The Heritage Foundation
LEADERSHIP FOR AMERICA

214 Massachusetts Avenue, NE • Washington DC 20002 • (202) 546-4400 • heritage.org

CONGRESSIONAL TESTIMONY

Next Steps for Homeland Security Research

Testimony before
Committee on Science, Space and Technology
United States House of Representatives

March 15, 2011

James Jay Carafano, Ph.D.
Deputy Director, Kathryn and Shelby Cullom Davis Institute for International Studies;
Director of the Douglas and Sarah Allison Center for Foreign Policy Studies
The Heritage Foundation

My name is James Jay Carafano. I am the Deputy Director of the Kathryn and Shelby Cullom Davis Institute for International Studies and the Director of the Douglas and Sarah Allison Center for Foreign Policy Studies at The Heritage Foundation. The views I express in this testimony are my own, and should not be construed as representing any official position of The Heritage Foundation.

Thank you for the opportunity to appear before the committee today and address this vital subject. In my testimony I will address: (1) the progress the Department of Homeland Security (DHS) has made in improving the organization and processes for homeland security research; (2) remaining concerns; (3) vital steps to improving the organization of these activities; and (4) priorities for future research.

My responsibilities at The Heritage Foundation comprise supervising all the foundation's research on public policy concerning foreign policy and national security. Homeland security has been a particular Heritage research priority. The foundation produced the first major assessment of domestic security after 9/11.[1] Over the past nine years we have assembled a robust, talented, and dedicated research team. I have had the honor and privilege of leading this team for many years. Heritage analysts have studied and written authoritatively on virtually every aspect of homeland security and homeland defense. The results of all our research are publicly available on the Heritage Web site at *www.heritage.org*. We collaborate frequently with the homeland security research community, including the Center for Strategic and International Studies (CSIS), the Aspen Institute, the Center for National Policy, the Hudson Institute, the George Washington University Homeland Security Policy Institute, and the Strategic Studies Institute and Center for Strategic Leadership at the Army War College. Heritage analysts also serve on a variety of government advisory efforts, including task forces under the Homeland Security Advisory Council and Advisory Panel on Department of Defense Capabilities for Support of Civil Authorities. I also am a member of the National Academies Board on Army Science and Technology and served on the DHS advisory board for the Quadrennial Homeland Security Review (QHSR).[2] Heritage's research programs are strictly non-partisan, dedicated to developing policy proposals that will keep the nation safe, free, and prosperous.

Call to Action

From the outset our research has focused on ensuring that the organization and activities of the Department of Homeland Security are as efficient and effective as possible. In 2004 David Heyman, who headed the Homeland Security program at CSIS (and who now is Assistant Secretary for Policy at the U.S. Department of Homeland Security), and I led a research project that produced "DHS 2.0: Rethinking the Department of Homeland Security," the first

[1] L. Paul Bremer III and Edwin Meese III, *Defending the American Homeland: A Report of the Heritage Foundation Homeland Security Task Force* (Washington, D.C.: The Heritage Foundation, 2002).
[2] I testified on the results of the QHSR before the House Homeland Security Committee. See James Jay Carafano, "What Comes After Quadrennial Homeland Security Review?" Testimony before the Committee on Homeland Security, Subcommittee on Management, Investigations, and Oversight, United States House of Representatives, April 29, 2010, at http://www.heritage.org/Research/Testimony/What-Comes-After-Quadrennial-Homeland-Security-Review#_ftn2.

comprehensive review of the newly established Department of Homeland Security.[3] When we wrote this initial report, the Science and Technology Directorate (S&T) did not have enough of a "track record" for the task force to make a detailed assessment. In 2007, however, my colleague at the Hudson Institute, Dr. Richard Weitz, and I published "Rethinking Research, Development, and Acquisition for Homeland Security," the results of a follow-on research project that specifically focused on the activities of the S&T directorate.[4] The major concerns we identified were:

- *Lack of response to customer needs.* From the beginning, agencies within the DHS have complained that the directorate's portfolios do not adequately reflect their requirements and are not sufficiently responsive to operational needs.

