

TEACHING NEW DOGS OLD TRICKS: RESHAPING THE DEPARTMENT OF HOMELAND SECURITY'S TECHNOLOGY DEVELOPMENT INFRASTRUCTURE

Michael Greenberger*

ABSTRACT: This article discusses the Department of Homeland Security's (DHS's) use of technology to help fight the war on terror. First, this article reveals how DHS has made little progress in encouraging the development of important technology, despite receiving ample resources from Congress to do so. Second, this article looks to the Office of War Mobilization's (OWM) work during World War II as a possible template for galvanizing the Nation's technological talent and resources to fight terror. Third, this article suggests a program for refining the OWM template to meet modern day needs. In this regard, DHS is the "new dog," that should be "taught" the "old tricks" that so ably helped this country during World War II.

CITATION: Michael Greenberger, Teaching New Dogs Old Tricks: Reshaping the Department of Homeland Security's Technology Development Infrastructure, 47 Jurimetrics. 281-296.

I. THE PRESENT AND UNNECESSARY HOMELAND SECURITY TECHNOLOGY DEFICIT

At the opening of the 110th Congress, the newly minted Democratic House leadership introduced House Bill I¹, a 273 page bill

* Professor, University of Maryland School of Law and Director, University of Maryland Center for Health and Homeland Security (CHHS). The author wishes to thank Mona Kalash, J.D. candidate, University of Maryland School of Law, CHHS Staff Attorney Erin Hahn, CHHS Law & Policy Analyst Jonathan Minkove, and Research Assistants Anthony Villa and Rafael Maryahin, J.D. candidates, University of Maryland School of Law, for their substantial assistance in preparation for this article.

¹ H.R. 1,110th Cong. (2007).

designed to implement the recommendations of the 9/11 Commission² not yet adopted by Congress more than two years after publication of the Commission's report. A centerpiece of House Bill 1 was the requirement that the Department of Homeland Security (DHS) inspect all passenger aircraft cargo within three years of the legislation's enactment³ and all cargo destined for the United States by sea within five years.⁴ H.R. 1 passed overwhelmingly with strong bipartisan support.⁵

This support was not universal, however. Opponents of House Bill 1, including the Bush Administration and DHS, argued that there was a lack of effective "see through" technology to speed inspection of air and sea cargo and the legislation would cause delays for inspection by "eyes" only, thereby hindering commercial traffic.⁶ The Democratic sponsors of the legislation correctly argued, however, that appropriate "see through" technology does, in fact, exist, and it has been successfully deployed in Hong Kong, the busiest container port in the world.⁷ Three companies manufacture devices that can detect liquid explosives, for example, as well as a device that "can 'see' through glass or plastic bottles and identify any of 2,500 different chemical compounds."⁸

Deploying this "see through" technology would have proven useful in the aftermath of a thwarted terrorist threat on August 10, 2006, to blow up passenger jets using liquid explosives.⁹ Instead, DHS's Transportation

² NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT, (2004), available at <http://www.gpoaccess.gov/911/pdf/fullreport.pdf>.

³ H.R. 1 § 406.

⁴ H.R. 1 § 501.

⁵ 153 CONG. REC. H125,221-22 (daily ed. Jan. 9, 2007).

⁶ 153 CONG. REC. E71, 71-72 (daily ed. Jan. 11, 2007) (statement of Rep. John L. Mica). Spencer S. Hsu, House Passes Bill to Implement More of 9/11 Panel's Suggestions, WASH. POST, Jan. 10, 2007, at A03.

⁷ Press Release, U.S. Rep. Edward J. Markey, House Passes Markey Measures To Screen 100% of Air and Ship Cargo in 9/11 Bill (Jan. 9, 2007), available at <http://markey.house.gov/index.php?option=content&task=view&id=2515&Itemid=125>; see also Stephen E. Flynn, Port Security Is Still a House of Cards, FAR E. ECON. REV., Jan.-Feb. 2006, at 5, 11 (describing the system deployed in Hong Kong for the detection of radioactive material).

⁸ Hiawatha Bray, U.S. Delays Security for Liquid Bombs: Mass. Companies Offer Technologies, but TSA Has Reliability, Practicality Issues, BOSTON GLOBE, Aug. 17, 2006, at D1. It is quite telling that DHS failed to recognize the availability of the technology necessary to implement the widely praised recommendations of the 9/11 Commission. Prospects for Change, News Hour with Jim Lehrer Transcript (July 23, 2004), http://www.pbs.org/newshour/bb/terrorism/july-dec04/commission_7-23.html (last visited July 22, 2007) (quoting former CIA director Robert Gates, "I think that the Commission has rendered a historic service, and I think all of their recommendations merit serious consideration.").

⁹ The government's lack of knowledge about, or reluctance to use, this technology after over ten years of research and billions of dollars was an embarrassment after the August 2006 plot. See Bray, *supra*

Security Administration (TSA) imposed burdensome bans and restrictions on drinks and cosmetics to be carried on board by passengers.¹⁰

In fact, that the U.S. government "ha[d] know[n] for years that liquid explosives posed a threat to airline safety" but "made little progress in deploying technology that could help defend against such attacks ..."¹¹ In the year after the 1995 terror plot to bomb twelve American planes using liquid explosives was discovered in the Philippines, the White House Commission on Aviation Safety developed a package of surveillance projects, including projects to develop bomb detection technologies.¹² In response, Congress increased the Federal Aviation Administration's budget from \$785 million to \$9.1 billion, including money for security improvements and research and development.¹³ By 2003, however, DHS "redirected more than half of the \$110 million it had for research and development. . . delaying research in areas including detecting liquid explosives."¹⁴ On August 11, 2006, a day after the foiled plot, DHS finally decided to initiate a program to obtain detection technology and it planned to test "see through" "devices using 500 milliliter-sized bottles filled with liquid explosives that the government knows terrorists are likely to use."¹⁵

II. THE FAILING DHS TECHNOLOGY STRUCTURE

A. The S&T Directorate and HSARPA.

DHS's tardiness in keeping up with technological advances (much less having a leadership role in this area) is startling given the importance Congress attached to the use of technology in the war on terror. When

note 8. Absent the efforts of British intelligence, the plot would likely have been carried out because the proper technology to detect the explosive materials was still not in place. *Id.*

¹⁰ Trip Advisor, Travel Advisory, Heightened Security Brings New Regulations, [http://www.Tripadvisor.com/TravelAdvisorv-k78-Heightened security brings new regulations.html](http://www.Tripadvisor.com/TravelAdvisorv-k78-Heightened%20security%20brings%20new%20regulations.html) (last visited July 17,2007.)

