small businesses located in 41 states. While this can be a daunting percentage for the potential proposers, the number of projects that move on to Phase II is much higher. To date, one hundred and forty one (or 33 percent) of the Phase I projects have moved on to Phase II. Although a young program (by comparison to other federal agencies SBIR programs), approximately 10 Phase III awards have been awarded to companies that developed technologies under prior DHS SBIR Phase I or Phase II contracts.

The DHS SBIR Program Office truly supports small businesses. Looking at the size of the small business companies among the DHS SBIR submission base, historically, a high percentage are very small. Data from proposal submissions show that 65 percent of the proposal submissions come from small businesses comprised of 24 or fewer employees at the time of award. In fact, 39 percent of the proposal submissions come from companies with between 2 and 9 employees. The chart below shows the distribution of firms submitting Phase I proposals from FY04 through FY10 by number of employees.

## Proposal Submissions by Size of Company (FY04.2 – FY10.2 data)

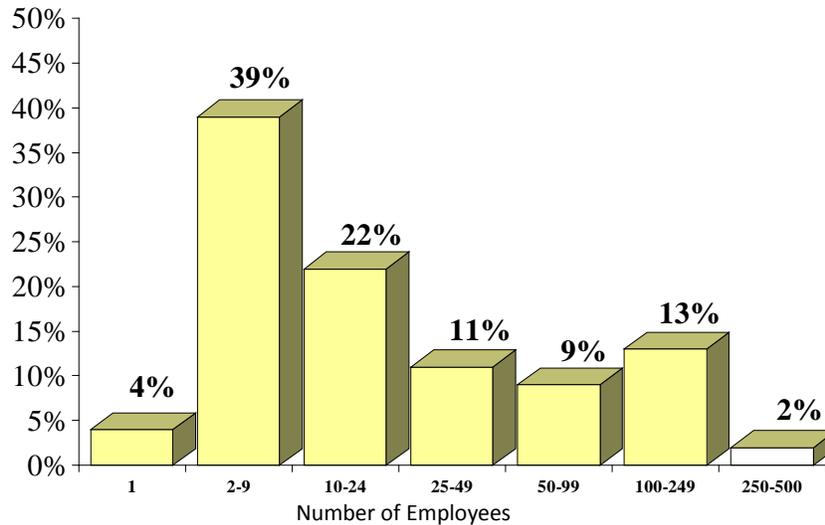


Figure 17 Proposals are received from various company sizes.

Outreach is conducted throughout the United States and includes, but is not limited to, presentations and participation at national, regional, state, and local conferences and workshops. Targeted outreach is conducted to reach women-owned, minority-owned, HUBZone, veteran-owned and other disadvantaged business, ensuring each has an opportunity to participate in the DHS SBIR Program. In addition, the SBIR Program Office participates in the vendor outreach sessions sponsored by the DHS Management Directorate's Office of Small and Disadvantaged Business Utilization. The vendor outreach sessions<sup>6</sup> are a series of pre-arranged 15-minute appointments with Small Business Specialists from various components of the Homeland Security procurement offices. These sessions provide the small business community an opportunity to discuss their capabilities and learn of potential procurement opportunities.

In summary, the DHS SBIR Program<sup>7</sup> is used as a tool for the Science and Technology (S&T) Directorate to seed innovation in our homeland security enterprise industrial base, and in so doing, develop leading-edge technologies with the potential to meet the needs of our operational components today and in the future.

<sup>6</sup> See [http://www.dhs.gov/xopnbiz/smallbusiness/editorial\\_0524.shtm](http://www.dhs.gov/xopnbiz/smallbusiness/editorial_0524.shtm) for additional information about the Vendor Outreach Sessions.

<sup>7</sup> See <http://www.sbir.dhs.gov> for additional information on the DHS SBIR Program.

## Long Range Broad Agency Announcement (BAA)

The Long Range BAA is a funding mechanism for *original research* that addresses the long-term operational needs of the Department of Homeland Security. The Long Range BAA is also used to fund *original research* that advances the foundations of technical knowledge in the basic sciences. Products that are available to the commercial marketplace, or support services of any kind, cannot be contemplated or purchased through the Long Range BAA, according to the *Federal Acquisition Regulations*. Above all, the Long Range BAA is expressly for original, state of the art research, or unique prototypes that require proof of concept. All submissions are peer reviewed.

Successful submissions to the Long Range BAA answer questions such as, “What research problem do you propose to solve? How is your solution different from and superior to currently available solutions or from the efforts of others to achieve a similar solution? What data and analysis do you have to support the contention that funding your R&D project will result in a significant increase in capability for DHS?” Under this LRBA, firms submitting proposals are not competing against each other, but are attempting to demonstrate that their proposed research meets the agency’s requirements. The agency may decide to award contracts to those Offerors who submit ideas which the agency finds suitable.

