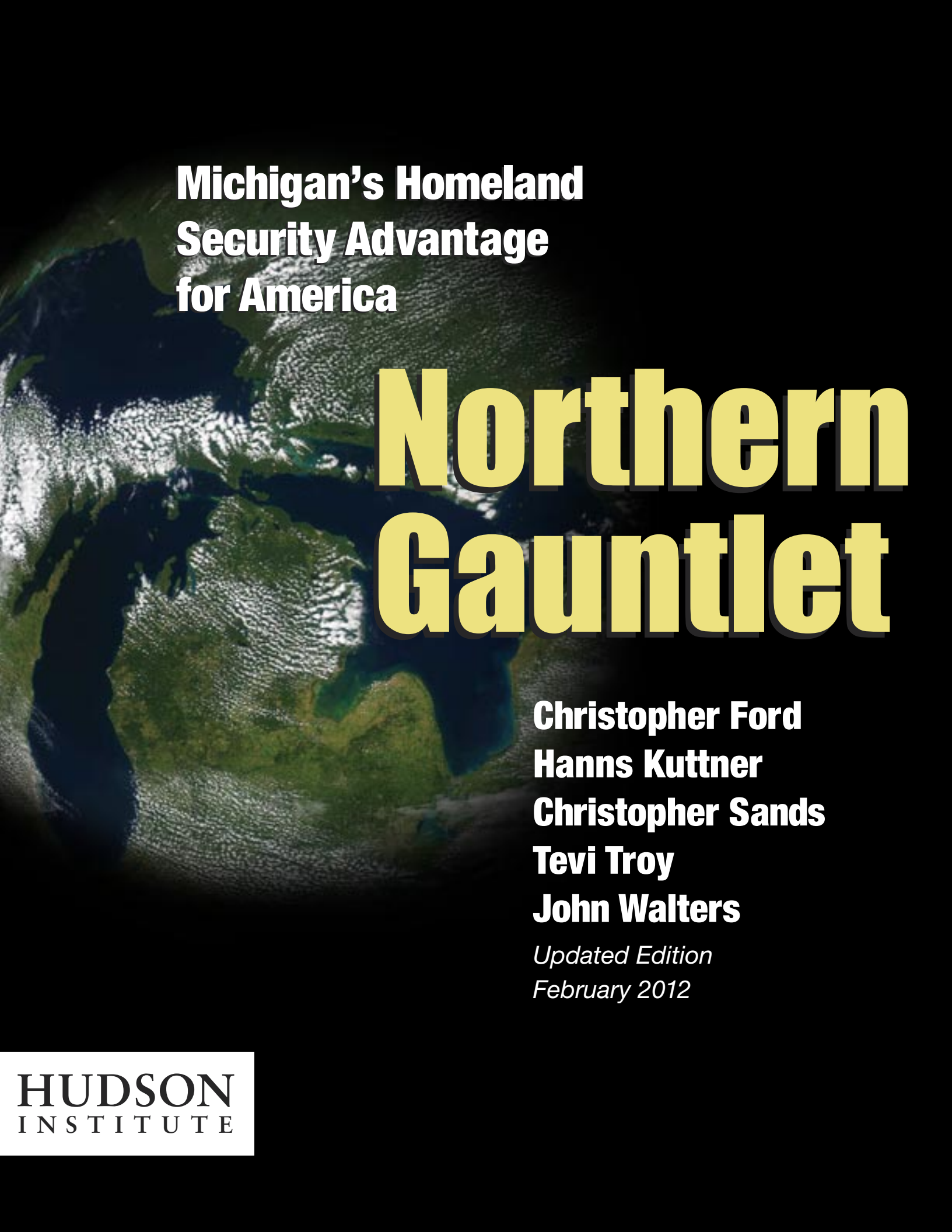


Michigan's Homeland Security Advantage for America

Northern Gauntlet

Christopher Ford
Hanns Kuttner
Christopher Sands
Tevi Troy
John Walters

Updated Edition
February 2012

HUDSON INSTITUTE

Northern Gauntlet

Michigan's Homeland Security Advantage for America

Christopher Ford
Hanns Kuttner
Christopher Sands
Tevi Troy
John Walters

Hudson Institute

Contents

Executive Summary

Napoleon Bonaparte is attributed with the observation that "Geography is destiny" and in Michigan's case, geography has shaped not only the destiny of the people who live there, but also affected the lives of millions of Americans and Canadians whose interests pass through the Great Lakes State. Michigan is at the heart of the Great Lakes which carried countless tons of cargo from Chicago and Duluth through to Cleveland, Buffalo and Toronto and onward to the Atlantic by way of the Erie Canal to New York or the St. Lawrence Seaway through Montreal. Tunnels and bridges as well as ferries link highway and railway networks that connect towns and cities across the United States to Canadian trade. And pipelines and powerlines link Michigan to Canadian energy, making the state a crucial hub for the largest U.S. energy trading relationship.