¹¹ Matthew L. Wald & Eric Lipton, Liquid Threat is Hard to Detect, N.Y. TIMES, Aug. 11, 2006, at A1.

¹² James Ott, Security Rates 'Top Priority,' AVIATION WK. & SPACE TECH., Sept. 16, 1996, at 36.36

¹³ Airports Still Fall Short in Screening for Explosives, Critics Say, DALLAS MORNING NEWS, NOV. 25,1997, at 4a.

¹⁴ Wald & Lipton, supra note 11.

¹⁵ Chris Strohm, DHS Science Chief Calls Liquid Explosives Detection a Priority, GOVERNMENT EXECUTIVE.COM, Sept. 13, 2006, http://www.govexec.com/dailyfed/0906/091306_cdpml.htm.

Congress created DHS through the Homeland Security Act of 2002,¹⁶ Congress created within DHS a Science and Technology Directorate (S&T Directorate).¹⁷ The objective of the Directorate was to ensure that the Nation's technology was being deployed to examine container ship interiors, communicate between different emergency response departments, and to "protect. . . subway and transit passengers" with "synchronized video cameras [and] with . . . chemical and bio-logical sensors."¹⁸

Under the Homeland Security Act, Congress also created the Homeland Security Advanced Research Projects Agency (HSARPA), an agency Congress modeled after the highly successful Defense Advanced Research Projects Agency (DARPA).¹⁹ DARPA has become legendary in implementing defense programs that nurture the development of highly successful techno-logical efforts.²⁰

Since 2003, Congress appropriated \$3.95 billion to advance the S&T Directorate and HSARPA.²¹ By July of 2005, however, the Department had failed miserably in using the ample statutory and financial resources afforded it. The then Secretary of Homeland Security, Michael Chertoff, candidly admitted that "[i]n aviation, our security and our convenience and efficiency can be strengthened by better use of technology, both existing and next generation technology," and that "[t]here is more opportunity, much more opportunity" to use the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act) (discussed in the next subsection) to encourage the private sector to develop technology.²² Criticism of these lagging efforts in

¹⁶ Pub. L. No. 107-296, 116 Stat. 2135 (codified as amended in scattered sections of 6 U.S.C.).

¹⁷ Homeland Security Act, 6 U.S.C. § 181 (Supp. IV 2004).

¹⁸ U.S. Department of Homeland Security: Second Stage Review: Hearing Before the S. Comm. on Homeland Security and Governmental Affairs, 109th Cong. 15, 17, 21, 29 (2005) (testimony of Michael Chertoff, Secretary, U.S. Dept. of Homeland Security).

¹⁹ Homeland Security Act, 6 U.S.C. § 187 (Supp. IV 2004). DARPA exists within the Department of Defense (DOD).

²⁰ See DARPA, BRIDGING THE GAP: POWERED BY IDEAS 1, http://www.darpa.mil/body/pdf/BridgingTheGap_Feb_05.pdf (last visited June 27, 2007).

²¹ This figure includes requested, not actual, funding for 2006 and no amounts for 2007. GENEVIEVE J. KNEZO, CONG. RESEARCH SERV., HOMELAND SECURITY RESEARCH AND DEVELOPMENT FUNDING, ORGANIZATION, AND OVERSIGHT, 4 (2005), available at shelby.senate.gov/legislation/Homeland.pdf.

²² Press Release, Dept. of Homeland Sec, Sec'y Michael Chertoff, U.S. Department of Homeland Security, Second Stage Review Remarks (Jul. 13, 2005), available at http://www.dhs.gov/xnews/speeches/speech_0255.shtm.

technology leadership continues to mount.²³ Indeed, the confusion over the availability of technology to detect liquid explosives described above only serves to corroborate the widespread disappointment on this front.²⁴

B. The SAFETY Act.

DHS's poor administration of the SAFETY Act²⁵ offers a glaring example of DHS's inability to develop anti-terror technology. The SAFETY Act purported to provide "a narrow set of liability protections for manufacturers of... important technologies"²⁶ to encourage "development and deployment of anti-terrorism technologies by providing liability protections for sellers of 'qualified anti-terrorism technologies' and others."²⁷ The SAFETY Act's provisions divide technologies into two classes, each class receiving different benefits.²⁸ A manufacturer may submit a product or service to the DHS Secretary for approval as a qualified antiterrorism technology (QATT).²⁹ Upon such

²³ See U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-05-136, HOMELAND SECURITY: FURTHER ACTION NEEDED TO PROMOTE SUCCESSFUL USE OF SPECIAL DHS ACQUISITION AUTHORITY 28 (2004); U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-04-890, TRANSPORTATION SECURITY R&D: TSA AND DHS ARE RESEARCHING AND DEVELOPING TECHNOLOGIES, BUT NEED TO IMPROVE R&D MANAGEMENT 6 (2004).

²⁴ See supra notes 7-14 and accompanying text.

²⁵ 6 U.S.C. §§ 441-444 (Supp. IV 2004).

²⁶ H.R. REP. NO. 107-609, at 118 (2002).

²⁷ Regulations Implementing the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (The SAFETY Act), 71 Fed. Reg. 73,294 (Dec. 11, 2006) (to be codified at 6 C.F.R. pt. 25)

²⁸ Homeland Security Act, 6 U.S.C. § 441-442 (Supp. IV 2004).

