Crossing the "Valley of Death": Transitioning Cybersecurity Research into Practice

Douglas Maughan
Department of Homeland Security, Science and Technology Directorate

David Balenson, Ulf Lindqvist, Zachary Tudor
SRI International

Abstract—New and innovative technologies will only make a difference if they are deployed and used. It does not matter how visionary a technology is unless it meets the needs and requirements of customers/users and it is available as a product via channels that are acceptable to the customers/users. One of the biggest ongoing challenges within the cybersecurity research community is transitioning technology into commercial or open source products that are available in the marketplace. This article presents a research and development (R&D) execution model developed to significantly increase the success rate of technology transition, based on experience from cybersecurity programs in R&D funding agencies. To illustrate the effectiveness of the model, we describe several examples of successful technology transition from the cybersecurity R&D program at the United States Department of Homeland Security, Science and Technology Directorate (DHS S&T).

Keywords: technology transition, cybersecurity, research and development, open source, small business

I. INTRODUCTION

The challenges of transitioning[1] technology from research to real-world deployment occur in all areas of technical research, and are generally not unique to cybersecurity. However, at this time, it is extremely important to significantly improve the success rate of technology transition in the cybersecurity field. The cybersecurity problem is bigger than ever, with government and industry being victims of severe attacks, including successful attacks against companies that specialize in security technology. For the past several years, we have seen rampant

[1] We use the term *technology transition* to broadly describe all efforts to ensure that technologies developed in research settings will eventually be deployed and used operationally. We do not make the distinction between *technology transition* and *technology transfer* that is sometimes used in the DoD community.

theft of sensitive information and intellectual property. We are also starting to see destructive attacks, some even targeting critical infrastructures. New and innovative solutions are desperately needed to get the problem under control, and those solutions must be widely deployed in operational settings to make a difference. Two key actions are needed, on a national level: 1) We need to increase R&D funding levels, and 2) we need to get much better at taking the best results of R&D all the way to deployable solutions. If we were to fail to accomplish both of these actions, the nation would be set up for a disaster some years from now, when it would not have security solutions developed to match the challenges of the rapidly evolving world of information technology. It is therefore in the best interest of our entire society to make sure that technologies are transitioned from the research into the hands of users.

There are many promising technologies that are currently undergoing research and development, and while that is absolutely necessary, it is not sufficient. We cannot afford to have technologies be put on a shelf because the funded projects ended and the researchers moved on to new problems that were yet unsolved. When a solution to a problem is being developed, we must also ensure that the solution meets the needs and requirements of users and it is made available for deployment via channels that are acceptable to the users. To achieve widespread operational deployment and use, solutions can for example be made available directly to users as commercial products or as open source, or indirectly by providers or operators of critical infrastructure.

There are many reasons why technology transition does not happen easily. It is usually not an issue of researchers being unwilling to support transition – most researchers want to see their work have an impact – but good intentions are unfortunately not sufficient. There are differences in the personality types and skills that are suitable for computer science and engineering research versus those that are suitable for business, customer interaction, and entrepreneurship. There are counterexamples of successful individuals who possess all those skills, but it is a rare phenomenon. Incentives to encourage technology transition may also be lacking. A researcher whose success is measured in the number of peer reviewed publications and academic honors may not be motivated to spend a lot of time and energy on technology transition. Depending on the research organization, there may or may not exist direct financial incentives for researchers to pursue commercialization of their results, such as royalties or shares of a startup company. Even when such financial incentives exist, they may not serve as sufficient motivation due to the personalities and organizational culture often found in research environments. Furthermore, if research project funding does not explicitly include technology transition efforts, researchers may not be able to perform the work associated with transition unless they can find another way to fund it.

A metaphor that is often used to illustrate the challenging gap that exists between research on one hand, and operational technology use on the other, is “The Valley of Death” – see Figure 1. The first use of The Valley of Death metaphor to describe the gap that must be bridged in a successful technology transition effort is attributed to Congressman Vern Ehlers [1][2], and variations of this theme have since been used.