The Long Range BAA is open to ALL responsible sources. Foreign or foreign-owned Offerors are advised that their participation is subject to the foreign disclosure review procedures, applicable export control laws, and other applicable federal laws, regulations, and policies pertaining to foreign entities. Offerors must be willing to cooperate and exchange software, data, and other information in an integrated program with other contractors or system integrators selected by DHS S&T. Offerors may be single entities or teams, and they may be private sector companies, nonprofit organizations, Government laboratories, airport authorities, Federally Funded Research and Development Centers (FFRDCs), or academic institutions. Historically Black Colleges and Universities (HBCUs), Minority Institutions (MI), Small Business concerns, Small Disadvantaged Business concerns, Service-Disabled, Veteran-Owned Small Business concerns, and HUBZone Small Business concerns are encouraged to submit proposals and to join other entities as team members in submitting proposals.

The Long Range BAA is not a program, but a funding mechanism. As such, it does not have a pre-defined level of funding allocated to it. For this reason, the provision of funds is an important consideration when an otherwise promising proposal is evaluated. A subset of S&T Directorate funding may be obligated through the LRBA should there be R&D proposals of sufficient interest. The source and type of funding for LRBA awards will be determined on a case by case basis per individual award. It is the division’s prerogative to fund the full amount of the proposal or just a portion; this typically depends on the value of the solution to the division. Many solutions that are ultimately funded through the LRBA are valued between \$150,000 and \$1,000,000.

We make every effort to evaluate submissions in a timely fashion. In general, this means Offerors will receive a notification of results approximately 60 days after the date of a white paper submission and 120 days after the date of a full proposal submission. For additional information, including submission instructions, evaluation criteria, and to apply online, go to <https://baa.st.dhs.gov/>. The DHS S&T point of contact for the Long Range BAA is Mr. W. Adrian Groth at [adrian.groth@hq.dhs.gov](mailto:adrian.groth@hq.dhs.gov) or (202) 254-6928.

## Commercialization Office

The DHS S&T Commercialization efforts are conducted by the Commercialization Office, established in October 2008, and headed by the DHS Chief Commercialization Officer Thomas A. Cellucci, Ph.D., MBA. Commercialization is broadly defined as the process of developing markets and producing and delivering products or services for sale.

The Commercialization Office is responsible for creating initiatives that identify, evaluate and commercialize technology for the specific goal of rapidly developing and deploying products and services that meet the specific operational requirements of the Department of Homeland Security's Operating Components and its other stakeholders such as first responders and critical infrastructure/key resources (CIKR) owner/operators and other stakeholders. The Commercialization Office is responsible for developing and driving the implementation of the processes for DHS S&T's outreach with solution developers in the private sector to establish and foster mutually beneficial working relationships that facilitate cost-effective and efficient product/service development efforts. The Commercialization Office works to leverage the private sector's resources to develop Commercial-Off-The-Shelf (COTS) products aligned specifically to meet DHS stakeholders' detailed operational requirements.

The Commercialization Office assists the private sector by enabling them to learn about DHS business opportunities, and plays a vital role internal to DHS to coach, teach and assist project managers, transition managers, division heads and stakeholders in developing detailed operational requirements through recently published books, tutorials and teaching materials that are an integral part of the Commercialization Office's major program initiatives.

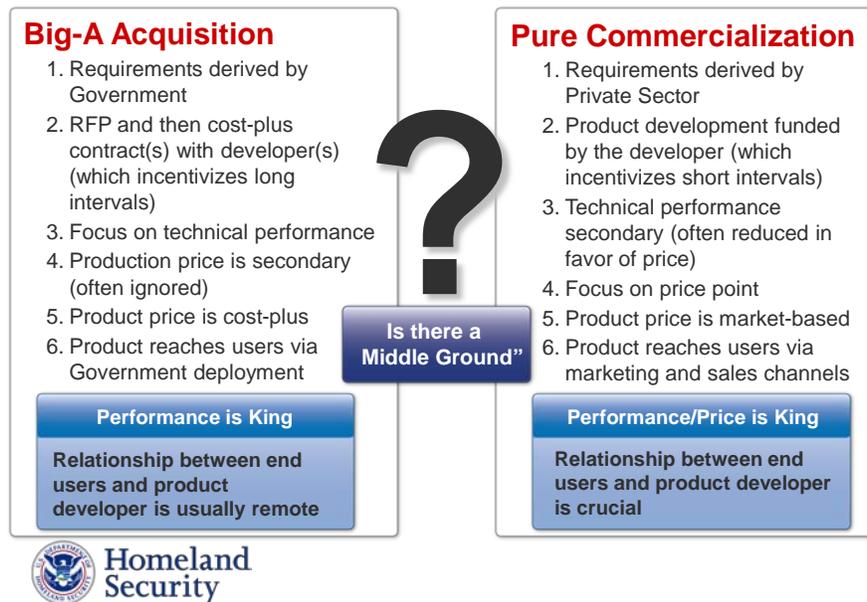
### Mission

The mission of the Commercialization Office is to develop and execute programs and processes that identify, evaluate and commercialize widely-distributed products or services that meet the operational requirements of the Department's operating components, first responder community and other Department end users such as CIKR owners and operators, when required. Developing and managing DHS S&T's outreach effort with the private sector to establish and foster mutually-beneficial working relationships leading to the fielding of technologies to secure the Nation is a primary function of the Commercialization Office. The Commercialization Office has four major activities: Requirements Development, the Commercialization Process, Public-Private Partnership Programs and Private Sector Outreach.