²⁹ The process of "[designation of qualified ant-terrorism technologies]" is delineated in

§ 441(b). This provision states that "The Secretary may designate anti-terrorism technologies that qualify for protection under the system of risk management set forth in this part in accordance with criteria that shall include, but not be limited to, the following:

- (1) Prior United States Government use or demonstrated substantial utility and effectiveness.
- (2) Availability of the technology for immediate deployment in public and private settings.
- (3) Existence of extraordinarily large or extraordinarily unquantifiable potential third party liability risk exposure to the Seller or other provider of such anti-terrorism technology.
- (4) Substantial likelihood that such anti-terrorism technology will not be deployed unless protections under the system of risk management provided under this part are extended.
- (5) Magnitude of risk exposure to the public if such anti-terrorism technology is not deployed.
- (6) Evaluation of all scientific studies that can be feasibly conducted in order to assess the capability of the technology to substantially reduce risks of harm.
- (7) Anti-terrorism technology that would be effective in facilitating the defense against acts of terrorism, including technologies that prevent, defeat or respond to such acts."

Id. QATT is later defined as "any product, equipment, service . . . , device, or technology . . . designed,

designation, if the seller's technology later harms an individual, the seller is immune from punitive damages, joint and several liability, and economic damages.³⁰ Liability is restricted to noneconomic damages in direct proportion to seller's percentage of responsibility.³¹ Plaintiffs may only recover for physical harm, and damages cannot exceed seller's liability insurance coverage offset by the amount of plaintiffs collateral source compensation.³²

Secondly, the SAFETY Act allows DHS to "certify" technologies for QATT designation.³³ After receiving certification, a seller may assert in a law-suit against it the government contractor defense which, if successful, provides a seller immunity from punitive damages and joint-and-severable non-economic damages.³⁴ Certification creates a rebuttable presumption that the government contractor defense applies, which can only be overcome if a plaintiff proves the seller acted "fraudulently" or "with willful misconduct" in applying for SAFETY Act liability protection.³⁵

Finally, the placement of technology on an official DHS "Approved Product List" obviously has benefits that far exceed the immunity granted in terms of marketing to the federal, state, and local governments, as well as the private sector. This kind of listing amounts to a "Good Housekeeping Seal of Approval."

Incredibly, DHS delayed implementing final regulations under the SAFETY Act for four years.³⁶ DHS had been running the program under interim regulations, even though commentators view this process as

developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause, that is designated as such by the Secretary." 6 U.S.C. § 444(1).

³⁰ 6 U.S.C. § 442(b)(2)(A)-(B).

³¹ 6 U.S.C. § 442(b)(2)(A).

³² 6 U.S.C. §§ 442(b)(2)(A)-(B), 442(c), 443(c).

³³ 6 U.S.C. § 442(d)(3).

³⁴ 6 U.S.C. § 442(d)(1)-(3); Regulations Implementing the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act), 68 Fed. Reg. 59,684, 59,691 (Oct. 16, 2003) (to be codified at 6 C.F.R. pt. 25); *Boyle v. United Techs. Corp.*, 487 U.S. 500, 512-13 (1998) (stating original formulation of government contractor defense).

³⁵ 6 U.S.C. § 442(d)(1).

³⁶ Interim regulations were in effect two years after the passage of the SAFETY Act, and final rules took effect on July 10, 2006. See Statement of Jay M. Cohen, Under Sec'y of Sci. & Tech. Directorate, Dep't of Homeland Sec., to the Subcomm. on Mgmt., Integration and Oversight and Subcomm. on Preparedness, Sci. and Tech. of the H. Comm. on Homeland Sec. (Sept. 13, 2006), <https://www.safetyact.gov/DHS/SACTHOME.nsf/IndNews> (follow "Under Secretary's Testimony" hyperlink [hereinafter Cohen statement]; see also Regulations Implementing the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act), 71 Fed. Reg. 33,147 (June 8, 2006) (to be codified at 6 C.F.R. pt. 25).

expensive, cumbersome, and time consuming. One prominent observer explained that this process is "overly burdensome because it requires the submission of a variety of information, some of which is unnecessary, tedious to obtain and not meaningful because the responses would be too speculative."³⁷ The National Defense Industrial Association and the American Bar Association, for example, have complained that the "extensive cost and pricing data discourage[s] many sellers of [the technology] from submitting applications."³⁸

The review process under the initial application procedure is lengthy. Once the applications are submitted, DHS has thirty days to evaluate the package and inform the applicant of missing information.³⁹ Once DHS deems the application complete, S&T has another ninety days, which it can extend without cause or explanation, to recommend to the Under Secretary whether the technology should be designated-certified.⁴⁰ During this time, DHS may require more information from the applicant, ask the applicant further questions about the application, or discuss the application with other government agencies or private entities.⁴¹ After the S&T assistant secretary makes a recommendation, the DHS Under Secretary has another thirty days to notify the applicant of the decision.⁴² The applicant can be approved, denied, or asked to resubmit with more information.⁴³

The application process was so defective that, in August 2006, DHS conceded that "through the practice of issuing numerous 'requests for information,' in some cases the Department might have caused unnecessary delay and imposed undue burdens on applicants."⁴⁴ DHS further "recognized that the initial SAFETY Act Application Kit was overly burdensome and the application process could be streamlined and made less bureaucratic."⁴⁵ DHS stated that it "has refined ... the

³⁷ Jeniffer De Jesus & Bruce Shirk, *Homeland Security Update: The SAFETY Act Interim Regulations*, 18:01 U.S. GOV'T CONT. LITIG. REP. 16, 21 (citing Letter from the Am. Bar Ass'n Section of Pub. Contract Law to the U.S. Dep't of Transp. (Dec. 15, 2003), available at <http://dmses.dot.gov/docimages/p77/261806.pdf> thereafter ABA comment letter]; Letter from the Nat'l Def. Indus. Ass'n, to the Dep't of Transp. (Dec. 15, 2003), available at http://dmses.dot.gov/docimages/pdf88/261840_web.pdf [hereinafter NDIA comment letter]).