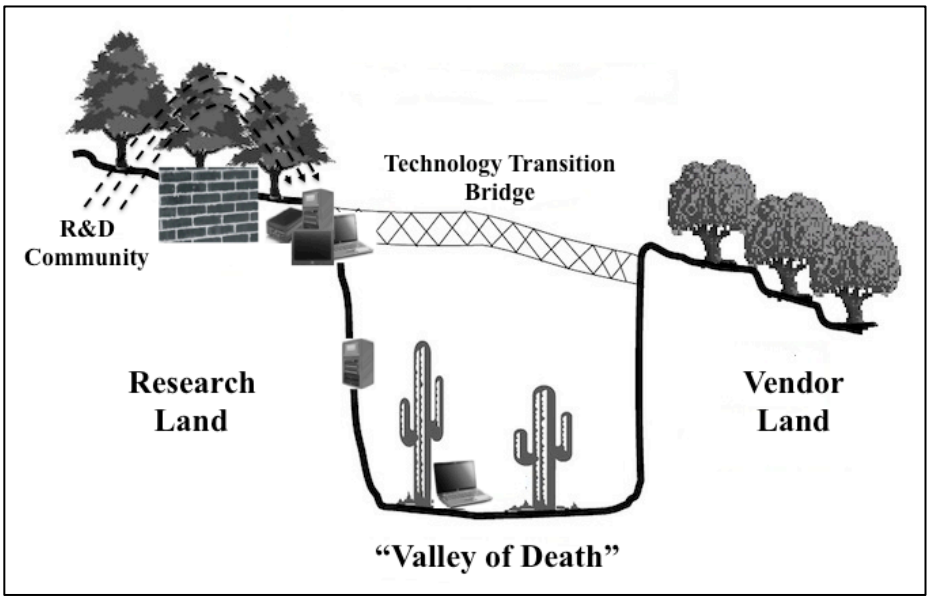

Figure 1 - The Valley of Death Between Research and Industry

Numerous studies have been performed and reports written on the difficulties and challenges of technology transition in Government-funded R&D and approaches to overcoming those challenges. A 2004 National Academy of Sciences report, *Accelerating Technology Transition: Bridging the Valley of Death for Materials and Processes in Defense Systems* [3][4], noted inefficiencies and long delays in the transition of new technologies due to complexities in the research, development, and transition processes and differences in the goals, timeframes, and funding levels of the different players in the process (researchers, industry and operational users). The report identified active collaboration among researchers, industry, and operational users during all phases of technology transition as a key goal for success. Similarly, a 2007 *Department of Defense Report to Congress on Technology Transition* [4], cited evidence of a chasm between the Science and Technology (S&T) and acquisition communities, i.e., the "valley of death", which could be bridged only through cooperative efforts and investments by both communities. A 2009 GAO Report to Congress on Technology Transfer in Department of Energy Labs [5] attributed limitations in the extent to which technologies are commercialized to gaps in staff expertise, lack of funding, and lack of flexibility in negotiating agreements with outside parties.

To overcome these challenges and improve the technology transition track record in the cybersecurity R&D community, we need to share experiences, working models, and best practices for technology transition. In this article, we present a research and development (R&D) execution model developed to significantly increase the success rate of technology transition, based on experience from cybersecurity programs in R&D funding agencies. While the model was developed by the cybersecurity R&D program at the United States Department of Homeland Security,

Science and Technology Directorate (DHS S&T), it is generally applicable to other R&D organizations. In fact, other R&D funding agencies already practice portions of the model.

Despite the challenges, the DHS S&T cybersecurity R&D program has successfully transitioned a number of R&D technologies from research into widespread deployment and use where they are having a real impact on operational cybersecurity. IronKey received R&D funding to develop a secure universal serial bus (USB) device and has grown from a small start-up into a thriving company supporting widespread use of their product. Endeavor Systems received Small Business Innovative Research (SBIR) funding to develop a botnet detection and mitigation tool that led to their acquisition by McAfee. And, the Open Information Security Foundation (OISF) received funding the develop Suricata, an open source intrusion detection and protection system, creating a strong development community that continues to develop the product to meet unmet IDS/IPS needs. To illustrate the effectiveness of the R&D execution model, we will further describe these examples of successful technology transition from the DHS S&T cybersecurity program. Such examples serve to show that given the right model, cybersecurity R&D programs can transition research results into operational use where they can have an impact on cybersecurity.

II. KEY ELEMENTS OF TRANSITION SUCCESS

Before presenting the model, we describe some key elements that we find to be vital to repeatable, successful technology transition, based on our experience and observations:

Pervasive emphasis – by design, technology transition should be an integral part in all aspects of an R&D program. In any program plan, call for proposals, review process, funding vehicles, Principal Investigator (PI) meetings, site visits/reviews, reports, and all other program activities and metrics, technology transition should constitute a key requirement and evaluation criterion.

Early involvement – technology transition should be designed into the program from its first inception. This includes a program plan that is based on a firm understanding of customer needs and requirements.

Active engagement – technology transition is an active sport, where success requires significant effort throughout the entire process. Researchers and program managers must engage the customers (the identified end-users of the technology) and keep them engaged before, during, and after the execution of the research. This includes identifying and selecting specific customers that are ready and able to be involved in the entire process.

Tangible support – the agency that funds the research should also provide its performers with support that is dedicated to technology transition. This includes providing funding for technology transition activities, providing and requiring specialized innovation training for researchers, organizing events such as

technology showcases and matchmaking, and providing introductions and connections between researchers and potential technology customers.

It should be noted that there is not just one single path that can lead to successful technology transition. On the contrary, multiple alternative paths exist and some are better suited than others for certain R&D organizations and customers. **Large companies** gain access to new technologies produced by their own internal R&D teams, or by licensing technology from outside labs or small companies, or by acquiring a small business. The large company would then typically commercialize the technology through their own product portfolio and sales channels. A **small business** such as a startup company can get R&D funding from government agencies, for example via the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs – funding that can boost technology development and supplement funds from other investors. To ultimately be successful, a startup company may require external funding, such as angel funding or venture capital, at some stage of its growth. Experienced venture capitalists are known to provide important support and guidance for technology transition, in addition to providing the funding itself. Licensing and acquisition are avenues that can feed technologies from small businesses into the sales and support apparatus of a large company. For **academia and research labs**, licensing technology directly to an established company can be an effective transition path, while more adventurous and driven researchers who have the right kind of support from their institution can take the path of founding a startup company. While some institutions have offices and programs dedicated to support licensing and ventures, many show remarkably little interest in supporting technology transition and any success is typically the result of extremely dedicated efforts by the inventors themselves. For all R&D sources of new technology, **open source** is an alternative to traditional transition channels. A number of government programs encourage or require technology to be released under open source licensing, as part of the R&D activities. Open source availability is well documented as a powerful and effective means to bring important capabilities into adoption, use, and support by larger communities.