### Commercialization Process

Why is there a need for a commercialization process? DHS requirements, in most instances, are characterized by the need for widely distributed COTS (Commercial-Off-The-Shelf) products. Oftentimes, the need is for thousands, if not millions, of products for DHS' seven operating components and the fragmented, yet substantial first responder and CIKR markets. Figure 18 shows the major differences between a "pure" Acquisition versus "pure" commercialization processes.

## Two Models for Product Realization



13

Figure 18 Comparison of “Pure Acquisition” versus “Pure Commercialization” models for product/system development.

The Commercialization Office has developed from these product development cycles a “hybrid” commercialization model in which DHS serves as the primary developer of detailed operational requirements documents along with a thorough analysis and estimate of the potential available market(s) that are readily shared with the private sector through public-private partnerships that allow for collaborative product/service development. The bullets below delineate the overall description of DHS’ new commercialization model.

- Development of a Commercialization-based Operational Requirements Document (C-ORD)
- Assessment of addressable market(s) to develop the potential available market (PAM)
- Publish C-ORD and conservative estimate of the PAM on public DHS web portal, soliciting interest from potential partners
- Execute a no-cost Cooperative Research and Development Agreement (CRADA) with multiple private sector entities, transferring technology and information (if necessary)
- Develop supporting grants and standards as necessary
- Assess operational test and evaluation (T&E) performance after a product/service is developed
- New Commercial-off-the-shelf (COTS) product marketed by the private sector with DHS imprimatur

To execute this hybrid commercialization model, the Commercialization Office launched its first private sector outreach program, called the SECURE program, in June 2008 to develop products and services in a private-public “win-win” partnership described in detail at [www.dhs.gov/xres/programs/gc\\_1211996620526.shtm](http://www.dhs.gov/xres/programs/gc_1211996620526.shtm). The SECURE Program is based on the simple premise that the private sector is willing and able to use its own money, resources, expertise and experience to develop and produce fully developed products and services for DHS if significant market potential exists. The private sector has shown remarkable interest in devoting its time and resources to

such activities, if and when an attractive business case can be made related to large revenue/profit opportunities, which certainly exist at DHS and its ancillary markets. The private sector requires two pieces of critical information from DHS: 1. detailed operational requirement(s), and 2. a conservative estimate of the potential available market(s). This information can then be used to generate a business case for possible private sector participation in the program.

What a commercialization-based public-private partnership offers to the private sector is detailed information and opportunity. The public sector has turned into the “consumer” in this free market scenario, who literally gives the private sector a detailed description of what they need, as well as insight into which agencies would be interested in potentially purchasing a product/service that fulfills these requirements. While it remains prudent business to verify this kind of information, there is considerable value for the private sector to obtain this information because four things are provided to the private sector that would not happen in normal market dynamics: 1) decreases in resources spent researching the market; 2) increases in time and money spent can now be focused on product design and manufacturing; 3) reduces risk of the research data being incorrect, and 4) provides an estimate as to how large the potential market can be.

The development and communication of detailed requirements or needs is the cornerstone to the success of these public-private partnerships. The public sector’s ability to collect the needs of its stakeholders will catalyze and support the future actions of the partnership. Requirements definition creates a method in which appropriate decisions about product or system functionality and performance can be made before investing the time and money to develop it. Effective communication with and access to the stakeholders of a given agency will bring greater clarity and understanding to the challenges that they face. Understanding requirements early in the search for solutions removes a great deal of guesswork in the planning stages and helps to ensure that the end-users and product developers are “on the same page.”

In this partnership model, the proactive articulation and sharing of requirements and needs provides the necessary starting point to begin effective communication with private sector partners. Openly publishing the needs or requirements of public sector stakeholders has a number of ancillary benefits for those involved. A common challenge for solution developers has been a general lack of insight into the exact needs of public sector stakeholders. Instead, the private sector attempts to develop solutions that may not exist and try to sell products based on the merit of its capabilities and features rather than its ability to solve the specific problem of the users. This is a situation where “a solution defines a problem” that it can solve, rather than the problem guiding the development of a solution to close a “capability gap.”