³⁸ De Jesus & Shirk, *supra* note 37, at 3. (citing NDIA comment letter, *supra* note 37, at 3; ABA comment letter, *supra* note 37, at 24-25).

³⁹ *Id.* at 18.

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² *Id.*

⁴³ *Id.* at 19.

⁴⁴ Cohen statement, *supra* note 36.

⁴⁵ U.S. DEP'T OF HOMELAND SEC., SAFETY ACT APPLICATION KIT v (2006), <https://www>.

Application Kit... to reduce burdens and to focus more precisely on collecting the information necessary for the review of a particular anti-terrorism technology."⁴⁶

Shortly after the Final SAFETY Act Rules went into effect in July 2006, DHS did, in fact, issue a new Application Kit for the program on August 14, 2006, hoping to encourage more manufacturers to apply to certify or designate their technologies.⁴⁷ However, the Final Rules do not change the inefficient application evaluation timeline outlined above. The DHS Under Secretary of the S&T Directorate still has thirty days to notify an applicant that receipt of the application is complete, ninety days to review the application, and the ability to extend without reason the review period for another forty-five days.⁴⁸ So, while the review process could be complete in 120 days, it could take as long as 165 days if DHS decides to avail itself of the additional review time. There is an expedited review option, but DHS has absolute discretion in determining the timing of the review.⁴⁹

In a misleading statement, the Under Secretary of the S&T Directorate, Jay Cohen, announced in a September 13, 2006 statement that "[p]erhaps the most dramatic change in the Final Rule is the reduction of the evaluation cycle from 150 days to a maximum of 120 days," a cycle that "will be strictly adhered to."⁵⁰ But the Final Rules do not guarantee this 120 day maximum because of the ability of DHS to tack on an additional forty-five days without giving "reason or cause for such [an] extension."⁵¹ Additionally, the new Application Kit, while designed to be "interactive and flexible,"⁵² is still burdensome, and DHS estimates that it will take an average of 120 hours to complete, possibly as many as 180 hours.⁵³ While DHS views the new Application Kit and the Final Rules as refinements providing much-needed clarification to the SAFETY Act application process, these changes do not provide much

safetyact.gov (follow "Application Kit" PDF link under "Printer Friendly Materials") [hereinafter SAFETY ACT APPLICATION KIT]; Cohen statement, supra note 36.

⁴⁶ SAFETY ACT APPLICATION KIT, supra note 45, at v; Cohen statement, supra note 36.

⁴⁷ Cohen statement, supra note 36.

⁴⁸ Regulations Implementing the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act), 71 Fed. Reg. 33,147, 33,163 (June 8, 2006) (to be codified at 6 C.F.R. pt. 25).

⁴⁹ Id. See also Jonathan Marino, DHS to Speed Contractors' Exemptions from Lawsuits, GOVERNMENT EXECUTIVE.COM, Aug. 16, 2006, <http://www.govexec.com/dailyfed/0806/081606jl.htm>.

⁵⁰ Cohen statement, supra note 36.

⁵¹ Regulations Implementing the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act), 71 Fed. Reg. at 33,163.

⁵² SAFETY ACT APPLICATION KIT, supra note 45, at v; Cohen statement, supra note 36.

⁵³ SAFETY ACT APPLICATION KIT, supra note 45, at vii.

evidence of an improved or more streamlined evaluation process. Moreover, the changes do especially little for manufacturers who have an existing application pending and who may want to update the application if they achieve a breakthrough in their technology. As it stands, such an applicant cannot update the existing application, but will likely have to start from scratch.⁵⁴

C. Certifying an Old and Controversial Anthrax Vaccine.

While the pace of certifications has picked up since issuance of the new Application Kit,⁵⁵ the quality of that decision making has been called into question by a troubling and ironic example of a recent designation and certification under the SAFETY Act: the 2006 designation and certification of the BioThrax anthrax vaccine, a technology of Emergent BioSolutions Inc. as a QATT.⁵⁶ This application was granted despite the fact that the plain language and legislative history of the SAFETY Act make it clear that the statute was not to be used for vaccine development.⁵⁷ Beyond that problem of legislative intent is the fact that BioThrax is an older vaccine that has had its share of controversy.⁵⁸

Various public health experts have argued that BioThrax causes serious health problems, particularly among women and people prone to autoimmune diseases.⁵⁹ The potential side effects include Guillain-Barre syndrome (a condition that can kill or paralyze), other neurological disorders, chronic fatigue syndrome, and depression.⁶⁰ The validity of these concerns is highlighted by a 2004 ruling in *Doe v. Rumsfeld*,⁶¹

⁵⁴ Marino, *supra* note 49.

⁵⁵ See Dep't of Homeland Sec., Approved Product List for Homeland Security, <https://www.safetyact.gov> (follow "Approved Product List for Homeland Security" hyperlink under "Designations/Certifications") (last visited June 10, 2007); Dep't of Homeland Sec., Designations for Homeland Security, <https://www.safetyact.gov> (follow "Designations for Homeland Security" hyperlink under "Designations/Certifications") (last visited June 10, 2007).

⁵⁶ *Id.*

⁵⁷ See Michael Greenberger, *The 800 Pound Gorilla Sleeps: The Federal Government's Lackadaisical Liability and Compensation Policies in the Context of Pre-Event Vaccine Immunization Programs*, 8 J. HEALTH CARE L. & POL'Y. 7,22 (2005).

⁵⁸ See *infra* notes 61-71 and accompanying text.

⁵⁹ See Greg Gordon, *Mandatory Anthrax Vaccinations Raise Concerns*, McCLATCHY NEWSPAPERS (Dec. 22, 2006), available at <http://www.veteransforamerica.Org/ArticleID/9140>.