There are many interrelated factors affecting technology transition, including time and schedule, budgets, customer or end-user participation, demonstrations, testing and evaluation, and product partnerships. Given these factors, and because one transition path can be a better fit than another, funding agencies may not want to require a specific transition path (such as open source). Instead, the funding agency should work with each of its performers to help them identify the best transition path depending on the specifics of the R&D organization, the technology, and the customer.

III. A PROVEN R&D MODEL FOR TRANSITION

The R&D execution model is a template for how the key elements of transition success above can be implemented as an integral part of a cybersecurity R&D program. The model is shown in Figure 2 and is affectionately known as the “Circle

of Life". It is comprised of a continuous cycle of requirements gathering, pre-R&D, R&D, and post-R&D activities oriented towards technology transition. The cycle begins with collecting prioritized requirements from customers and critical infrastructure owners and operators. Pre-R&D activities include the development of research agendas to help align research programs with community needs and solicitations that result in research programs focused on satisfying those needs. R&D execution involves program support activities that ensure researchers, program managers, and customers continue to work together to develop innovative technologies that can be transition for operational use. It also involves testing and evaluating technologies with realistic data as an integral part of the research. Post-R&D activities involve technology transition and deployment activities, including technology assessments and evaluations, experiments and pilots, and outreach. Assessments and evaluations ensure that technologies are vetted prior to operational deployment. Experiments and pilot deployments allow technologies to be tested and evaluated with real users in real operational environments. Finally, researchers must also conduct outreach to promote their technologies and attract transition partners. In short, the model includes the full spectrum of necessary activities – research, development, test, evaluation, and transition (RDTE&T) – needed to develop completed "research products" that are tested in the hands of operational end-users and potentially result in widespread deployment and use. We will describe all of these activities in further detail in the following sections.

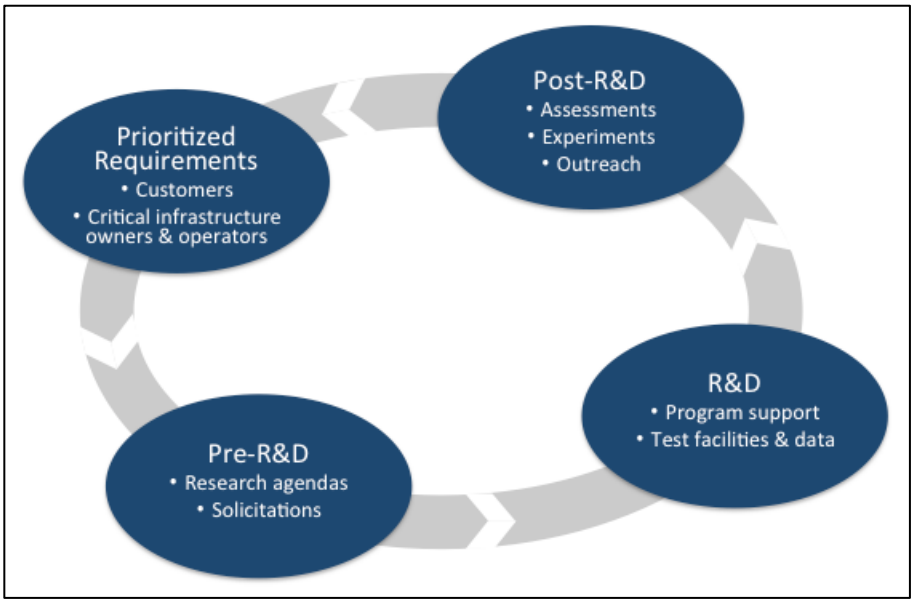

Figure 2 – Cybersecurity R&D Execution Model for Technology Transition

PRIORITIZED CUSTOMER REQUIREMENTS

The model starts with collecting prioritized requirements from customers and critical infrastructure owners and operators. It is essential for researchers and government program managers to know and work with the customers or ultimate users of the technologies that will result from research. Direct interaction with

operational users enables researchers to identify and articulate critical requirements and develop solutions that will solve operation challenges and problems, and fit into operational systems, processes, and procedures. Such interaction is not easy; customers and users are often busy addressing their primary job or mission, with limited time to interact with researchers. Researchers must push their customers to think beyond incremental changes to their existing tools and technology and consider radically new technologies and tools that can solve the problems and needs of the future. Operational needs and requirements must be expressed as research problems that can be understood by researchers. By identifying future needs today, researchers can begin to develop solutions for potential transition tomorrow. If current needs had been expressed yesterday as research challenges, then there would be transitionable technologies available today to satisfy those needs.