Requirements provide criteria against which solutions can be tested and evaluated. They offer detailed metrics that can be used to objectively measure a possible solution’s effectiveness. Detailed operational requirements will guide product development so that solutions’ specifications actively solve the stated problem(s). The effective articulation of the requirements creates the mindset in which fulfilling requirements becomes the focus of product development. This requirements-led method places the users’ need at the center of all future actions so that solutions are developed and delivered quickly and efficiently.

With more knowledge about the needs and requirements of their potential customers, the private sector is in a better position to consider how their current technology offerings align to needed capabilities. The next thing that must be considered is how many potential users are in a given market to determine if investment of additional resources to develop the solution will provide the necessary returns. In many cases, the market for a commercialization-based public-private partnership is substantial, composed of millions of potentially funded users. In addition, many government agencies across the federal, state, and local government levels may have similar requirements for products and services (if the ability to modify and add or take away options is available). Furthermore, the products developed for the government can often be sold in civilian markets such as critical infrastructure and key resources owners and operators. Even if the government does not purchase a specific company's product, in many cases it can still be useful and have value for non-governmental applications.

Innovative ideas flow freely in the private sector, most especially from small businesses. There is a demand for these innovative technologies as other private sector companies begin to position themselves to address these newly emerging commercial markets found in the private sector. Mergers and acquisitions continue to take place in the private sector as larger companies and investors seek to build their enterprises. Discovering the potential benefits of partnering with the public sector has demonstrated its attractiveness to investor communities like venture capitalists and angel investors. This investment has created more opportunities for those innovative ideas to grow and develop into fully deployable products. Sharing information like needs and requirements provides a defined target that allows those private sector partnerships to take hold. These strategic partnerships are becoming more common and it is now a regular event for these strategic partners to pursue the public sector together to engage and demonstrate new technology offerings.

A commercialization-based public-private partnership benefits the public sector because the private sector competes in an open and transparent way for the public sector's purchase potential and business. Since companies and businesses openly receive information about the requirements or needs of an identified market, multiple companies may competitively make products/services that meet requirements at the lowest cost to the potential buyer. The end user benefits by being able to purchase the best product at the lowest price.

The taxpayer wins in a commercialization-based public-private partnership because their tax money is not spent on research and development for the private sector. Normally the government pays a company for research and development, yet many products/services are *not* developed. All of this is funded by taxpayers' money, often without much benefit to society. In a commercialization-based public-private partnership, the research and development of the product is *not* paid by government. It is the private-sector that spends money on research and development, and then sells the product to the government at the lowest price. This results in saving the taxpayer money as well and, in fact, expands the net realizable budgets of the private sector.

Given the current economic situation facing our country, it becomes increasingly important for the public sector to make wise investments of its time, money and resources. Most government agencies do not have the budgets necessary to complete every research and development project that they would like to undertake. The effective prioritization of programs is critical to managing the limited resources

available to various agencies. Rigorously developed requirements for each project facilitate these prioritization efforts and increase the ability to perform critical analyses of alternatives (AoAs) used in determining the best course of action to solve a problem. An analysis of alternatives will uncover a great deal of information on potential solutions that may already exist and is a necessary consideration before pursuing a commercialization public-private partnership. When successful, the option to utilize commercialization public-private partnerships to solve a problem frees resources for those projects that require significant government involvement and expenditure of resources.

The Department of Homeland Security (DHS) through the Science & Technology Directorate (S&T) initiated an innovative commercialization-based public-private partnership called the System Efficacy through Commercialization, Utilization, Relevance and Evaluation (SECURE) Program. The SECURE Program leverages the resources, experience and expertise to develop and deliver fully deployable solutions aligned to the detailed operational requirements of DHS' many stakeholders. The SECURE Program covers the needs of all of the DHS stakeholders including the operating components (FEMA, TSA, CBP, Secret Service, ICE, USCIS and Coast Guard), but most especially first responders (local police and fire department, hospitals, rescue teams) and critical infrastructure/key resources (CIKR) owners and operators, representing a large market for potential private sector partners. It is the role of DHS to ensure that these stakeholders are provided with the mission-critical capabilities that they need in order to perform their jobs well.

The SECURE Program was developed as a way to address requests for assistance from DHS stakeholders to find better solutions to their problems. These stakeholders were used to a culture where vendors presented "solutions looking for problems" and wanted to find a better way to not only have solutions developed to address their needs, but also to have some assurance that the products being sold to them have been thoroughly tested and evaluated in real operational environments. The requirements of these stakeholders are gathered and articulated in a Commercialization Operational Requirements Document (C-ORD). When appropriate, approved C-ORDs are posted online so that potential solution providers or vendors with capability offerings may apply for participation in the SECURE Program. In an open and freely competitive way multiple vendors are able to offer potential solutions to provide the required capabilities outlined in a given C-ORD.

