

Testimony of Joseph F. Martin
Director (Acting), First Responders Group, Science and Technology Directorate
U.S. Department of Homeland Security

U.S. House of Representatives, Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

February 12, 2014

Good morning Chairman Ratcliffe, Ranking Member Richmond, and distinguished members of the Subcommittee. Thank you for the opportunity to testify before you today on the role of the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T). S&T's mission is to help strengthen America's security and resiliency by providing assessments, analysis and reports and developing innovative technology solutions for the Homeland Security Enterprise. In this testimony, I will discuss how technology shapes today's threat environment, empowering homeland security operators and first responders with new capabilities but also enabling malevolent actors. To address this, S&T helps operators harness and utilize technology, scientific knowledge, and engineering as a force multiplier and, where possible, to gain leap-ahead capabilities. To illustrate the role of technology and how S&T delivers it to the Homeland Security Enterprise, I will talk about S&T's experience with first responders and how we work with them to overcome gaps and achieve their missions more effectively, efficiently, and safely.

Today, S&T and the Homeland Security Enterprise exist in an environment of rapidly evolving threats and opportunities, and the accelerating pace of risk and technological development loom over every mission in the Department. Threats now range from lone wolf violent extremists to non-state actors with state-like capabilities to rogue states with increasingly sophisticated abilities. In the past, only state actors had the resources and technical capacity necessary to create extreme levels of destruction and disruption. Today, individual actors have access to technology that is sufficient to make explosive devices, develop biological weapons, or execute sophisticated cyberattacks. The wide variation of potential malicious actors—ranging from individuals to terrorist groups to state actors—each have a wide range of capabilities and options to carry out acts that pose immense challenges to homeland security operators. All of this is compounded by the accelerating evolution and revolution of technology. The fields of manufacturing and material sciences, information technology, and biosciences have made revolutionary gains in the last decade. With the commercial sector, particularly small and medium-sized business, driving innovation and with trends like the maker movement proliferating and democratizing technology, new homeland security challenges and opportunities continue to mount.

Reinventing R&D to be more modern and agile

The traditional federal model for research and development (R&D) is based on decades-old assumptions that, in many cases, are ill-suited to today's environment and can stifle innovation in government. Federal funding still drives the majority of basic and applied research, but private sector investment focused on late-stage development surpassed government's total annual R&D investments in the 1980s and has continued this trend. In homeland security, innovation cycles in

areas like advanced analytics, communications, additive manufacturing, and cyber occur so quickly that traditional government vehicles for investment and acquisition struggle to keep up with advances and changes in technology.

Recognizing the growing need for homeland security-tailored technology paired with an evolving innovation ecosystem that includes greater investment by the private sector, S&T is reinventing its approach to R&D to be more agile in helping our partners stay ahead of threat trends. We are becoming more forward leaning, bringing more focus to our portfolio, and engaging more effectively with industry. We are dedicating a portion of our R&D programs to leveraging technical expertise in critical areas that touch on all aspects of operation (e.g., data analytics, network security). We are partnering with emerging innovation leaders in industry and shifting our R&D and testing and evaluation toward DHS Component-based innovation centers focused on bringing new solutions to widespread operational use. Taken together, this will make S&T a more capable R&D agent for homeland security operators and first responders.

S&T's Visionary Goals

As part of being more forward leaning, S&T recently finalized five visionary goals as North Star-like objectives. To arrive at the five goals below, S&T used an inclusive, transparent platform to garner input not only from all of S&T but also from our partners and stakeholders inside and outside of government. The goals are cross-cutting and coalesce S&T around common objectives, align with departmental doctrine and policy, and address strategic challenges and threats identified by the Homeland Security Enterprise. Finally, and perhaps most importantly, the Visionary Goals inspire and excite the science and technology ecosystem around ambitious, innovative solutions.

- *Screening At Speed: Security that Matches the Pace of Life*
Noninvasive screening at speed will provide for comprehensive protection while adapting security to the pace of life rather than life to security. With safeguards to protect privacy, unobtrusive screening of people, baggage, or cargo will enable the seamless detection of threats with minimal impact on the pace of travel and speed of commerce.
- *A Trusted Cyber Future: Protecting Privacy, Commerce, and Community*
In a future of increasing cyber connections, underlying digital infrastructure will be self-detecting, self-protecting, and self-healing. Users will trust that information is protected, illegal use is deterred, and privacy is not compromised. Security will operate seamlessly in the background.
- *Enable the Decision Maker: Actionable Information at the Speed of Thought*
Predictive analytics, risk analysis, and modeling and simulation systems will enable critical and proactive decisions to be made based on the most relevant information, transforming data into actionable information. Even in the face of uncertain environments involving chemical, biological, radiological or nuclear incidents, accurate, credible, and context-based information will empower the decision maker to take instant actions to improve critical outcomes.
- *Responder of the Future: Protected, Connected, and Fully Aware*
The responder of the future is threat-adaptive and cross-functional. Armed with comprehensive physical protection, interoperable tools, and networked threat detection and

mitigation capabilities, responders of the future will be better able to serve their communities.