Michigan's economy has been shaped by its geography, and in particular its role as the gateway for the largest volume of trade in the largest bilateral trading relationship in the world. The fur trade crisscrossed Michigan, with important trade hubs at Detroit and Mackinac. Natural resources and especially lumber harvested in Michigan used the lakes for shipping and access to manufacturing in central Canada and New England. From the very beginning, Michigan-headquartered automotive companies established plants in Ontario in order to export throughout the former British Empire. The energy, skill, and ingenuity of Michiganders contributed to building the strong and prosperous linkages between Canada and the United States.

As trade and traffic grew on the lakes and through the state, the northern border developed into an interface between the law enforcement, customs, and national security systems of two countries that worked closely together as allies and partners.

The terrorist attacks of September 11, 2001 shocked the people of Michigan and the entire world, but the consequences of the attack included a new and more fortified northern border. Michigan found itself on the front lines of the Global War on Terrorism, with the U.S. Federal government, the State of Michigan, Michigan-based companies, Michigan's public and private universities, and numerous Michigan communities investing billions of dollars and person-hours in improving domestic and border security.

A decade later, the world has been transformed by a new awareness of the vulnerability of open societies like that of the United States, as well as of Canada. Threats posed by foreign and "home-grown" terrorists continually shift, requiring an agile and dynamic response from security services. The deep economic integration between Canada and the United States makes close cooperation between law enforcement and military resources of the two countries more critical than ever before. And the governments alone cannot cope with the risk associated with securing our homeland; public-private partnerships are increasingly the key to innovation in the homeland security sector. In fact, the civilian economy is as much a target as government itself.

This report was commissioned by the Michigan Security Network to assess the role that Michigan could play in the growing homeland security sector. It is an analysis of the demand side of the sector—the threats and changing priorities of U.S. (and to some extent Canadian) national security—and also of the potential supply side capabilities Michigan has to meet homeland security requirements in the near-term future.

Hudson has focused on three critical areas of Michigan's strength and U.S. vulnerability: biodefense, cybersecurity, and border-related security. The report identifies a series of concrete areas and actions that could leverage the comparative advantages of Michigan's strategic location, research and production capabilities, existing homeland security facilities and assets, its people and networks to meet threats in these domains.

Michigan remains a natural hub for movement along and across the North American heartland. The development of the homeland security sector in Michigan has yet to reach its full potential. A secure Michigan would help to secure both the United States and Canada—a northern gauntlet, protecting shared prosperity today and for future generations.

Introduction

Hon. John Walters

Michigan boasts the greatest concentration of people and commerce anywhere on the U.S.-Canada border. The state has a 721-mile maritime boundary with Canada formed by Lakes Superior, Huron, St. Clair and Erie and the St. Mary's, St. Clair, and Detroit rivers. Its border terrain includes northern forests and farmable plains. And in the face of today's global threats, Michigan's land, sea, and air routes must be safeguarded each day—in the hot summer and in the icy conditions of a Great Lakes winter—while allowing the massive flow of commerce and people from Canada and around the world. Michigan is part of the front line for securing America and a leader in assembling the knowledge and resources to keep us safe, free, and doing business.

A recent *Washington Post* study[1] noted that:

> Michigan ranks 17th of 50 states in the number of domestically focused counterterrorism and homeland security organizations, and 12th overall in organizations established or newly involved in counterterrorism since 9/11 (tied with Indiana and Virginia). In dollar amount, the state ranked 22nd in fiscal 2009 in federal homeland security spending and 10th in domestic preparedness and antiterrorism programs. Measured per capita, the state ranked 39th in overall federal government expenditures.

The *Post* also reminds us of Michigan's role in meeting the terrorist threat:

> Michigan had 43 terrorism-related convictions from Sept. 11, 2001, through March 2010, according to the Justice Department, ranking second in the nation. Detroit is one of the 64 urban metropolitan areas that have been designated by the federal government as "high-threat, high-density" with regard to acts of terrorism. U.S. intelligence refers to one major alleged terrorist plot related to Michigan having been thwarted since 9/11: the "underwear bomber" plot in 2009 involving indicted Northwest Airlines passenger Umar Farouk Abdulmutallab; the bomber's alleged intent was to blow up the plane en route to Detroit. The intelligence community also ranks Michigan in the top 10 states with the largest Muslim populations, a measure that it applies to potential threats of homegrown terrorist involvement.