It is important to stress the relationship that DHS has with its non-federal stakeholders in the first responder and CIKR communities. DHS has direct authority over its operating components and can directly influence acquisition activities. This same relationship does not extend to its non-federal stakeholders who are responsible for managing their own budgets and purchasing decisions. Because the SECURE Program is not a procurement activity, DHS is able to share valuable information about its non-federal stakeholders to the private sector and gain knowledge about potential solutions without the need for contracts or monetary exchanges. First responders and non-federal stakeholders now have a unified voice to convey their needs or requirements and gain from the collective size as potential available markets.

The SECURE Program, in addition to leveraging cooperative public-private partnerships, incorporates a rigorous review process based on rigorous operational test and evaluation (OT&E) to ensure that the operational performance of a system is directly aligned to stated stakeholder requirements,

but also that the system meets or exceeds the stated performance of the private sector vendor or supplier. This review process analyzes capability requirements in addition to an evaluation of the systems safety record, quality assurance criteria, performance limitations and other considerations to ensure that when a system is deployed in the field it is both effective and safe.

Its “sister program,” FutureTECH focuses on the long-term needs of the Department that require the development of new technologies to address future capability gaps. We have demonstrated through the SECURE and FutureTECH programs that the federal government can engage and influence - in a positive way - the private sector by offering detailed requirements and conservative estimates of potential market(s). The reason that these partnerships are successful is simple and straightforward: firms spend significant resources in trying to understand market needs and potentials through their business and market development efforts. By offering this information, government saves the private sector both time and money while demonstrating its genuine desire to work cooperatively to develop technologies and products to meet DHS stakeholders’ needs in a cost-effective and efficient way.

After providing independent third-party testing and evaluation of potential products, services or technologies to show they do in fact meet or exceed the requirements listed in the detailed operational requirements, private sector entities can potentially enter into a partnership with the Department in order to deliver commercial-off-the-shelf (COTS) products to the Department’s stakeholders. In addition to providing products to DHS and its stakeholders, these partnership programs, SECURE<sup>8</sup> and FutureTECH<sup>9</sup> give the much needed assurance to the First Responder and CIKR communities that a certified product or service works as specified and is aligned to a requirements document.

The products that are developed through this partnership (even the ones that were not purchased by DHS) can be offered to other private sector entities, such as airport security, school and university security, and security for professional sports and concerts, many of whom support the defense of critical infrastructure and key resources nation-wide. There is then an increase in public safety and security, all while the private sector, public sector and taxpayer benefit from the partnership.

Early response from groups within DHS, the private sector, and first responders about this process and programs like SECURE™ has been very favorable<sup>10</sup>. The Department plans to regularly update its website with Commercialization Operational Requirements Documents (C-ORDs) to continually expand this innovative private-public partnership. In addition, as evidenced in Figure 19, the taxpayers, private sector and public sector view programs like this as “win-win-win.”

---

<sup>8</sup> Cellucci, Thomas A. “Commercialization Office: Offering Transformational Change Beyond DHS,” June 2009.

<sup>9</sup> Cellucci, Thomas A. “FutureTECH: Guidance to Understanding Future DHS S&T Critical Research/Innovation Focus Areas,” April 2009.

<sup>10</sup> Margetta, R. “S&T Official Working to Move Product Development Out of DHS, Into Private Sector,” Congressional Quarterly Homeland Security. June 27, 2008.

<b>Benefit Analysis – “Win-Win-Win”</b>		
<b>Taxpayers</b>	<b>Public Sector</b>	<b>Private Sector</b>
1. Citizens are better protected by DHS personnel using mission critical products	1. Improved understanding and communication of needs	1. Save significant time and money on market and business development activities
2. Tax savings realized through private sector investment in DHS	2. Cost-effective and rapid product development process saves resources	2. Firms can genuinely contribute to the security of the Nation
3. Positive economic growth for American economy	3. Monies can be allocated to perform greater number of essential tasks	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work.
4. Possible product “spin-offs” can aid other commercial markets	4. End users receive products aligned to specific needs	4. Significant business opportunities with sizeable DHS and DHS ancillary markets
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. End users can make informed purchasing decisions with tight budgets	5. Commercialization opportunities for small, medium and large business

**Figure 19 The SECURE™ Program is viewed positively by DHS stakeholders. The success of the program lies in the fact that all participants receive significant benefits.**

## DHS S&T Research Council

**Purpose.** The DHS S&T Research Council supports, facilitates, and promotes collaboration across the Directorate on basic research-related matters to ensure a comprehensive, integrated basic research portfolio while maintaining the appropriate flexibility for its member organizations. The Research Council is an advisory body to the Director of Research and to its members.