- *Resilient Communities: Disaster-Resilience for the Future*
Critical Infrastructure of the future will be designed, built, and maintained to be resilient to naturally occurring and man-made disasters. Decision makers will know when a disaster is coming, anticipate the effects, and use already-in-place or rapidly deployed countermeasures to shield communities from negative consequences. Resilient communities struck by disasters will not only bounce back but bounce back quicker.

In establishing S&T's Visionary Goals, we took a major step forward in creating two-way dialogue around our work. This crowdsourcing shaped our final product with additional feedback that we would not necessarily have otherwise been able to tap into. As a natural extension, we created the National Conversation on Homeland Security Technology, which brings together all interested parties (responders, operational users, citizens, academia, and industry to name a few) to play a role in shaping the future of homeland security technology. Through online forums and in-person discussions, we will foster understanding of the homeland security market and build progress toward outcomes that will keep us all safer and minimize disruption to the pace of daily life.

Using science and technology to address first responder operational needs

To look at the role of technology and how S&T delivers new capabilities to the Homeland Security Enterprise, an illustrative example is our work for the responder community. More than 70,000 federal, state, local, tribal, and territorial and entities support public safety and emergency response in every community across the Nation. First responders cross disciplines, including law enforcement, fire services, emergency medical services and emergency management, and serve communities of widely ranging sizes and specific needs against a backdrop of complex operational realities and limitations.

First responders also face a myriad of threats that materialize in various fire, natural disaster, terrorism, and mass casualty emergencies. As a result, responder organizations must plan for wide-ranging response including routine, day-to-day duties as well as rare, catastrophic events. Those organizations also face the challenge of furnishing responders with equipment and training that enable all-hazard response to rare events without interfering with routine duties.

To identify common gaps and address the most pressing responder needs, S&T has an organization within the Directorate—its First Responders Group (FRG)—dedicated to strengthening first responder safety and effectiveness. S&T, through FRG, focuses on evolving, high-impact threats and how to prepare responders without disrupting day-to-day operational duties. Example projects include all-hazard communications and data interoperability, situational awareness, and personal protective equipment as well as more specific work in radiological/nuclear response and recovery. As new threats emerge, S&T works with the first responder community to identify and fill resulting capability gaps guided by several principles for identifying solutions:

- *Operational Needs Drive Projects*: Recognizing that initiatives must be based on user needs and driven from responders in the field
- *Building on Existing Investments*: Encouraging efficiencies by building on existing investments saves money by avoiding unnecessary and duplicative development of new hardware, software, data development, and training
- *Leveraging Existing Solutions*: Conducting technology foraging to help leverage existing interagency and private sector solutions before any investments in new solutions are made
- *Forming Partnerships*: Building partnerships across federal, state, local, tribal, and territorial agencies as well as with international partners to maximize funding and increase adoption
- *Daily Use Solutions*: Seeking technological solutions that improve not only catastrophic response but daily use by first responders
- *Non-Proprietary Solutions*: Ensuring that technologies from different manufacturers can actually interoperate requires the use of open source, non-proprietary solutions and standards-based approaches
- *Affordable and Accessible Solutions*: Recognizing that solutions need to be affordable and commercially available for purchase

As you will see detailed below, S&T tailors its business model to succeed with state, local, tribal, and territorial first responders in addition to DHS operational components including the Domestic Nuclear Detection Office (DNDO), National Protection and Programs Directorate (NPPD), and Secret Service. Industry engagement is fundamental, and our programs are innovative not only in outreach to responder and commercial communities but also in use of funding vehicles. Prize competitions and consolidation and integration of international markets, for example, draw down risk to industry and incentivize product development.

First responder engagement at every stage of development

FRG engages end users at every stage of the technology development process. By engaging end users at the beginning of the technology development cycle for requirements and then continuing throughout the R&D process, FRG fosters user-produced innovation and ensures that the solutions developed have a high probability of being transitioned to the field. Prototypes will then be commercialized, deployed, and adopted as rapidly as possible. For fielded technologies, this enhances widespread adoption of these technologies in the field. This early and frequent engagement also helps FRG to better align current and future investments with responders' highest priority needs.