⁶⁰ *Id.*

⁶¹ 341 F. Supp. 2d 1 (D.D.C. 2004), modified by *Doe v. Rumsfeld*, No. Civ.A. 03-707(EGS), 2005 WL 774857 (D.D.C. Feb 06, 2005) (ordering the injunction modified to allow voluntary use of the vaccine "pursuant to the terms of a lawful emergency use authorization ("EUA") pursuant to section 564 of the Federal Food, Drug, and Cosmetic Act"). See also *Doe v. Rumsfeld*, 172 Fed. Appx. 327 (D.C. Cir.

where the district court granted an injunction blocking mandatory BioThrax shots administered to military personnel until the Food and Drug Administration (FDA) reviewed the license of Emergent BioSolutions.⁶² The vaccine has been the subject of much controversy within the military, with high-ranking military officers even refusing to take the vaccine because of a fear of contracting neurological or other physical illnesses.⁶³ The vaccine, which has been around for decades, is administered to military personnel, especially to those in high-risk areas such as the Middle East and Korea, where it is feared the inhaled form of anthrax could be used in a bioterror attack.⁶⁴

In *Doe*, military personnel and Department of Defense civilian contract employees successfully alleged that the FDA's Final Rule and Order authorizing the use of the BioThrax was invalid, because the vaccine was never proven safe and effective against inhalation or "weaponized" anthrax, even though the Final Rule and Order stated it was effective "independent of the route of exposure."⁶⁵

Although the FDA subsequently declared the vaccine safe, health concerns related to the drug remain. A May 2006 Government Accountability Office report states that "data on the prevalence and duration of short-term reactions to the vaccine are limited" and may be more adverse in women.⁶⁶ The report goes on to conclude that "the long term safety of the licensed vaccine has not been studied."⁶⁷ Mark Zaid, an attorney for the plaintiffs in the *Doe* case, continues to claim that BioThrax "is an unnecessary, unproven and potentially unsafe vaccine."⁶⁸ Accordingly, the same group of plaintiffs in *Doe* recently filed another suit in response to the government's decision to reinstate the mandatory

2006) (holding that the action was moot based on the Food and Drug Administration's classification of the vaccine as "safe and effective").

⁶² See also *Doe v. Rumsfeld*, 297 F. Supp. 2d 119,134-35 (D.D.C. 2003) ("Plaintiffs argue that their injuries from non-consensual inoculations would be irreparable. They note that the informed consent documents provided to civilians as a result of the anthrax laden letters in the Fall of 2001 identify side effects such as Guillain-Barre syndrome, multiple sclerosis, angiodema, aseptic meningitis, severe injection site inflammation, diabetes, and systemic lupus erythmatosis.").

⁶³ Andrew Conte, *Vaccine Refusal Draws Crime Charge*, KY. POST, Jan. 15,2000, at 8A.

⁶⁴ Gordon, *supra* note 59.

⁶⁵ 341 F. Supp. 2d at 3.

⁶⁶ U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-06-756, ANTHRAX: FEDERAL AGENCIES HAVE TAKEN SOME STEPS TO VALIDATE SAMPLING METHODS AND TO DEVELOP A NEXT GENERATION ANTHRAX VACCINE 18 (2006), available at <http://www.gao.gov/new.items/d06756t.pdf>.

⁶⁷ *Id.*

⁶⁸ Christopher Lee, *Mandatory Anthrax Shots to Return*, WASH. POST, Oct. 17,2006, at A3.

vaccination program, asserting the FDA's 2005 approval of the vaccine is faulty and that the drug remains unsafe.⁶⁹

Thus, at the very time that DHS was apparently unaware of readily available technologies to detect, for example, liquid explosives, thereby causing continued disruption and delays in air passenger traffic, it made BioThrax, an old and notorious anthrax vaccine still in the midst of litigation about its safety, one of the few technologies to receive certification as a QATT, thereby providing the vaccine's manufacturer with the broad lawsuit immunity protection that QATT status confers.⁷⁰ This is surely a case of effective manufacturer lobbying outweighing the substantive underpinnings of the SAFETY Act.⁷¹

III. AN HISTORICAL MODEL: WORLD WAR II MOBILIZATION BOARDS

It is evident that the DHS technology infrastructure and the SAFETY Act's method of developing and obtaining antiterrorism technologies are not working. DHS must find other methods to encourage and develop technology in an efficient manner. This article recommends that DHS create a highly "interactive and flexible" process by using existing legislative authority and funding to establish a small, but highly skilled, Department of Homeland Security Technology Mobilization Board (DTMB), which would act like the highly praised Office of War Mobilization (OWM) used during World War II. The DTMB would review and search out antiterrorism technology and quickly decide

⁶⁹ Josh White, *Defense Employees Set For Another Suit to Halt Mandatory Anthrax Shots*, WASH. POST, Dec. 13, 2006, at A19.

⁷⁰ The SAFETY Act is not the only legislation that provides such lawsuit immunity. In December of 2005, Congress adopted the same approach of shielding manufacturers from liability used in the SAFETY Act to create the Public Readiness and Emergency Preparedness Act (PREP Act), Pub. L. No. 109-148, C, 119 Stat. 2680, 2818-32 (2005) (to be codified at 42 U.S.C. §§ 247d-6d-6(e)). The Act gives drug companies complete immunity from civil liability for anything related to the development and production of drugs, vaccines or devices. The relevant provision "grant[s] immunity from suit and liability to any covered person for any claims for loss relating to the administration or use of a covered countermeasure." *Id.* Led by Sen. Kennedy, the bill has faced great opposition from the Democrats for its failure to protect the public. Kennedy has proposed a new bill that will address the needs of both the pharmaceutical industry as well as the American Public. See Statement on Pandemic Flu Funding/Liability on DOD Appropriations, Senator Edward M. Kennedy (Dec. 17, 2005), <http://www.americanchronicle.com/articles/viewArticle.asp?articleID=4319>.