PRE-R&D ACTIVITIES – COLLABORATIVE RESEARCH AGENDAS

Having clearly identified and articulated research challenges and requirements helps focus R&D on developing solutions to current and relevant problems. It is important to both contribute to and draw from the collaborative research agendas to ensure alignment of research with overall community priorities. Coordinated US Government cybersecurity R&D efforts and groups include the White House Comprehensive National Cybersecurity Initiative (CNCI), Networking and Information Technology R&D (NITRD), Cyber Security and Information Assurance Interagency Working Group (CSIA IWG), and the Special Cyber Operations Research and Engineering (SCORE). These groups and others have developed a number of national documents that define research agendas and priorities for cybersecurity research. *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program* [6] defines a set of interrelated priorities for U.S. government agencies that conduct or sponsor cybersecurity R&D and organizations that perform the R&D. An inter-agency group comprised of members from DARPA, DHS S&T, DoD, DoE, IARPA, NIST, NASA, NSA, NSF, and others, working in coordination with the academic and industry research community, developed the plan. It describes and prioritizes end-states and capabilities that must be achieved to secure cyberspace and hence provides strategic guidance for R&D efforts. Similarly, DHS S&T's document, *A Roadmap for Cybersecurity Research* [7], provides detailed research and development agendas and defines 11 hard problem areas in cybersecurity, for use by government agencies and the research community. Groups in various critical infrastructure sectors have also defined their own sector-specific research agendas and plans, such as banking and finance [8] and energy [9].

PRE-R&D ACTIVITIES – SOLICITATIONS

The development of solicitations, such as a Broad Agency Announcement (BAA), used to request research proposals and ultimately fund research programs and activities, are another critical aspect of pre-R&D activities. The solicitations must clearly articulate the research goals, objectives, and requirements in order to ensure that the proposed research is properly targeted towards the desired research

problems and needs. The solicitation must identify and provide detailed descriptions of the technical topics areas (e.g., software assurance, enterprise-level security metrics, usable security) so that the researchers can propose solutions that address the right technology needs. The technical descriptions should include necessary background information and references, the problem to be solved, the types of solutions that are potentially applicable, illustrative examples, and performance metrics. The technical topics should be derived from customer requirements and align with an organization's strategic plans as well as external plans, such as those resulting from the collaborative efforts of the CNCI.

Technology transition must be an integral component of a solicitation. Researchers must be compelled to consider technology transition before, during, and after their research and include technology transition as an integral component of the proposed research activities. To accomplish this, they should identify the maturity level of their proposed solution and the amount of time, effort, and funding needed to complete the solution and transition it into widespread use. Relatively mature technologies may only require funding for a short timeframe to conduct technology demonstration in an operational environment. Prototype technologies, which are less mature, need a longer timeframe with a development phase as well as the demonstration phase. And new technologies, which are even less mature, need an even longer timeframe with applied research, development, and optionally demonstration phases. A structure such as this supports immediate transition wherever possible, and starts to create transition paths for newer, less mature capabilities by having the researcher consider and commit to ultimate transition from the outset of the proposed research.

These levels of maturity are a simplified form of the Technology Readiness Levels (TRLs), initially developed by National Aeronautics and Space Administration (NASA) and widely used by the Department of Defense (DoD). The TRLs are a series of nine increasing levels or measures of maturity of a technology to be incorporated into a system or subsystem [10]. The TRLs provide much greater granularity and are oriented towards traditional systems and software engineering, making them more suitable for large systems integration efforts. We believe the three simple levels are better suited for academics, small startups, etc. who are developing research prototypes and proof-of-concepts.

For all three maturity levels, researchers should be compelled to provide a commercialization plan or other plans for getting the technology into established transition paths, including commercial partnerships or the open source community. The intent is to force the researchers, as part of their technical plan development, to consider the ultimate commercialization of their research results, including considerations such as what is the expected user base, how the technology will be used, and how it will transition in to broad use. Of key importance are the identification of technology transition paths that are appropriate for the type and maturity of the technology involved, and any additional factors that might increase the likelihood of it being commercialized.

R&D EXECUTION ACTIVITIES FACILITATING TECHNOLOGY TRANSITION

The activities of the execution phase of an R&D program are critical to developing technologies that meet important customer needs. The commitment to technology transition that began in the solicitation (pre-R&D) phase is continued in the execution phase. The researchers, as well as project management staff, are reminded of the need to make technology transition a critical part of the research effort. Support and resources are also provided to help increase the chances of transition success.

R&D stakeholders (customers or users who provided the initial prioritized R&D requirements and potential transition partners) are engaged and invited to participate throughout the execution phase. Stakeholder feedback is regularly sought through demonstration of developed prototypes. The important elements of the R&D model and the important role of the stakeholders are regularly emphasized, not only to keep stakeholders engaged, but also to remind the PIs that the customer need (and eventual satisfaction) is what is driving the R&D program, not the innovative technologies themselves.