- *Inability to manage complex programs*. The directorate's most prominent accelerated R&D effort—the attempt to rapidly deploy new technologies to defend against smuggled nuclear and radiological weapons—failed so badly that in April 2005 the Administration established the separate Domestic Nuclear Detection Office (DNDO) to manage these programs.

- *Limited success in partnering with other federal agencies and international partners.* The S&T directorate faced significant challenges in sharing homeland security responsibilities and resources with other federal departments and agencies that are not incorporated within the DHS. These entities retain key roles in researching and developing scientific, engineering, and medical technologies relevant to homeland security.

- *Failure to convert technologies for use by non-federal customers.* Of particular note, the S&T directorate had yet to develop a clear strategy for acquiring and converting technologies for use by the state and local governments and the private sector.

In response to these challenges among our key recommendations were:

- *Putting First Things First.* The directorate needed to tighten its focus on its primary customer base—the agencies within the department. We recommended that DHS should get out of the business of brokering and developing technologies and supporting research for state and local responders and the private sector. Rather, government should limit its support to these other users to setting national standards in coordination with established government agencies such as the National Institute of Standards and Technology and non-governmental organizations such as the American National Standards Institute.

- *Getting a Bigger Bang for the Buck***.** Rather than treating collaborative research with other federal agencies and international partners as an afterthought, we concluded the

[3] James Jay Carafano and David Heyman, "DHS 2.0: Rethinking the Department of Homeland Security," Heritage Foundation *Special Report* No. SR-02, December 13, 2004, at http://www.heritage.org/Research/Reports/2004/12/DHS-20-Rethinking-the-Department-of-Homeland-Security.
[4] James Jay Carafano and Richard Weitz, "Rethinking Research, Development, and Acquisition for Homeland Security," Heritage Foundation *Backgrounder* No. 2000, January 22, 2007, at http://www.policyarchive.org/handle/10207/bitstreams/11911.pdf .

directorate should give first priority to establishing effective partnerships and leveraging the capabilities of these other efforts.

- *Reorganizing and Reprioritizing*. We recommended restructuring R&D programs to best serve the operating agencies within the DHS, and concluded the S&T Directorate should provide the DHS with overall acquisition guidance as well as basic science and technology.

- *Rethinking Acquisition*. In many cases, R&D was not linked to acquisition or there was a failure to recognize that a new technology was not the best answer to the department's needs. Furthermore, the department lacked an integrated program that matches acquisition with training, human capital development, and improving operational practices.

Present Assessment

I would like to credit the current leadership of the DHS and the S&T directorate for making a sincere effort to address these shortfalls. In particular:

- *The current organization of the S&T directorate represents a significant improvement* in aligning research portfolios; establishing effective representation of stakeholder interests; and improving the capacity of S&T to contribute to acquisition and operational analysis. Furthermore, the department has announced plans to expand S&T's role in test and evaluation, as well as involving S&T in "life cycle" assessment of acquisition programs. The role of the director of the office of Acquisition and Operational Analysis should probably be expanded.

- *S&T has made a more concerted effort to leverage the Centers of Excellence and its Federally Funded Research and Development Centers (FFRDC)*. Developing homeland security technologies and expertise requires years of intense effort by an integrated team of scientists, engineers, and managers. Repeated reorganizations only disrupt this challenging effort and should be avoided. Specifically, not curtailing or further limiting the terms of the Centers of Excellence is important. Likewise, the FFRDCs and their expanding capacity to provide operational research, systems engineering, and complex systems analysis have demonstrated real value added. They should be sustained and further exploited.

- *The directorate has also made a sincere and significant effort to establish federal research partnerships* and to improve the oversight process for interagency agreements.[5] Likewise, DNDO was cited by the department's Inspector General in 2007 for improving coordination between federal and state agencies on domestic protocols for detection and response.[6]

[5] See, Office of the Inspector General, "The Science and Technology Directorate's Process for Funding Research and Development Programs, Department of Homeland Security," OIG-09-88, July 2009, pp. 24-25.
[6] Office Inspector General, "DHS' Domestic Nuclear Detection Office Progress in Integrating Detection Capabilities and Response Protocols, OIG-08-19, December 2007, p. 1.