Finally, the *Post* noted that Michigan is a major intelligence and operational node in the homeland security network protecting all Americans: ". . . one of 22 states with more than one Joint Terrorism Task Force (JTTF) and one of 16 states with more than one fusion center.

---

[1] *Washington Post* "Top Secret America: Michigan" Available at: http://projects.washingtonpost.com/top-secret-america/states/michigan/

For Michigan and the U.S., protecting the homeland is paramount. Ceaseless vigilance and innovation have enhanced our security and the international tries crucial to economic strength. Canada is America's number one export destination and Michigan is the gateway for more trade with Canada than any other state. Significantly, much of that trade is conducted along sophisticated supply chains using just-in-time logistics to move goods back and forth between suppliers and assemblers in Canada and the United States. Major shippers such as General Motors, Ford, and Chrysler worked with the U.S. Customs Service (now U.S. Customs and Border Protection) to develop the Automated Customs Environment (ACE) and the Customs-Trade Partnership Against Terrorism (C-TPAT).[2] Together with other firms in the automotive industry including Honda, Toyota and hundreds of suppliers, they have made Michigan the access route of choice. More participants in the innovative Free And Secure Trade (FAST) trusted shipper program choose passage through Michigan than any other region of the northern *or* southern border.

Extraordinary achievement is built by talented men and women effectively mobilized. Michigan is home to the largest concentration of engineers outside of California, working in both the private sector and research universities. Private sector R&D spending levels are among the nation's highest. The Michigan University Research Corridor (URC) includes Michigan State University, the University of Michigan, and Wayne State University, which together attract 93 percent of all external academic research, and development dollars that are spent in the state of Michigan. It is one of the top five producers of patents in the United States.[3] Michigan is an education leader in early vocational and mid-career job skills upgrading and retraining thanks to its world-class network of community colleges and private educational institutes.

Michigan's strategic location, technical expertise, existing Federal security presence, strong local law enforcement cooperation, and the sophisticated and engaged private sector, as well as its advanced research and development capacity all position the state for a leading role in the defense of the nation.

Yet there is room for growth: earlier this year, the United States and Canada embarked on a new approach to managing security at their shared border that will generate opportunities for pilot projects, new technology development and introductions, and experiments in operations, cross-border coordination and partnership along the northern border.[4]

Michigan has built the front line, defends that line, and is positioned to make that line even more secure in the years ahead.

---

[2] See *Toward a New Frontier: Improving the U.S.-Canadian Border* by Christopher Sands (Brookings Institution, 2009) Available at: http://www.hudson.org/files/publications/Toward_New_Frontier_Sands.pdf

[3] See *Michigan's University Research Corridor: Empowering Michigan, Annual Report 2010* Available at: http://urcmich.org/commentary/2011annualreport.pdf

[4] See *The Canada Gambit: Will it Save North America?* By Christopher Sands (Hudson Institute, 2011) Available at: http://www.hudson.org/files/publications/Canada%20Gambit%20Web.pdf

Biodefense

Tevi Troy

America remains woefully unprepared for a potential bioterror attack. Despite tremendous strides since 9/11, including spending an estimated $60 billion, the creation of the Office of the Assistant Secretary for Preparedness and Response (APSR), Biomedical Advanced Research and Development Authority (BARDA), and Project Bioshield, significant vulnerabilities still remain. In its most recent report card, the Commission on the prevention of Weapons of Mass Destruction Proliferation and Terrorism, a bipartisan organization chaired by former Senators Bob Graham (D-FL) and Jim Talent (R-MO) gave the federal government a failing "F" grade on bioterrorism preparedness.[5]

Numerous reasons contributed to the federal governments' low grade. First, no umbrella agency exists to oversee the numerous autonomous facilities, such as private and university labs, which can legally handle dangerous pathogens not on the government's list of biowarfare agents.[6] Additionally, in an era of impending budget cuts, homeland security will have to engage in a prioritization process to determine where to put precious and limited biopreparedness resources going forward.

Furthermore, amidst today's calls for significant budget cuts, many states are reluctant to participate in a coordinated biopreparedness program without financial support from the federal government. Because federal budgets are already strapped, the federal government will continue to find it difficult to provide funds for such a program. This lack of cooperation will undoubtedly hurt the country in the instance that it has to respond to a bioterrorism threat. According to the most recent Robert Wood Johnson Foundation report on bioterrorism preparedness, 33 states and the District of Columbia cut funding for public health for the last fiscal year.[7] Since fiscal year 2005, federal funding for public health measures has decreased by 27 percent. The federal government, state governments, and local governments need to streamline their biopreparedness efforts in order to maximize benefits.