Bringing many R&D performers together as part of a research project portfolio introduces complexity in managing both the individual projects as well as the portfolio. Providing all the researchers, as well as the program managers (PMs), with innovation training gives them a common framework to discuss and define customer requirements, conduct research, and describe project success is one way to reduce the communication complexity of leading multiple projects towards successful transition. One such framework, the Five Disciplines of Innovation (5DOI) [11], is practiced and advocated by SRI International. Briefly stated, the five disciplines are:

- **Important Customer Needs (I)** – begin with a meaningful problem
- **Value Creation (V)** – have a common language to discuss and create value
- **Innovation Champions (C)** – appoint someone who is passionate about the project and its success
- **Innovation Teams (T)** – ensure collaboration within and across teams
- **Organizational Alignment (A)** – manage to achieve innovation success

As shown in Figure 3, the elements are all needed to achieve market success.

Figure 3 - SRI's 5 Disciplines of Innovation. All must be present for success.

As part of the cybersecurity R&D program at DHS S&T, lead researchers and PMs are given innovation training in which they learn the 5DOI, refine their presentation skills to help focus their value proposition, develop habits of collaboration, and become accustomed to the focus on customer needs and successful transition. Throughout the R&D process, for both individual projects and the project portfolio, technology demonstrations, roadmapping activities, and technology workshops are held to demonstrate continued value and to elicit feedback from customers, users, researchers, and other stakeholders. PI meetings, traditionally a rote exercise of reciting plans and milestones, are used as interactive forums where researchers, managers, and customers can provide valuable feedback to each other and find areas of mutual interest or collaboration (a "watering hole" in the 5DOI lexicon).

It is critical that new R&D technologies undergo test and evaluation (T&E) as an integral part of the research, starting from the beginning and continuing throughout the effort. Making research infrastructure, such as test facilities and realistic datasets directly available to researchers make it easier and more likely that they will test and evaluate their technologies with respect to system performance goals. Performers may use the facilities of the Cyber Defense Technology Experimental Research (DETER) testbed or they may use other facilities as appropriate. The DETER testbed provides the necessary infrastructure – networks, tools, and supporting processes – to foster national-scale experimentation on emerging security research and advanced development technologies. Similarly, performers are free to provide their own datasets, or they can use those available through the Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT). PREDICT was developed in response to the ongoing need for datasets and the problem for the networking and information security research communities. The goal of PREDICT is to create a national R&D resource to bridge the gap between the producers of security-relevant network operations data and technology researchers, developers, and evaluators. Using test facilities such as DETER and realistic test data from sources like PREDICT enables researchers, developers, and evaluators to accelerate the research, design, production, and evaluation of next-generation, cyber security solutions that can lead to commercial products.

POST-R&D ACTIVITIES

Post-R&D activities are for the most part directly focused on transitioning research results to customers and potential users. In this phase, researchers must broaden the scope of their transition activities and expose their technology and tools to a wider audience. Post-R&D transition activities include technology assessments and evaluations, experiments and pilots, and outreach to potential investors and users.

Assessments and evaluations ensure that new cybersecurity technologies are vetted prior to operational deployment within potential user environments. They are conducted through technical assessment, modeling, vulnerability and risk analysis and red team evaluations and operational assessments. Such efforts impact and influence the entire cybersecurity community, both within the Federal government and in the private sector, in identifying and assessing cyber threats and

vulnerabilities and assisting in the acquisition, evaluation and deployment of cybersecurity technologies.

Operational users need experimental deployment opportunities to investigate operational capabilities of the new technologies. Experiments and pilot deployments allow for R&D technologies to be tested and evaluated with real users in real operational environments and provide feedback for researchers and vendors. The feedback also allows operational users to validate and refine their requirements and ultimately make their systems and infrastructure more secure.

As part of their post-R&D activities, researchers must also conduct outreach to increase awareness of emerging commercial technologies and gain insight of cybersecurity needs and requirements of investors, vendors, and users looking to engage these potential new suppliers. Researchers may attract systems integrators or large companies to whom they can sell or license their technologies. Researchers may also attract investors who are willing to provide funding needed to create spin-offs or small business start-ups that can commercialize their technology in hopes of eventually growing into the marketplace or being acquired by a larger company. It is important to identify potential users or marketplaces to help justify investment and creation of commercial products.

There are many ways to reach out to potential investors, vendors, or users. In addition to individual efforts by PIs and government program managers to promote their R&D technologies, they can also participate in collective efforts such as community events and technology showcases. The DHS S&T cybersecurity program has initiated a number of such outreach activities. Three examples include the Infosec Technology Transition Council (ITTC), the Security Innovation Network (SINET), and the System Integrator Forum.

The ITTC is a working forum, created by DHS S&T and SRI International, where experts and leaders from government, private, financial, IT, venture capital, academic, and science sectors come together several times each year in the San Francisco Bay Area to address a variety of problems related to cybersecurity technology. The primary objective of ITTC is to identify proactive IT security solutions and to assist in the acceleration of their development and deployment into the market place. Seasoned professionals in IT security and law enforcement, together with representatives from academia and science, strategically align themselves with subject-matter experts and organizations to pursue this objective. Recent meetings have included talks by current and former government officials, FBI, Secret Service, legal experts, critical infrastructure providers, and members of the research and development communities.