**2. Membership.** The membership of the Research Council includes representatives from the organizations within S&T who manage or contribute to basic research efforts. The members of the Research Council are:

**a. Chair:** DHS S&T Executive Director of Research & Development Partnerships

**b. Permanent Members:**

- i. DHS S&T Division Research Leads
- ii. DHS S&T Director of the Office of University Programs (OUP)
- iii. DHS S&T Director of the Office of National Laboratories (ONL)
- iv. DHS S&T Program Executive Officer – Counter-Improvised Explosive Devices [PEO (C-IED)]
- v. DHS S&T International Programs Representative

**c. Invited Participants (as needed)**

Expectations of members and participants:

- Attend meetings or ensure an alternate is present
- Prepare for meetings and consider advance material provided
- Participate in discussions and offer recommendations
- Participate in data-gathering efforts as requested
- Relay information to Division leadership and staff as appropriate

**3. Objectives.** The DHS S&T Research Council provides a forum for the members to work together, share ideas, understand each others' portfolios, integrate and coordinate efforts, and collaborate on efforts of mutual interest. Through the Research Council, members are made aware of best practices implemented by their colleagues in the execution of their research portfolios. These best practices are vetted through the Research Council and then codified in the Basic Research Strategy. The efforts of the Research Council emphasize integration, coordination, collaboration, facilitation, and (as appropriate) consistency of approach.

## Keep it Simple and Make it Easy

Open and free communication creates opportunities for engagement, understanding and partnership. It is our goal at the R&D Partnerships Group to be proactive in not only sharing information, but provided information that is detailed, well-articulated and sparks action. It is not enough for our Group to share information, but to do it in a way to promotes all efforts and opportunities offered by our diverse membership. Effective communication opens opportunities to create greater awareness and understanding across the Homeland Security Enterprise. Figure 20 shows our approach to open communication and fostering partnerships that deliver results.

## Three Step Approach: Keep it Simple and Make it Easy



Figure 20 A communications plan that everyone understands.

It is important for the R&D Partnerships Group to serve as “transmitters and receivers” of information that allow for greater involvement and contributions from many partners.

## Help Us to Help You

The Private Sector outreach efforts of the R&D Partnerships Group focus on informing the public on “How to do Business with DHS.” These efforts receive positive feedback from the private sector and media. Outreach efforts center on notifying the private sector about opportunities that exist for partnership and business development to address the needs of the Department and are conducted through invited talks to trade conventions, reaching small, medium and large businesses. Appendix B of the book contains an

Outreach Workshop model that has been used successfully by the R&D Partnerships Group to share information about the vast competencies of the Group and numerous opportunities to engage with us.

The R&D Partnerships Group conducts outreach to businesses of all sizes – including minority-owned, HUBZone, veteran-owned and other disadvantaged business. It is well known that much of our nation’s (and the world’s) innovation emanates from small business, but they often find some of their most difficult challenges with raising capital or performing effective market research necessary for business growth. To address these challenges, we have visited and met with thousands of small business owners, CEOs and entrepreneurs/innovators across the United States to inform them of the business opportunities that exist at the U.S. Department of Homeland Security (DHS). In addition, we have developed a series of books recently published by DHS that small businesses can use to augment and enhance their ability to efficiently and cost-effectively develop market-driven products and/or services. We have also produced numerous well-received articles and materials germane to small business. Refer to [http://www.dhs.gov/xres/programs/gc\\_1234200779149.shtm](http://www.dhs.gov/xres/programs/gc_1234200779149.shtm) for more detailed information and access to all of these useful resources.

The R&D Partnerships Group continues to travel extensively throughout the United States to meet with small business through our Science and Technology (S&T) Directorate private sector outreach efforts. Statistical information on these efforts is posted to our website address above and updated on a quarterly basis. It is also important to note that DHS has a number of valuable resources businesses may explore. Below is a handy reference for businesses wishing to do business with DHS:

U.S. Department of Homeland Security and other Federal Contact Information: DHS and/or Federal Contact	Description	Contact Information
<b>Private Sector Office</b>	Part of the DHS Office of Policy, the Private Sector Office engages individual businesses, trade associations and other nongovernmental organizations to foster dialogue with the Department. It also advises the Secretary on prospective policies and regulations and in many cases on their economic impact. The Private Sector Office promotes public-private partnerships and best practices to improve the nation’s homeland security, and promotes Department policies to the private sector.	<a href="http://www.dhs.gov/xabout/structure/gc_116622019104_2.shtm">http://www.dhs.gov/xabout/structure/gc_116622019104_2.shtm</a>
<b>Federal Business Opportunities (Fed Biz Opps)</b>	“Virtual marketplace” that captures the official Federal government procurement opportunities allowing contractors to retrieve services posted by government buyers.	<a href="https://www.fbo.gov/">https://www.fbo.gov/</a>
<b>Small Business Innovation Research (SBIR)</b>	SBIR is a set-aside program (2.5% of an agency's extramural budget) for domestic small business concerns to engage in Research/Research and Development (R/R&D) that has the potential for commercialization.	<a href="https://www.sbir.dhs.gov/">https://www.sbir.dhs.gov/</a>
<b>Small Business Assistance</b>	Provides numerous resources, links and contacts to ensure that small companies have a fair opportunity to compete and be selected for Department of Homeland Security contracts.	<a href="http://www.dhs.gov/xopnbiz/smallbusiness/">http://www.dhs.gov/xopnbiz/smallbusiness/</a>
<b>Mentor-Protégé Program</b>	Designed to motivate and encourage large business prime contractor firms to provide mutually beneficial developmental assistance to small business, veteran-owned small business, service-disabled veteran-owned small business, HUBZone small business, small disadvantaged business, and women-owned	<a href="http://www.dhs.gov/xopnbiz/smallbusiness/editorial_0716.shtm">http://www.dhs.gov/xopnbiz/smallbusiness/editorial_0716.shtm</a>