---

[5] Joby Warwick and Anne Kornblut, "U.S. is unprepared for major bioterrorism attack, commission finds" *Washington Post*, January 27, 2010 http://www.washingtonpost.com/wp-dyn/content/article/2010/01/26/AR2010012601265.html

[6] Joby Warwick and Anne Kornblut, "U.S. is unprepared for major bioterrorism attack, commission finds" *Washington Post*, January 27, 2010 http://www.washingtonpost.com/wp-dyn/content/article/2010/01/26/AR2010012601265.html

[7] Jeffrey Levi, Serena Vinter, Laura M. Segal, and Rebecca St. Laurent, "Ready or Not? Protecting the Public's Health from Disease, Disasters, and Bioterrorism" *Trust for America's Health* December 2010, http://www.healthyamericans.org/assets/files/TFAH2010ReadyorNot%20FINAL.pdf

The recent film "Contagion" highlighted some additional vulnerabilities in our system, including the serious possibility that we might see suboptimal levels of cooperation from some foreign governments in the case of some kind of bioevent; that there could be higher-than-expected absentee rates by first responders; that even if we have an appropriate countermeasure, that there could distribution and supply troubles with getting it to individuals in need; and that irresponsible talking heads could exacerbate public-health challenges.

Two other significant problems are accurate risk estimation and the difficulty of preparing a comprehensive biopreparedness plan. Because agencies tasked with developing strategies for dealing with bioterrorism vary in their assessment of the risk of bioterror threats, the federal government finds it difficult to put an overarching plan in place. Finally, the process of preparing adequately for a bioterror threat takes considerable time. The federal government cannot simply turn on a light switch in order to force states to comply with its proposals or shore up their defenses.

Given these very real concerns, the United States needs to increase the current state of bioterror readiness at the local, state and federal levels in order to be able to meet a significant bioterror attack.

How Michigan Can Help

With all of these challenges, gaming out all the possibilities on a smaller scale would be advantageous to both federal and to state officials in figuring out how best to cope with the bioterror threat. For a variety of reasons, Michigan is well suited to test biodefense strategies. It is a border state, and can be used to figure out the best modes of cross border cooperation. In 2010, 12,633,157 individuals entered the United States from Canada via Michigan[8], and the United States will need to examine its immigration policies in case of a serious biological threat. It is also a diverse state, both geographically and demographically, with an active labor movement, and is therefore a good testing ground for distribution systems and for measuring out the extent of possible labor challenges from unionized work forces, in both the public and the private sector.

One other key area where Michigan can play a key role in on the technical side. While government has an important role to play in terms of planning and distribution, preparedness is not possible without homeland security solutions from the private sector. Government can figure out strategies and even fund projects, but the products themselves must come from the private sector. Michigan has a strong tradition in this space. Emergent Biosolutions, a $573 million company whose main vaccine facility is in Lansing, is the primary provider of the anthrax vaccine stockpiled by the United States government. It is a private sector company that is well-versed in the need to work with government at the state and national levels. In fact, the company acquired its Lansing facility in 1998 from the Michigan Department of Public health (MDPH).

[8] U.S. Department of Transportation, Research and Innovative Technology Administration, Bureau of Transportation Statistics, Border Crossing/Entry Data; based on data from U.S. Department of Homeland Security, Customs and Border Protection, OMR database.

Michigan should use its existing technical expertise to help nurture the development of other private sector countermeasures that can help protect U.S. and Michigan citizens in case of some type of biological event.

Cybersecurity

Christopher Ford

In a May 2009 speech about how to protect the nation's digital infrastructure, President Obama made a bold and telling statement: "America's economic prosperity in the 21st century will depend on cybersecurity." He went on to declare that "this cyber threat is one of the most serious economic and national security challenges we face as a nation." Michigan Governor Rick Snyder has responded that Michigan has the potential to be a national leader in cybersecurity technology and innovation, given its skilled work force and the presence of major firms and government agencies whose cybersecurity needs will escalate in the next decade.

How can Michigan leverage its present advantages to develop a world class cybersecurity capacity and industry cluster? How can targeted workforce skills training and development attract leaders in this area to locate in Michigan to expand on current capabilities and meet the needs of local firms and agencies?