⁷¹ BioThrax's manufacturer has had repeated lobbying successes despite controversy surrounding the vaccine, including having five million doses of BioThrax added to the national stockpile, and spending more than \$1 million on aggressive lobbying since 2005 to get health agency officials to agree to an even larger deal. See, e.g., Eric Lipton, *Bid to Stockpile Bioterror Drugs Stymied by Setbacks*, N.Y. TIMES, Sept. 18, 2006, at A1.

whether the new technology should be used and promoted in the homeland security effort. By creating a quick review process, companies, researchers, and inventors will promptly know not only of their product liability status, but whether their technology will be used and recommended by DHS, that is, placed on DHS's "Approved Product List." As shown below, the OWM provides historical precedent for a highly skilled and nimble administrative process for the evaluation of antiterrorism technologies.⁷²

A. The Office of War Mobilization

The OWM was created in 1943 by President Franklin Roosevelt in order to convert a peacetime economy to one focused on supporting the Nation's World War II fighting needs.⁷³ The board was composed of a director and a small staff never exceeding twenty-five people.⁷⁴ In his executive order, President Roosevelt provided that the purpose of the new office was "[t]o unify the activities of the Federal agencies and departments engaged in or concerned with production, procurement, distribution or transportation of military or civilian supplies, materials, and products and to resolve and determine controversies between such agencies or departments."⁷⁵ In serving in this capacity, OWM and its successor agencies had the authority to issue "directives and policies" to carry out its charter.⁷⁶ The creation of this office won widespread approval.⁷⁷

The small OWM staff was comprised of a handful of talented government officials, with recently retired Supreme Court Justice, James Byrnes, serving as the director.⁷⁸ Byrnes had been "a former member of the House of Representatives, the Senate, and the Supreme Court, and

⁷² DHS has also recently mentioned that it has "instituted a program to conduct SAFETY Act reviews in parallel with key anti-terrorism procurement processes. While the Department has institutionalized that process within DHS, we are taking additional steps to appropriately institutionalize SAFETY Act reviews with procurements of anti-terrorism technologies throughout the Federal government." SAFETY ACT APPLICATION KIT, *supra* note 45, at vi.

⁷³ Ernest R. May, *Small Office, Wide Authority*, N. Y. TIMES, Oct. 30, 2001, at A17.

⁷⁴ HAROLD C. RELYEA, CONG. RESEARCH SERV., HOMELAND SECURITY: THE PRESIDENTIAL COORDINATION OFFICE 3 (2004), available at <http://www.fas.org/sgp/crs/RL31148.pdf>.

⁷⁵ Exec. Order No. 9,347, 8 Fed. Reg. 7207 (May 27, 1943).

⁷⁶ *Id.*

⁷⁷ HERMAN MILES SOMERS, PRESIDENTIAL AGENCY: OWMR, THE OFFICE OF WAR MOBILIZATION AND RECONVERSION 52 (1950).

⁷⁸ *Id.* at 52, 54.

former director of the Office of Economic Stabilization."⁷⁹ The small size of the staff was acknowledged as necessary to foster "the relations of the director with agency heads by bringing promptly to the attention of the director questions requiring his consideration, and to serve agency heads by expediting matters requiring action by the director."⁸⁰ In addition, the size of the staff ensured that it would not "en-gag[e] in administrative activities and operations and . . . [not] undertake] or interfere] with the normal functions of other agencies."⁸¹

In 1944, Congress statutorily replaced the OWM, created by executive order, with the Office of War Mobilization and Reconversion (OWMR).⁸² OWMR was an independent agency whose director was chosen by the president and held a two-year term. Although the OWMR staff was larger than that of OWM, it was still small compared to other government agencies.⁸³ Professor James Q. Wilson noted that "OWM was a decision maker. . . . OWM ran no programs, created no czars, and had a minuscule budget [but] [i]t worked."⁸⁴

B. Why It Worked

Prior to the creation of OWM, the Roosevelt administration lacked wartime "synchronization."⁸⁵ There was a widespread concern both in and out of government that converting the peacetime economy to a wartime footing called for a centralization of the mobilization process.⁸⁶ Through OWM, an expedited deliberate process organized the economy in a manner dictated by the dire circumstances the war presented.⁸⁷ Put simply, "[t]he government lacked a place, where, within a reasonable time, a synthesis could emerge from the struggle."⁸⁸ OWM provided that "place."

⁷⁹ RELYEA, *supra* note 74, at 3.

⁸⁰ SOMERS, *supra* note 77, at 55.

⁸¹ *Id.* at 55-56.

⁸² War Mobilization and Reconversion Act of 1944, 58 Stat. 785 (1944).

⁸³ See SOMERS, *supra* note 77, at 81.

⁸⁴ JAMES Q. WILSON, *BUREAUCRACY: WHAT GOVERNMENT AGENCIES DO AND WHY THEY Do IT* 271 (1989).

⁸⁵ ALAN L. GROPMAN, *MOBILIZING U.S. INDUSTRY IN WORLD WAR II* 86 (Inst. For Nat'l Strategic Studies, McNair Paper Series No. 50, 1996), available at <http://www.ndu.edu/inss/McNair/mcnair50/mcnair50.pdf>.

⁸⁶ *Id.* at 83, 89 n.2.

⁸⁷ SOMERS *supra* note 77, at 5.

⁸⁸ *Id.* at 38-40.

The OWM format was widely praised during the war and long after as an excellent framework for providing "a strong staff arm for executive policy and program coordination."⁸⁹ One commentator gave several reasons for its well recognized success,⁹⁰ including—

1. It had direct confidence and backing by the president and was only accountable to him.⁹¹
2. The Board could take quick action directly or through the President. Furthermore, instead of trying to eliminate disputes between agencies, it would "reduce their volume and magnitude through early delineation of general policy and the provision of a locale for final arbitration."⁹²
3. The directors had more than great abilities and broad perspective: they also "possess[ed] independent position and prestige based on wide experience and public respect."⁹³
4. The staff was small and its members were high ranking and of high caliber.⁹⁴

It was also widely recognized that OWM would not have been such an effective synchronizing tool without the initial competent leadership provided by James Byrnes. Byrnes used his "extensive experience, keen intelligence, and high common sense" to use the office as a highly effective decision-making tool.⁹⁵ Historian Alan Milward, explains that the decisions facing Byrnes and OWM were of major significance and could only be resolved successfully by "possessors of great political power."⁹⁶ The persons making those decisions, therefore, were required to have full knowledge of the circumstances leading to the dispute, the control of the administrative machinery to carry out a decision, and the will to make such essential decisions.⁹⁷ Byrnes and his colleagues possessed all of these attributes and were the "supreme umpire[s] over the powerful."⁹⁸

⁸⁹ RELYEA, *supra* note 74, at 4 (quoting SOMERS, *supra* note 77, at 1).