SINET is a non-profit organization, supported in part with DHS S&T funding, that fosters collaboration and provides a number of opportunities to engage the community. SINET brings together members of the Federal Government, IT and security providers, systems integration, venture capital, investment banking, and the academic and science communities. The SINET IT Security Entrepreneurs Forum (ITSEF) and SINET Showcase link technology creators, developers, investors and

users in key technology markets around the country. ITSEF is held at Stanford University in the heart of Silicon Valley. SINET Showcases are held in Washington, DC and other major cities around the country to provide a venue for innovative security companies to present technologies that meet industry and government needs.

The DHS S&T System Integrator Forum is an example of an outreach event, held in 2007 and 2008, which brought together system integrators and government sponsors of information systems projects and showcased several new cyber security solutions funded by DHS S&T. The forum introduced high-quality, top-performing cybersecurity technology development projects funded under DHS BAA or SBIR programs to large integrators of technology who serve the federal government and private industry. Participants were selected for the maturity of their solution, relevance to government needs, the commercial viability of their approach, and their business leadership.

IV. DHS S&T SUCCESSFUL USE OF THE MODEL

Technology transition from research into current, emerging, and future systems is clearly and explicitly stated as an integral part of the DHS S&T cyber security R&D program mission and goals [12][13]. To accomplish this mission and achieve these goals, the program developed and fully employs the R&D Execution Model described above. At the core of the model is the Cyber Security R&D Center (CSRDC), which brings together and facilitates all the elements of the model [14]. The CSRDC plans, coordinates, manages, and conducts activities to secure cyberspace. CSRDC works with research organizations, critical infrastructure operators and developers, and others. Its activities are all focused on successful technology transition and include the development of the cybersecurity research roadmap, research program management, testbeds, experimentation and exercise development, and coordinating various government-industry collaborations.

By applying the R&D Execution Model, in which technology transition is built-in as an integral component of the RDTE&T lifecycle, the DHS S&T cybersecurity R&D program has successfully transitioned technologies from funded projects (including SBIRs) into the commercial market place through spin-offs, acquisitions, and commercial products, including open source software. Table 1 lists several examples of such technology transition successes. These successes serve to show that the R&D Executions Model is not just an abstract model; it's employed by DHS S&T and it works to drive successful cybersecurity technology transitions.

Table 1 – Examples of DHS S&T Cybersecurity R&D Technology Transition Successes

Company – Technology	Transition Success
IronKey – Secure USB Memory Device	Commercial company, founded in 2005. Protects over 3,000 enterprises and 70 financial institutions. Standard issue to S&T employees from S&T CIO. Purchased by Imation in 2011. Renamed to Marble Cloud in 2012.

Coverity – Open Source Hardening (SCAN) Vulnerability scanning service for open source software	Developed by research team from Stanford University. Analyzes 150+ open source software packages daily.
Komoku – Rootkit Detection Technology	Sold to high-security government agencies, including DARPA, the U.S. Navy, and the DOD. Komoku formed as startup in 2004, acquired by Microsoft in 2008.
Secure64 – DNSSEC Automation Secure platform, automated signing DNSSEC server	DNSSEC server products: over 300 systems in 10 countries, on 4 continents, 15 Governmental Agencies in USA
HBGary – Memory and Malware Analysis	Over 100 pilot deployments as part of Cyber Forensics program.
Endeavor Systems – Malware Analysis Tools Botnet detection and mitigation	Piloted at several government agencies, including the FAA. Acquired by McAfee in 2009.
Telcordia – Automated Vulnerability Analysis	In use by DoD, SEC.
George Mason University (GMU) / Proinfo – Network Topology Analysis (Cauldron)	Commercial product sold and supported by startup CyVision at NSA, DHS, FAA and several commercial customers.
Stanford University – Anti-Phishing Technologies	Open source. Most browsers have included Stanford R&D technology.
Secure Decisions – Data Visualization Visual analysis for network flow data	Pilot with DHS/NCSD/US-CERT. Available commercially.
OpenSSL **O**pen source toolkit for SSL and TLS with general purpose crypto library	DHS S&T provided funding and guidance to help secure FIPS 140-2 validation for the most current version of the cryptographic module.
Grammatech – Binary Analysis tools	Available commercially. Used by several Intel agencies.
Open Information Security Foundation (OISF) – Suricata Intrusion Detection (IDS) Project	Open source next generation IDS/IPS development project funded by DHS S&T and private software companies.

IRONKEY SECURE USB MEMORY DEVICE

DHS S&T funded IronKey to develop a secure universal serial bus (USB) device that could provide a more secure environment for data protection. The IronKey USB memory device provides secure Web browsing, cryptographic authentication, end-point security, self-service password recovery, and secure password management. It can withstand both simple and sophisticated attacks protecting critical information for emergency responders. IronKey won the Government Computer News' Best of FOSE Award for FY 2007 and is now available to the public as a more secure alternative than standard USB drives. In addition to DHS S&T funding, IronKey received over $20M of venture funding and has gone from the 2 founders to over 100 employees since 2005. In 2011 storage device manufacturer Imation Corp. acquired IronKey and in 2012 IronKey was renamed to Marble Cloud.