What has been accomplished is noteworthy, especially for a directorate that in 2006 was criticized in Congress for being a "rudderless ship without a clear way to get back on course."[7] In contrast, a 2009 report by the National Academy of Public Administration concluded, "S&T has made strides towards becoming a mature and productive research and development organization, particularly during the last three years." [8]

Yet, despite this leadership team's hard work, significant concerns remain.

- *DHS still lacks an integrated requirements and acquisition process* and a means for integrated development of human capital, operational, training, education, and sustainment programs. DHS needs an integrated end-to-end process. This system needs to be formal and robust and include both a "deliberate" process for developing long-term needs as well as a "crisis-action" process for meeting unanticipated requirements and ensuring rapid acquisition to meet challenges such as those faced during the 2010 Gulf oil spill.

- *The DNDO model remains a concern.* In 2007, we expressed concern about establishing organizational activities that tried to do too much—overseeing everything from concept development to testing and evaluation, acquisition and deployment. We were also concerned that creating a "stovepipe" activity to manage the nuclear detection portfolio, as a separate activity made sense. Those concerns still remain.[9]

- *S&T still lacks a solid track record for transitioning technologies*, particularly for partners outside the department. S&T has improved stakeholder input primarily through its Integrated Product Teams.[10] Particularly noteworthy is the directorate's Community Perceptions of Technology Program managed by the Homeland Security Studies and Analysis Institute, which provides early stakeholder input on the policy implications of fielding new technologies. I have participated in several of the roundtables organized under this program. It is an exceptional initiative, one that should serve as a model for other government R&D efforts. Nevertheless, transitioning technology is still a significant challenge.

- *The department still lacks a truly strategic approach to research and innovation* that would allow appropriately prioritizing and focusing its efforts. HSARPA (the Homeland Security Advanced Research Projects Agency)has been a disappointment.

Moving Forward—The Organization

[7] Senate Report. 109-273, p. 88.
[8] National Academy for Public Administration, "Department of Homeland Security Science and Technology Directorate: Developing Technology to Protect America," June 2009, p. ix.
[9] See, for example, U.S. Government Accountability Office, "Nuclear Detection: Domestic Nuclear Detection Office Should Improve Planning to Better Address Gaps and Vulnerabilities," GAO-09-257, January 2009.
[10] Ibid., pp. 42-53.

Organizational and process restructuring bring costs and as well as benefits. That reality is often forgotten when attention is turned to improving the efficiency and effectiveness of an organization. Opportunity costs matter. This truism is nowhere more important to remember than when considering the DHS and S&T, which have seen a tsunami of reorganization and restructuring over the department's short tenure of existence.

That said, while tinkering ought to be kept to a minimum, there are some critical changes that might to be considered.

- *The time has probably come to give S&T a more defined statutory mission* that clearly outlines its role in acquisition, life-cycle management, and the integration with other enablers for the department, such as training, human capital management, and sustainment. This step should be taken through a reauthorization bill.

- *It might be time to rethink the mission, structure, and purpose of the DNDO* and whether these activities would not be better managed under major department activities rather than as a stand-alone activity.[11] It might make sense, for example, to transfer the office's transformational and applied R&D portfolios to S&T.

- *Congress and the department need to decide—whither the Homeland Security Advanced Research Projects Agency?* The act establishing the DHS created HSARPA. At the time, legislators assumed its mission would parallel the function that DARPA serves for the Department of Defense. That vision has never been fully realized and it is an open question whether a DARPA-like activity is truly essential for DHS or whether DHS would not be better off putting the overwhelming majority of its resources on its present operational needs and leveraging existing organizations, like DARPA, for the rare occasion it needs to look at truly futuristic or "out of the box" solutions.

  Today, HSARPA primarily provides an additional layer of management for a broad portfolio of programs and projects. While it is important to reduce the overwhelming number of direct reports to the undersecretary, it is an open question whether HSARPA best fills this role.[12]

Moving Forward—The Mission

It is time for a serious strategic debate on the direction of the department's homeland security research. We know an awful lot about the competitive environment of ensuring our nation's security. That should reflect in the department and the nation's homeland security research agenda.