⁹⁰ *Id.* at 4-6.

⁹¹ *Id.* at 4-5.

⁹² *Id.* at 6.

⁹³ *Id.*

⁹⁴ *Id.*

⁹⁵ GROPMAN, *supra* note 85, at 86.

⁹⁶ SOMERS, *supra* note 77, at 65 (quoting ALAN MILWARD, *WAR, ECONOMY AND SOCIETY: 1939-1945* 110-113(1979)).

⁹⁷ *Id.*

⁹⁸ *Id.*

The OWM also leveraged its power by effectively utilizing the staff of various agencies to provide it with relevant information and allowing it to act as a "disinterested decision-maker—judge in effect."⁹⁹

IV. THE PROPOSAL: DHS TECHNOLOGY MOBILIZATION BOARD

OWM can be viewed as an historical blueprint for an efficiently run executive branch institution able to encourage, develop, and promote effective homeland security technology. Ironically, President Bush referenced that blueprint, shortly after 9/11, when he created the Office of Homeland Security (OHS) within the Office of the President.¹⁰⁰ Initially, "OHS was to be located within the White House Office and would be headed by a director who would have Cabinet rank and would report directly to him."¹⁰¹

Similar to the OWM, OHS's "mission ... would be, in the President's words, to 'lead, oversee, and coordinate a comprehensive national strategy to safeguard our country against terrorism and respond to any attacks that may come.'"¹⁰² On the surface this coordination effort "was reminiscent of the efforts of President Franklin D. Roosevelt to create an effective war mobilization and preparedness coordination entity. Success was realized with the Office of War Mobilization."¹⁰³

Unfortunately, it is now well recognized that President Bush did not give OHS the same attention, support, and prestige that President Roosevelt gave to his war mobilization efforts.¹⁰⁴ In turn, that led Congress and then President Bush himself to support the creation of DHS.¹⁰⁵ However, DHS can now itself learn from the blueprint of the OWM to implement an improved technology initiative.

⁹⁹ *Id.*

¹⁰⁰ Address Before a Joint Session of the Congress on the United States Response to the Terrorist Attacks of September 11, 37 WKLY. COMP. PRES. DOC, 1349 (Sept. 24, 2001).

¹⁰¹ RELYEA, *supra* note 74, at 1.

¹⁰² *Id.* (quoting Address Before a Joint Session of the Congress on the United States Response to the Terrorist Attacks of September 11, 37 WEEKLY COMP. PRES. DOC, 1349 (Sept. 24, 2001). "The White House Office was established with E.O. 8248. This order organized the primary units within the Executive Office of the President, which had been created by Reorganization Plan 1 of 1939 (53 Stat. 1423). Other than providing appropriations and a personnel authorization for the White House Office, Congress has not legislatively limited the President's prerogatives regarding its operations." RELYEA, *supra* note 74, at 1 n.2.

¹⁰³ RELYEA, *supra* note 74, at 3.

¹⁰⁴ Susan B. Glasser & Michael Grunwald, Department's Mission Was Undermined from Start, WASH. POST, Dec. 22, 2005, at A1.

¹⁰⁵ See *id.*

First, to be able to make quick decisions like the OWM, a DHS Technology Mobilization Board (DTMB) should be a relatively small institution with the authority to make rapid decisions about which counterterrorism technologies should be promoted within the federal government and to the states and localities.¹⁰⁶ Given the breadth of authority and funding Congress has already provided DHS for technology development, the creation of such a board within DHS should not even require legislation. For example, the board can be created under the legislative authority of, and within, either the S&T Directorate, HSARPA, or as a substitute structure for implementing the SAFETY Act. The creation of such a board would lead to a much more "interactive and flexible"¹⁰⁷ administrative structure than, for example, the present cumbersome and confused SAFETY Act application process, which depends upon "sellers" being willing to commit the time and expense to submit themselves to the present highly burdensome, uncertain, and bureaucratic process.

Second, as was true of the OWM, the DHS Secretary should populate this board with a cross section of skilled, high ranking, and high caliber scientists and researchers led by the kind of skilled supervision that former Congress-man, Senator, and Supreme Court Justice James Byrnes provided the OWM. In the early days following the 9/11 attacks, then Health and Human Services Secretary Thompson showed signs of following this approach when he brought in such world renowned physicians as Donald A. Henderson¹⁰⁸ and Philip K. Russell¹⁰⁹ to assist

¹⁰⁶ In my work as Director of the University of Maryland Center for Health and Homeland Security, I regularly advise state and local homeland security officials on issues pertaining to the use of reliable advanced technology. That work makes it clear to me that neither states nor localities have adequate resources to seek out the wide array of technology that is offered to them by the private sector, much less the universe of technology that may be applicable.

¹⁰⁷ SAFETY ACT APPLICATION KIT, supra note 45, at v; Cohen statement, supra note 36.

¹⁰⁸ On November 1, 2001, Thompson named Donald A. Henderson, M.D., as director of the Office of Public Health Preparedness. Press Release, U.S. Dep't of Health & Human Servs., Sec'y Thompson Names Henderson to Head Office of Pub. Health Preparedness (Nov. 1, 2001), available at <http://www.hhs.gov/news/press/2001pres/20011101a.html>. Dr. Henderson was a professor of epidemiology and international health at Johns Hopkins School of Public Health; he was dean of the school from 1977 through 1990 and founding director of its Center for Civilian Biodefense Studies. Id. He had also held positions with the federal government and the World Health Organization. Id. At the time of the 2001 appointment, Dr. Henderson had received awards from 14 countries and honorary degrees from 13 universities. Id.