Several of the key elements for transition success were used in IronKey's successful growth from a small start-up into a thriving company. The company's founder and key leaders attended SRI International's innovation training to learn the process and language DHS S&T used for innovation success. IronKey gave presentations on its technology and business plans at numerous outreach events sponsored by DHS S&T, where it received notice, encouragement and feedback to hone their message. DHS S&T supported an independent T&E effort that resulted in improvements to the

technology. DHS S&T also conducted a pilot project within DHS for the IronKey product, where it succeeded in real world usage. Following the successful pilot, the DHS S&T CIO purchased IronKeys as standard issue for S&T employees.

ENDEAVOR SYSTEMS BOTNET SYSTEM

DHS S&T funded development of the Endeavor Systems Inline Botnet Extraction and Response System, a botnet detection and mitigation tool developed under SBIR funding. An extension to their Firstlight product line, Endeavor focused on the development of a malware analysis engine and malware signature distributor. The tool also integrated the inline botnet extraction capability, analysis engine, and the signature distributor. Endeavor's founder and CTO was an enthusiastic graduate of SRI's innovation training, and credited it with helping to sharpen the Firstlight value proposition. Through visibility at S&T sponsored outreach events and early tests by law enforcement agencies, Firstlight's capabilities were promoted and refined. Endeavor Systems was acquired by McAfee in January 2009.

OISF SURICATA IDS/IPS

Suricata is a high performance intrusion detection system (IDS), intrusion prevention system (IPS), and network security monitoring engine developed by the Open Information Security Foundation (OISF). OISF is a non-profit that is funded by DHS S&T and has also attracted private funding. The Suricata engine was first released in 2009 and OISF continues to actively engage cyber security experts and software developers around the world to develop and enhance features of the engine. It incorporates features that go beyond traditional signature based detection and dramatically improve performance. The Suricata engine is available under a GPL v2 license. A number of partners have incorporated Suricata into their products, and a number of third-party tools and signature sets that are available for the well-known SNORT engine are also available for Suricata. Through it's funding of OISF, DHS S&T has brought together a community of network researchers and operators and leading security software developers, and encouraged collaboration and innovation based on the community's needs to produce Suricata and solve security challenges and answer unmet needs in the IDS/IPS marketplace.

V. CONCLUDING REMARKS

Successful transition of cybersecurity technology from research to operational use is absolutely necessary to address the rapidly evolving threats, but it is also a difficult endeavor with many challenges. One of the elements of the CNCI and the *Strategic Plan for the Federal Cybersecurity Research and Development Program* [6] is the Accelerating Transition to Practice (TTP) program. This program recognizes the inherent challenges in technology transition and looks to leverage existing investment in cybersecurity research technologies by further investing in some of the more promising federally-funded technologies in order to facilitate their transition to widespread deployment and use. The goal of this effort is to: (1) identify mature technologies that address an existing or imminent cybersecurity gap in public or private systems that impact national security, (2) identify and fund

necessary incremental improvements, and (3) increase utilization through partnerships, product development efforts and marketing strategies. Efforts are focusing on identified technologies that have a reasonably high probability of near-term successful transition, and which would have notable impact on the cybersecurity of the nation's networks or systems. It is a very ambitious endeavor with enormous potential for positive impact. TTP will provide a connection point for cyber security researchers, the federal government, and the private sector to transition technology from the research to the commercial marketplace and the nation.

We have identified and described key elements that are needed for repeatable, successful technology transition. The R&D execution model is a template for how these key elements can be implemented as an integral part of an R&D program. We showed examples of technologies that have been developed in the DHS S&T program and successfully transitioned.

Ultimately, it is the researchers and inventors who can make technology transition happen, but they need to be given the right support from government funding agencies. A program that not only requires plans and activities in technology transition, but also provides its funded researchers with dedicated funding, training, venues, contacts, and other tools and support for transition has the best chance of success. Improved coordination between agencies and programs could identify common requirements and technologies and could potentially broadly leverage R&D investments across government entities and further improve the rate of successful technology transition.

Researchers DO
Interact with the eventual users of your technology and gain a thorough understanding of their needs and requirements
Learn how to develop a value proposition that articulates your understanding of the need your solution meets, and quantitatively describes the benefits users gain from deploying your solution.
Use the transition support resources available from your institution and your funding agency

Researchers DON'T
Think that your solution will "sell itself". Even the best products need marketing.
Describe your solution only in terms of the technical approach.
Give up. There are many challenges to overcome in technology transition, and it often takes many failed attempts before success is reached.

Program Managers DO
Interact with the eventual users of the technologies to be developed in your program and gain a thorough understanding of their needs and requirements before you solicit research proposals.
Make technology transition a key requirement and evaluation criterion in all aspects of your program.
Guide and support your performers in their technology transition efforts, by providing funding and training, organizing events, providing introductions and connections to potential technology customers, and helping each of your performers identify the best transition path for their organization, technology, and customer.

Program Managers DON'T
Think that technology transition is the responsibility of someone else. You are in a unique position to facilitate and enable successful transition for technologies developed in your program.
Mandate a specific transition path such as open source, which may not be the best alternative for a particular technology or performer.
Wait until the last phases of your program to focus on transition.