[11] For the challenges faced by the DNDO, see, for example, Gene Aloise and Stephen L. Caldwell, "Combating Nuclear Smuggling," U.S. Government Accountability Office, GAO-10-1041T, September 15, 2010.
[12] See, National Academy for Public Administration, "Department of Homeland Security Science and Technology Directorate," pp. 11-13.

Transitioning technology outside the department is extremely difficult. Given that reality and all the serious competing priorities for resources(with a very few "strategic" exceptions) it is time for the department to make the tough call and dramatically scale back its efforts in this area.

S&T should

- Focus laser-like on getting close to its "internal" department customers.

- Limit itself to a coordinating and standards-setting role on technologies for state and local governments, first responders, and the private sector.

- Acknowledge there may be exceptions to the general rule of doing less, particularly in the areas of cybersecurity,[13] exceptionally vital infrastructure (such as the national electrical grid)[14] and technologies that might impact on the resiliency of small and medium business. These areas are the true Achilles' heel of the U.S. economy. Small and medium businesses, for example, make up over half of the American work force. The workers and the companies they serve are the backbone of the U.S. economy. On average, they create about two-thirds of all new jobs each year. Yet, they are most susceptible to interruptions from attacks and disruptions—and there is dearth of research supporting their particular needs.[15]

The department continues to have difficulty putting dollars where they can make a difference. The S&T agenda is still driven too much by stakeholders rather than real strategy. S&T should:

- Dramatically scale back on screening and detection technologies. The needs for these technologies should be driven real assessments of the most efficacious means to achieve risk reduction; the costs and benefits of measures, and limits of current technology rather than legislative fiats of Congress and whims of government officials.

- Step-up cyber-research. Cyber-research must be a high priority for the whole of government and DHS must play an important part. There is no area of homeland security threats, including our knowledge of the dangers of weapons of mass destruction, where government's basic knowledge of the challenge is more deficient. A 2007 Computer Science and Telecommunications Board research report concluded:

---

[13] As a 2007 Computer Science and Telecommunications Board research report concluded, however, the national research and development program is wholly inadequate. Homeland Security is a vital component of this program. See, James Jay Carafano and Eric Sayers, "Building Cyber Security Leadership for the 21st Century," Heritage Foundation *Backgrounder* No. 2281, December 16, 2008, at http://www.carlisle.army.mil/DIME/documents/bg_2218%5B1%5D.pdf,.

[14] The resilience of the U.S.–Canadian electrical grid and telecommunications systems, including developing limited redundancy and identifying means for the timely replacement of essential damaged parts or their rapid substitution is vital to ensure national resiliency in the face of catastrophic disasters. See, James Jay Carafano and Richard Weitz, "EMP Attacks—What the U.S. Must Do Now," Heritage Foundation *Backgrounder* No. 2491, November 17, 2010, at http://www.heritage.org/research/reports/2010/11/emp-attacks-what-the-us-must-do-now.

[15] James Carafano, "Homeland Security's blind spot" *The Examiner*, September 14, 2009, at http://washingtonexaminer.com/op-eds/2009/09/james-carafano-homeland-securitys-blind-spot.

"[B]oth traditional and unorthodox approaches will be necessary. Traditional research is problem-specific, and there are many cybersecurity problems for which good solutions are not known.… Research is and will be needed to address these problems. But problem-by-problem solutions, or even problem-class by problem-class solutions, are highly unlikely to be sufficient to close the gap by themselves. Unorthodox, clean-slate approaches will also be needed to deal with what might be called a structural problem in cybersecurity research now, and these approaches will entail the development of new ideas and new points of view that revisit the basic foundations and implicit assumptions of security research. Addressing both of these reasons for the lack of security in cyberspace is important, but it is the second—closing the knowledge gap—that is the primary goal of cybersecurity research…."[16]

Today, that goal (though admittedly the S&T agenda in this area is much improved) is still not being met.