First responder capability gaps are identified through a series of studies that culminate in a knowledge product known as Project Responder, which describes the highest priority needs for catastrophic incident response. The latest iteration, Project Responder 4, focuses on identifying high priority capability needs, shortfalls, and priorities for catastrophic incident response. It identifies a set of enduring and emerging capability needs, frames them into technology objectives, and assesses the state of science and technology to meet those needs. Findings are based on discussions with federal, state, and local first responders as well as technical subject matter experts. These interactions ensure that potential solutions reflect operational considerations and are based on an actionable and achievable technology path or roadmap. With Project Responder as a foundation, FRG uses its First Responder Resource Group, consisting of

more than 120 first responders and representatives of national first responder associations, to translate broad capability gaps and needs into defined, validated requirements, performance measures, and concepts of operations that can be incorporated into FRG's solicitations for projects. Recent requirements have ranged from location information and proximity to risk for responders to communication in any environmental condition to versatile clothing and equipment that protects against multiple hazards.

After identifying requirements, FRG conducts internal and external technology foraging to determine who else is working in this space and what partial or complete solutions may already exist. Wherever possible, existing investments by federal partners, academia, and the private sector are leveraged. FRG selects projects for funding based on a number of criteria including the practitioner-identified gaps, criticality/operational impact, threat likelihood, applicability, state of the science, cost-benefit analysis, ease of integration, transition likelihood, and time needed to prototype. Responders work with FRG program managers throughout the lifecycle of each project and assist DHS in creating awareness in the field of these newly-developed solutions.

Ultimately, S&T teams with the first responder community and commercial sector to transition technologies, standards, and knowledge products and integrate them into regular use. As solutions develop into mature, commercial products, they ultimately can be purchased by first responder organizations through the Federal Emergency Management Agency's (FEMA) Authorized Equipment List (AEL), which is a list of equipment approved for purchase using FEMA grants. As a service to first responders, FRG also provides objective buying advice for first responders looking at the AEL to help them make informed purchase decisions. The System Assessment and Validation for Emergency Responders (SAVER) program conducts objective assessments and validations of commercial off-the-shelf equipment and publishes explanations for different tools and technologies and their application. After S&T has helped commercialize a product and published it on the AEL, we still work with responders through FirstResponder.gov and other federal R&D agencies such as the National Institute of Justice to promote awareness and enable informed procurement decisions in the first responder community.

Radiological/nuclear response and recovery

One of FRG's highest priority areas is reinforcing response and recovery to a potential radiological or nuclear event. The detonation of a radiological dispersal device or improvised nuclear device (IND) has the potential to cause significant casualties, economic disruption, and critical infrastructure destruction. Responding to and recovering from such an event poses unique challenges to responder organizations. S&T, through its National Urban Security Technology Laboratory (NUSTL), works in conjunction with DNDO on pre-incident operations and with FEMA, the Department of Energy (DOE), and the Environmental Protection Agency (EPA) on response and recovery. A distinguishing aspect of S&T's program is that, recognizing the significant lag between development of new technology and broad deployment with responders, S&T focuses lab and academia experts on the immediate problem of how to prepare and use equipment already in the hands of first responders if a radiological or nuclear event were to occur. S&T's products and science-based guidance (e.g., how to manage complex incident data, methods to mitigate community exposure to radiation hazards) go directly to state and local

responders, increasing their capabilities to respond in the first minutes, hours, and days of a radiological emergency.

The foundation for S&T's work was analysis of significant but broadly dispersed work already completed or underway in the field combined with direct interaction with local agencies to understand their major roadblocks in preparing for radiological response. This was documented and synthesized in the *DHS S&T Radiological/Nuclear Response and Recovery Research and Development Investment Plan*. Based on the plan, the related portfolio now consists of 10 individual activities serving a broad coalition of stakeholders. Examples include the following:

- Compiling guidance and best practices on radiological particle containment, rapid gross-decontamination, and early phase waste management into an electronic application, making it easy for local agency decision-makers and responders in the field to access key information
- Revisiting scientific research and publications related to radiological dispersal device response to make guidance actionable for first responders through tools and preparedness efforts
- Improving radiological data management and modeling technology used by specialized federal agencies and making it more easily available and accessible to state and local agencies to increase operational capability and also increase communication and coordination between levels of government.

Another S&T project of interest is the Radiological Emergency Management System (REMS), which is a network of gamma radiation detectors that provides emergency managers with information on environmental radiation levels to support response and recovery operations in the event of a radiological or nuclear event. REMS was designed at NUSTL in coordination with DNDO and commercialized by a major instrument manufacturer. The New York Police Department, which has a deep relationship with NUSTL, has purchased and deployed dozens of REMS sensors as part of its operational system and stands as a baseline for potential use in other major metropolitan areas.

Though S&T's investment in radiological/nuclear response and recovery is relatively young, the portfolio is making a significant impact by leveraging millions of dollars in previous and ongoing investments by DNDO, FEMA, the Department of Defense, EPA, and DOE and by taking advantage of longstanding relationships with DHS Components like DNDO and FEMA with operational missions in this space.