ACKNOWLEDGMENTS

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Department of Homeland Security or the U.S. Government. The work by SRI International was funded by the US Department of Homeland Security Science and Technology Directorate (DHS S&T) under contract no. HSHQDC-10-C-00144. The SRI authors thank DHS S&T program managers Greg Wigton and Mike Pozmantier for their support.

REFERENCES

[1] Unlocking Our Future: Toward a New National Science Policy, Committee Print 105–B, Committee on Science, U.S. House of Representatives, One Hundred Fifth Congress, September 1998. (http://www.gpo.gov/fdsys/pkg/GPO-CPRT-105hprt105-b/content-detail.html)

[2] Lewis M. Branscomb and Philip E. Auerswald, Between Invention and Innovation An Analysis of Funding for Early-Stage Technology Development, Prepared for Economic Assessment Office Advanced Technology Program, National Institute of Standards and Technology, NIST GCR 02–841, November 2002. (http://www.atp.nist.gov/eao/gcr02-841/contents.htm)

[3] Accelerating Technology Transition: Bridging the Valley of Death for Materials and Processes in Defense Systems, National Academy of Sciences, 2004. (http://books.nap.edu/catalog.php?record_id=11108)

[4] Department of Defense Report to Congress on Technology Transition, July 2007. (https://acc.dau.mil/CommunityBrowser.aspx?id=173369)

[5] Technology Transfer: Clearer Priorities and Greater Use of Innovative Approaches Could Increase the Effectiveness of Technology Transfer at Department of Energy Laboratories, GAO Report to Congressional Committees, GAO-09-548, June 2009. (http://www.gao.gov/products/GAO-09-548)

[6] Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program, Executive Office of the President, National Science and Technology Council, December 2011. (http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf)

[7] A Roadmap for Cybersecurity Research, Department of Homeland Security, November 2009. (http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf)

[8] Research Agenda for the Banking and Finance Sector, Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, Research and Development Committee, September 2008. (http://www.fsscc.org/fsscc/reports/2008/RD_Agenda-FINAL.pdf)
[9] Roadmap to Achieve Energy Delivery Systems Cybersecurity, Energy Sector Control Systems Working Group, September 2011. (http://energy.gov/oe/downloads/roadmap-achieve-energy-delivery-systems-cybersecurity-2011)
[10] Technology Readiness Level, Wikipedia. (http://en.wikipedia.org/wiki/Technology_readiness_level)
[11] Innovation: The Five Disciplines for Creating What Customers Want, Curtis R. Carlson and William W. Wilmot (2006).
[12] Science and Technology Directorate Cyber Security Division. (https://www.dhs.gov/st-csd)
[13] Cyber Security Research and Development Broad Agency Agreement (BAA) 11-02, Amendment 014, June 30, 2011. (https://www.fbo.gov/utils/view?id=560a331a2f0105f32ca8c1e4f068c5e6)
[14] Cyber Security Research & Development Center (CSRDC), DHS S&T. (http://www.cyber.st.dhs.gov/)
[15] Maughan, W. Douglas, "Crossing the "Valley of Death": Transitioning Research into Commercial Products: A Personal Perspective," 2010 IEEE Symposium on Security and Privacy, vol., no., pp.21-26, 16-19 May 2010. (http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5504786&tag=1)

AUTHOR BIOS

Douglas Maughan is Director of the Cyber Security Division in the U.S. Department of Homeland Security (DHS) Science & Technology Directorate (S&T) Homeland Security Advanced Research Projects Agency (HSARPA) where he oversees Cyber Security R&D activities. Maughan received BS degrees in Computer Science and Applied Statistics from Utah State University, a MS degree in Computer Science from Johns Hopkins University, and a PhD in Computer Science from the University of Maryland, Baltimore County (UMBC). He is a member of IEEE. Contact him at douglas.maughan@dhs.gov.

David Balenson is a Senior Computer Scientist in the Computer Science Laboratory at SRI International. He's interested in technology transition and provides technical support, subject matter expertise, and project management for the U.S. Department of Homeland Security Cyber Security R&D Center (CSRDC). Balenson received BS and MS degrees in Computer Science from the University of Maryland, College Park (UMCP). He is a member of IEEE. Contact him at david.balenson@sri.com.

Ulf Lindqvist is a Program Director in the Computer Science Laboratory at SRI International. He manages research in critical infrastructure security and leads SRI's support for the U.S. Department of Homeland Security Cyber Security R&D Center. He holds a PhD in computer engineering and an MS in computer science and

engineering, both from Chalmers University of Technology in Sweden. He is a member of the IEEE Computer Society. Contact him at ulf.lindqvist@sri.com.

Zachary Tudor is a Program Director in the Computer Science Laboratory at SRI International. He supports operational and R&D projects in critical infrastructure security and provides technical support, subject matter expertise, and project management for the U.S. Department of Homeland Security Cyber Security R&D Center. He holds an M.S. in Information Systems and completed all coursework for a PhD in Information Technology from George Mason University. He is a member of the IEEE Computer Society. Contact him at zachary.tudor@sri.com.