	small business concerns.	
<b>SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program</b>	An efficient and cost-effective program to foster cooperative "win-win" partnerships between the U.S. Department of Homeland Security and the private sector. The Department works with the private sector to develop products, systems or services aligned to the needs of its operating components, first responders and critical infrastructure/key resources owners and operators – representing in many cases, large potential available markets.	<a href="http://www.dhs.gov/xres/programs/gc_1211996620526.shtm">http://www.dhs.gov/xres/programs/gc_1211996620526.shtm</a>
<b>S&amp;T Directorate – Homeland Security: DHS and/or Federal Contact</b>	<b>Description</b>	<b>Contact Information</b>
<b>TechSolutions Program</b>	Established to provide information, resources and technology solutions that address mission capability gaps identified by the emergency response community. The goal of TechSolutions is to field technologies that meet 80% of the operational requirement, in a 12 to 15 month time frame, at a cost commensurate with the proposal but less than \$1 million per project.	<a href="http://www.dhs.gov/xfrstresp/trainin/gc_1174057429200.shtm">http://www.dhs.gov/xfrstresp/trainin/gc_1174057429200.shtm</a>
<b>DHS SBIR Program</b>	The DHS SBIR program is a set-aside program (2.5% of the S&T Directorate’s extramural research and development budget) for domestic small business concerns to engage in Research/Research and Development (R/R&D) that has the potential for commercialization. Two solicitations are released each year in the November and May timeframes.	<a href="https://www.sbir.dhs.gov/">https://www.sbir.dhs.gov/</a>
<b>SAFETY (Support Antiterrorism by Fostering Effective Technologies) Act</b>	Part of the Homeland Security Act of 2002, the SAFETY Act encourages the development and deployment of anti-terrorism technologies to protect the nation and provide “risk management” and “litigation management” protections for sellers of qualified anti-terrorism technologies and others in the supply and distribution chain.	<a href="https://www.safet yact.gov/">https://www.safet yact.gov/</a>
<b>Homeland Security Advanced Research Projects Agency (HSARPA)</b>	Manages a broad portfolio of solicitations and proposals for the development of homeland security technology. HSARPA performs this function in part by awarding procurement contracts, grants, cooperative agreements, or other transactions for research or prototypes to public or private entities, businesses, federally funded research and development centers, and universities.	<a href="https://baa.st.dhs.gov/">https://baa.st.dhs.gov/</a>
<b>SECURE Program</b>	Please refer to the description above.	<a href="http://www.dhs.gov/xres/programs/gc_1211996620526.shtm">http://www.dhs.gov/xres/programs/gc_1211996620526.shtm</a>
<b>Unsolicited Proposals</b>	Composed of several component agencies which handle different types of acquisitions. This Department has several resources, links and contacts if a given small company has products or services which may be of interest to one or more of DHS component agencies.	<a href="http://www.dhs.gov/xopnbiz/opportunities/editorial_0617.shtm">http://www.dhs.gov/xopnbiz/opportunities/editorial_0617.shtm</a>

To put it simply, the R&D Partnerships Group welcomes the prospect of working with all kinds of businesses, including providing seminars and resources on how to raise capital and form strategic partnerships.

## Summary

The DHS S&T Research & Development Partnerships Group manages a set of core competencies that provide measurable value to DHS S&T in facilitating “win-win” working relationships with members of the Homeland Security Enterprise (HSE) comprised of both government and non-government agencies and organizations. The R&D Partnerships Group assists in both “transmitting and receiving information” to stakeholders across the HSE. Our Group enables collaboration opportunities for evaluating, expediting and monitoring the execution of programs with an increased speed-of-execution compared to “in-house only” activities. Our diverse and talented collection of expertise, capabilities and experience enhances the Group’s ability to deliver results and create significant impact in providing the HSE with high-impact capabilities that secure our Homeland.