Finally, while much has been to done to improve "partnerships," these activities must be further stressed as the highest priority. Some specific initiatives that S&T might consider include:

- Become a full partner in the federal nanotechnology effort. DHS, as do many federal agencies, has some nano-related programs, but these disparate research efforts are inadequate for what could be the greatest "game-changing" technology of the next decade. Today, the United States leads the world in nano-science, but that lead is narrowing fast. Our private sector can't plunge much further into nano-industries, given the current economic climate. But that could change rapidly, with a little help from Washington. In high-tech manufacturing, the main cost issue is tech investment—something quite sensitive to tax and regulatory policy. If federal policymakers lowered the cost of capital—by reducing taxes on capital gains and dividends, as well as corporate income taxes—it would stimulate capital investment in a variety of promising technologies. And few, if any, are more promising than nanotechnology. DHS, along with the rest of the government, should rethink its nanotechnology investment strategy. They should pivot right now to help foster the development of nanotechnology manufacturing infrastructure. That way, DHS and other federal agencies can incorporate innovations into its equipment—quickly and cheaply—as soon as the innovations emerge. The Pentagon has done this before. In the 1980s, the Defense Research Projects Agency helped set up Sematech, a consortium of U.S. semiconductor companies called to resolve common manufacturing challenges. DHS and other partner agencies should do the same for nanotechnology manufacturing.[17]

[16] Computer Science and Telecommunications Board, *Toward A Safer and More Secure Cyberspace* (Washington, DC: National Academies Press, 2007), p. 61.
[17] Adapted from James Carafano, "U.S. must gird for war in very small places," *The Examiner*, December 12, 2010, at http://washingtonexaminer.com/opinion/columnists/2010/12/james-jay-carafano-us-must-gird-war-very-small-places#ixzz1GViM4F10.

- Internationalize the SAFETY Act.[18] After 9/11, the U.S. Congress established one potential instrument: The Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act. The SAFETY Act lowered the liability risks of manufacturers that provide products and services used in combating terrorism. The act, passed in 2002, protects the incentive to produce products that the Secretary of Homeland Security designates as "Qualified Anti-Terrorism Technologies." The Department of Homeland Security has made a concerted effort to implement the program, and, as of 2009, about 200 companies have obtained SAFETY Act certification. This program should be used to accelerate the fielding of commercial products and services for cybersecurity.

  If other nations adopted similar liability protection regimes they could form a network to promote innovation. One potential source of outreach might be the Technical Cooperation Program (TTCP), an international organization that collaborates in defense-related scientific and technical information exchange and shared research activities with Australia, Canada, New Zealand, the United Kingdom, and the United States. TTCP is one of the world's largest collaborative science and technology forums. Outreach might focus initially on U.S. partners in Asia including Japan, Australia, New Zealand, Taiwan, South Korea, India, Hong Kong, and Singapore. Singapore is the United States' 15th-largest trading partner and ninth-largest export market. Foreign direct investment in Singapore is concentrated largely in technical service sectors; manufacturing; information; and professional scientific knowledge, skills, and processes.

  As national liability protection proliferates, new opportunities for international cooperation will emerge. Countries that adopt verifiably similar liability protections should extend reciprocal privileges to one another. An expanding global web of liability protection will facilitate the proliferation of homeland security technologies..

Thank you for the opportunity to testify today.

[18] Recommendations are adopted from James Jay Carafano, "Fighting Terrorism, Addressing Liability: A Global Proposal," Heritage Foundation *Backgrounder* No. 2138, May 21, 2008, at http://www.heritage.org/Research/Reports/2008/05/Fighting-Terrorism-Addressing-Liability-A-Global-Proposal.

****

The Heritage Foundation is a public policy, research, and educational organization recognized as exempt under section 501(c)(3) of the Internal Revenue Code. It is privately supported and receives no funds from any government at any level, nor does it perform any government or other contract work.

The Heritage Foundation is the most broadly supported think tank in the United States. During 2010, it had 710,000 individual, foundation, and corporate supporters representing every state in the U.S. Its 2010 income came from the following sources:

Individuals	78%
Foundations	17%
Corporations	5%

The top five corporate givers provided The Heritage Foundation with 2% of its 2010 income. The Heritage Foundation's books are audited annually by the national accounting firm of McGladrey & Pullen. A list of major donors is available from The Heritage Foundation upon request.

Members of The Heritage Foundation staff testify as individuals discussing their own independent research. The views expressed are their own and do not reflect an institutional position for The Heritage Foundation or its board of trustees.