¹⁰⁹ On November 1, 2001, Secretary Thompson also appointed Philip Russell, M.D., "as a special advisor on vaccine development and production" to the Office of Public Health Preparedness. Id. Dr. Russell, a virology expert, was a retired U.S. Army major general, founding president of the Albert B. Sabin Vaccine Institute, professor emeritus at Johns Hopkins School of Hygiene and Public Health, a member of the board of directors of the International AIDS Vaccine Initiative, and consultant to the Bill & Melinda Gates Foundation. Press Release, Albert B. Sabin Vaccine Inst., Sabin Vaccine

him in developing medical countermeasures for biological, chemical, and radiological attacks. Unfortunately, Secretary Thompson's efforts faltered as Drs. Henderson and Russell both left HHS by 2004 and scientists of similar prestige and abilities did not replace them.¹¹⁰

Third, the DTMB could make great headway by simply making effective use of "open sources" concerning important technology. As this article demonstrates above,¹¹¹ much of the counterterrorism technology that needs government promotion is already "off the shelf and well publicized in the everyday media."¹¹² Moreover, because these kinds of technology are already in use or readily available for use, the manufacturers are apparently not even seeking the kind of immunity that is proffered by the SAFETY Act. Thus, the present time consuming "certification" process might be completely avoided. Finally, because the approach of the DTMB would be to look outward to find technologies, it would not depend on "sellers" navigating a complicated bureaucracy to gain the government's attention. The DHS "application" process almost certainly limits the scope of what DHS examines. The universe of technology considered would almost certainly be much broader than under a system where DHS looks aggressively for products instead of waiting for manufacturers to approach it.

Fourth, a small and highly expert panel would be capable of identifying in a clear manner technology that is not now available and does in fact need further research and development.¹¹³ It could publicize

Institute's Philip K. Russell Named to New HHS Office of Pub. Health Preparedness (Nov. 28,2001), available at <http://www.sabin.org/files/PDF/russell.pdf>.

¹¹⁰ A notable example of this occurred between 2004 and 2006 when the post was filled by Stewart Simonson, a corporate attorney with little public health experience who had served as legal counsel to Thompson when Thompson was governor of Wisconsin. See Sarah Lueck, Preparing for Emergencies—Health Official Weathers Criticism, Focuses on Public Protection, WALL ST. J., Dec. 12,2005, at A4. Critics viewed his appointment as an example of cronyism and have referred to him as "the Mike Brown of HHS." *Id.* (quoting Jerome Hauer, former director of emergency management in New York). At a "Homeland Security subcommittee hearing on government response to a chemical or biological attack," Simonson admitted, "We're learning as we go." Jeremy Scahill, Germ Boys and Yes Men, THE NATION, NOV. 28,2005, at 24, 24. In response to this admitted incompetence, "[w]hen Col. Lawrence Wilkerson, former chief of staff for Secretary of State Colin Powell,... speculated, 'If something comes along that is truly serious ... like a major pandemic, you are going to see the ineptitude of this government in a way that will take you back to the Declaration of Independence,' many of those professionally concerned with such scenarios couldn't help thinking of Simonson." *Id.* Former Wisconsin deputy attorney general, Ed Garvey, referred to Simonson as "[a] political hack, a sycophant," stating, "People just laughed when he was appointed to Amtrak, but when the word came out that he was in charge of bioterrorism, it turned to alarm. When you realize that people's lives are at stake, it's frightening. It's just one of those moments when you say, Oh, my God." *Id.* at 25.

¹¹¹ See *supra* note 8 and accompanying text.

¹¹² *Id.*

¹¹³ Even where DHS has only had a tangential role in supporting Congressional mandates for

needs of this sort and lead a nationwide discussion of the manner in which industry and inventors can bring products to fruition. In that vein, a further service of such a board could be providing guidance on much needed commercialization to researchers and inventors, many of whom are not now skilled in bringing ideas to practical fruition.

It has been recognized since the 9/11 attacks that the development of counterterrorism technologies is crucial to the United States' ongoing "War on Terror." The present administrative institutions within DHS, including that agency's administration of the SAFETY Act, have proven to be rife with inefficiencies. It is time for the government to try a new solution. By establishing a small, but elite, DTMB, DHS could create a structure for technological innovation that creates positive incentives for corporations, researchers, and inventors to demonstrate qualified antiterrorism technologies to the federal government. Basing the DTMB organization on OWM would ensure a more efficient technology development effort. Given the breadth of the statutory technology mandate already within DHS, no new legislation would likely be needed. Moreover, given the limited bureaucratic footprint of the proposed DTMB, relatively little new funding would be required.

The trick, of course, is properly staffing and organizing the DTMB. Again, a page should be taken out of President Roosevelt's World War II book, when he staffed the OWM with the highest caliber administrators and experts. The Secretary of DHS must do the same to make this proposal work. If he does, the elite and nimble structure of DTMB should ably plug the technology gap the United States now faces in fighting terrorism.

technology development, it has placed a choke hold on the progress of those agencies with the principal statutory mission. See generally Michael Greenberger, *Choking Bioshield: The Department of Homeland Security's Stranglehold on Biodefense Vaccine Development*, 1 *MICROBE* 260 (2006). For example, its dilatory policies have prevented HHS from satisfactorily implementing the Bioshield Act. *Id.* at 260-61. That was one of the major factors that led Congress to pass new BioShield legislation at end of the 109th Congress designed to stimulate research in the development of medical countermeasures to, *inter alia*, WMD attacks. See *Pandemic and All-Hazards Preparedness Act*, Pub. L. No. 109-417, 120 Stat. 852 (2006).