Next Generation First Responder Apex program

Since S&T's first Apex program began with the Secret Service in 2010, Apex programs have been some of our most successful. With recent expansion of Apexes as a portion of S&T's portfolio, much of the original Apex structure will remain – these will still be cross-cutting, multi-disciplinary efforts intended to solve problems of strategic operational importance – but the projects are being scaled to apply to a wider portion of the portfolio and will operate on longer five-year timelines. The Next Generation First Responder (NGFR) Apex program vision is first responders who are protected, connected, and fully aware and capable of faster, more efficient, and safer response to threats and disasters of all types. NGFR is developing an

integrated and modular ensemble that includes an enhanced duty uniform, personal protective equipment (PPE), wearable computing and sensing technology, and robust communication capability. The modularity and flexibility of NGFR's approach promotes affordability while still supporting diverse environments, including PPE and duty uniforms enhanced for fire resistance, liquid resistance and splash protection, puncture resistance, and improved usability and comfort.

NGFR is harnessing the best existing and emerging technologies and integrating them into a well-defined and standards-based open architecture. A fundamental element of NGFR's strategy to accomplish this will be tapping into the dynamic and growing market for wearable sensors and smart technology. It will use innovative outreach and funding vehicles like prize competitions to bring in innovative corners of the market that have not historically partnered with the Federal Government. NGFR will ultimately be able to provide real-time situation awareness and give previously unattainable recognition and avoidance of hazards before, during, and after incidents.

To support NGFR and many other projects, S&T is also being more innovative in its interface with the international first responder community. First responders around the globe share a common mission to ensure the safety and security of the people they serve. They are often asked to respond to complex incidents like the Deep Water Horizon oil spill and Fukushima Daiichi nuclear disaster. Most countries collaborate at an international level but largely address responder challenges independently and face funding challenges, duplicate effort, and struggle to gain traction in a fragmented global market. To facilitate more robust cooperation and build a larger market for global first responder needs, S&T leads the International Forum to Advance First Responder Technology. The forum is a government-sponsored platform for the following:

- Defining a common set of capability gaps across the globe
- Using assessments of global markets and opportunities to inform prioritization
- Providing a platform for international collaboration on R&D initiatives and solutions
- Engaging industry throughout, to prepare it to make advanced technology available at affordable prices.

The forum initially consists of government representatives from S&T's 13 bilateral partners, Finland, and Japan. It will give responders a global voice and use common problem sets and standards to create or broaden global markets for first responder technology. Ultimately, this lowers risk for industry and incentivizes investment in more robust capabilities and product lines.

Identity, Credential, and Access Management

To protect first responder voice and data communications, assuring secure access to networks and systems is critical. This requires the registration, verification, authentication, and authorization of network users. This technology area is commonly called Identity, Credential, and Access Management (ICAM). FRG, in close partnership with S&T's Cyber Security Division, NPPD's Office of Emergency Communication (OEC), the DHS Office of the Chief Information Officer, the White House's Program Manager for the Information Sharing Environment (PM-ISE), and other partners, is developing ICAM approaches for the Nation's public safety community. While many ICAM solutions do exist today, significant interoperability issues remain for many technical and policy reasons. This leads most public

safety officials to maintain multiple cyber identities to perform their job, which is not only inefficient but also adds security risks.

With more than 60 percent of the public safety community leveraging communication and information sharing capabilities of broadband services, S&T has a responsibility to help secure communications and data across these networks. This is an increasingly complex problem, but we collaborate with our partners to address this by developing and proliferating standards-based approaches that align with federal ICAM guidance. Related to this problem, S&T must assure that ICAM practices of the future (NPSBN) will meet the security needs of the public safety community and be interoperable with the practices of other networks. FirstNet is an independent authority charged with implementing a single wireless broadband data-sharing network, the NPSBN, primarily for public safety personnel. Ultimately, more than five million members of the public safety community may use FirstNet, and S&T, along with other public and private partners will help ensure the security and dependability of communications across the NPSBN for first responders.

In January 2015, with our partners, the PM-ISE, and the International Association of Chiefs of Police, S&T released a report recommending principles and actions for developing an ICAM interoperability strategy that will focus on registering, verifying, and authorizing network users. While this strategy focuses on FirstNet, the principles and actions will be relevant to any initiative that needs to identify and authorize users for access to secure resources. We will continue to work with our partners, in particular PM-ISE and NPPD OEC, to address immediate and longer term needs of first responders on high-priority ICAM issues.

Conclusion

Today, I discussed how technology shapes today's threat environment as a double-edged sword, empowering operators and first responders on one hand but enabling malevolent actors and raising the risk of complex technological disasters on the other. As our work with first responders demonstrates, S&T is helping the Homeland Security Enterprise harness and utilize technology as a force multiplier and to gain leap-ahead capabilities.

Thank you for inviting me to appear before you today. I appreciate the opportunity to testify and would be pleased to answer any questions you may have.