- The Small Business Innovation Research (SBIR) program stimulates technological innovation; uses small business to meet federal research/R&D needs; fosters and encourages participation by socially and economically disadvantaged; and increases private sector commercialization of innovation increasing competition, productivity and economic growth.
- The Long Range Broad Agency Announcement (BAA) is an acquisition solicitation vehicle to receive proposals from the community and fund selected proposals for development to solve operational needs and requirements.
- Interagency Division maintains various MOUs and MOAs with other government agencies for information sharing and collaboration.
- The Office of National Laboratories creates open lines of communication to the national labs to leverage their research and afford opportunities to engage directly with their scientists.
- The Office of SAFETY Act Implementation provides liability protection for anti-terrorism technologies and enables deployment of needed capabilities in high-risk situations.
- Homeland Security S&T Advisory Council (HSSTAC) serves as a source of independent, scientific and technical planning advice for the Under Secretary for Science and Technology.
- The Technology Transfer maintains the Department’s technology transfer activities (technical assistance, patent licenses, CRADAs, partnership intermediary agreements, etc.) in accordance with the Federal Technology Transfer Act of 1986.
- International Cooperative Programs Office has established several bi-lateral agreements with international partners to facilitate information sharing and cooperative science and technology research and development.
- The Office of University Programs monitors the activity of the 12 national Centers of Excellence (COEs) that focus on multidisciplinary research and education for homeland security solutions.
- The Commercialization Office has a repository of direct business contacts as well as a detailed chart that tracks thousands of company capabilities and their alignment to S&T’s high priority needs.
- The DHS S&T Research Council gathers subject matter experts on advanced research and emerging technologies in a collaborative way to identify areas of research focus across the HSE.

# Appendix A: R&D Partnerships Group Opportunities Guide

# DHS S&T R&D Partnerships Group Opportunities Guide

Opportunity  Activity, Vehicle, or Program	Major Business Opportunities												Engagement Opportunities						Education Opportunities			
	Research and Funding Opportunities	Product/Technology Designations and Certifications	Public-Private Partnerships	Licensing	CRADAs	Small Business Focus	Minority/Disadvantaged Business Focus	Potential Available Market (PAM) Estimates	Product Liability Protection	Intellectual Property	Requirements/Needs Sharing	Product/Technology Evaluation	Trade Shows/Conferences	Marketing Initiatives	"Start Up" America	OSTP	Council on Competitiveness	"One-on-One" Meetings	Technology Development Resources	Product Realization Models	Requirements Development Materials	Workshops
SBIR	X		X	X		X	X	X		X	X		X	X	X	X		X	X			X
SAFETY Act		X				X	X	X	X	X		X	X	X	X	X	X	X	X			X
Long Range BAA	X					X	X			X	X	X		X	X			X				X
SECURE Program		X	X		X	X	X	X		X	X	X	X	X	X	X	X	X		X	X	X
FutureTECH Program		X	X		X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X
Tech Transfer	X		X	X	X	X	X	X		X		X	X	X	X	X		X	X	X	X	X
Centers of Excellence	X		X			X	X			X			X	X	X	X	X	X	X	X		
MOUs/MOAs			X							X	X			X	X							
International Agreements	X		X					X		X	X		X									
Market Scans			X			X	X	X					X	X		X	X					
Technology Scans			X			X	X	X					X	X		X	X		X			
Market Research			X			X	X	X					X	X		X	X	X				
Technology Research			X			X	X	X					X	X		X	X	X	X			
Valuation Models			X											X	X	X						
DOE National Labs				X	X					X								X	X			
S&T Labs				X	X					X								X	X			
HSSTAC/NSTC																						
S&T Research Council																			X	X		

# Intra-DHS Opportunities Guide

Opportunity  Activity, Vehicle, or Program	Intra-DHS Information Sharing Opportunities										
	Databases	Contacts	Program Management Tools	Global Research Opportunities	Requirements Generation/Vetting	Standards Generation/Vetting	Capabilities Repositories	International Opportunities	Interagency Opportunities	Trip/Activity Reports	Strategic Planning Tools
SBIR	X	X	X	X			X		X	X	X
SAFETY Act	X	X	X	X		X	X	X	X	X	X
Long Range BAA	X	X	X	X	X	X	X	X		X	X
SECURE Program	X	X	X	X	X	X	X	X	X	X	X
FutureTECH Program	X	X	X	X	X	X	X	X	X	X	X
Tech Transfer	X	X		X	X	X	X	X	X	X	
Centers of Excellence	X	X		X			X		X	X	
MOUs/MOAs	X	X	X	X	X	X	X	X	X	X	X
International Agreements	X	X		X	X	X	X	X		X	
Market Scans	X	X	X	X			X	X	X	X	X
Technology Scans	X	X	X	X			X	X	X	X	X
Market Research	X	X	X	X			X	X	X	X	X
Technology Research	X	X	X	X			X	X	X	X	X
Valuation Models	X		X	X							X
DOE National Labs				X	X	X	X	X	X		X
S&T Labs				X	X	X	X	X	X		X
HSSTAC/NSTC			X								X
S&T Research Council			X	X		X					X