With new cyberattacks on firms and governments reported in the media daily, what are the challenges on the frontier of current cybersecurity—the unsolved problems, the newest threats, the necessary countermeasures and protections—for which Michigan's research and development capacity and workforce can develop responses?

The emerging field of cybersecurity has the potential to contribute significantly to Michigan's economic resurgence. The Michigan Cybersecurity Initiative will enable existing Michigan businesses and start-up enterprises to meet growing unmet demand in the cybersecurity market, providing business growth, investment, and jobs for Michigan.

This analysis analyzes cybersecurity dynamics and trends, assessing Michigan's strengths and needs, and recommending a comprehensive action plan designed to capitalize upon and enhancing Michigan's leadership in cybersecurity. The following is a summary of the action steps that can help the state remain a cybersecurity leader, secure its own networks, and help growth in the Michigan cybersecurity industry.

Cybersecurity Dynamics and Trends

Traditionally, most approaches to cybersecurity have focused upon the narrowly technical aspects of system vulnerability and specific threat-analysis or attack-defeat technologies. Increasingly, however, it is understood that far more than merely technical competence is needed. Cybersecurity issues must be addressed holistically, and are highly resistant to reductionist efforts to assign remedial responsibility within a single bureaucratic or institutional "stovepipe."

Cybersecurity requires collaborative relationships not only within organizations (*e.g.*, from the security awareness of individual users all the way up to the highest bureaucratic levels of enterprise-wide endeavor) but also *between* them. Ensuring cybersecurity, in other words, is not merely a technical but also a complex managerial and even "political" task that requires the development and maintenance of partnership relations between highly diverse stakeholders in nonhierarchical relationships over time and at multiple levels. There is no "killer ap" for cybersecurity; it is a *whole-system competence*. To be on the cutting edge of preparedness—and thus an attractive partner and locus for industry growth—requires a strong cybersecurity "culture," well-practiced cooperative instincts, managerial savvy, a willingness to explore innovative partnership opportunities, and ongoing political focus and attention.

Michigan's Competitive Strengths

Despite years of funding challenges for such programs, Michigan has been a leader in state government cybersecurity and the encouragement of industry growth. Having several years ago created a centralized "center for excellence" in cybersecurity management under the state Chief Information Security Officer (CISO), Michigan is seen as a leader in this field among U.S. state governments.

Michigan also participates in ongoing efforts to improve inter-state and federal-state coordination in cybersecurity awareness, training and education, threat prevention, response, and recovery operations. Michigan is a longstanding member of the Multi-State Information-Sharing and Analysis Center (MS-ISAC), a focal point for sharing and coordination established in 2003 that since last year also has maintained a 24-hour security operations center for real-time network monitoring. MS-ISCA is a partnership between state governments and federal representatives such as the National Cybersecurity and Communications Integration Center (NCCIC) at the Department of Homeland Security (DHS).

Having already demonstrated a close working relationship with DHS, Michigan was picked to partner with the Department in order to deploy the EINSTEIN 1 intrusion detection system (IDS) system on networks managed by the Michigan Department of Information Technology (MDIT). EINSTEIN 1 was a pilot program designed to provide the U.S. Computer Emergency Response Team (U.S.-CERT) with network flow data that would help it identify suspicious anomalies. The pilot program was a success, and in 2010, Michigan became the first state to implement EINSTEIN 2—a more advanced IDS based not merely upon traffic flow analysis but upon the identification of pre-defined attack "signatures" for malicious network traffic. This program, too, seems to have been quite successful, though DHS has reportedly discontinued it in Michigan.

Presently, Michigan is working to establish a Great Lakes Information Technology Center (GLITC), a centralized network hub to support state and other government entities in the state. (It is reportedly to become operational in 2014.)The center is expected to feature prominently in state business-promotion efforts, with the Michigan Economic Development Corporation (MEDC) hoping that its services as a convenient and secure state-of-the-art locus for "cloud"

computing can be made available (on a temporary basis) to help entice corporate relocation to Michigan.

In short, Michigan's established record of sound cybersecurity practice and IT-savvy economic development puts in among the foremost states in the cyber realm, positioning it well to remain a leader in the field.

Cybersecurity Economic Development Strategy

There are a number of additional steps Michigan can take to ensure that it retains a continued leadership role and becomes an ever more attractive location for cyber-related business development.

Michigan should keep itself at the forefront of public-private cybersecurity partnerships, continuing to build the trust of private sector operators and playing a facilitating and coordinating role in developing and promoting compliance with state-of-the-art "best practices." It is important to keep abreast of the field in cybersecurity technology and ensure a "race to the top" in the use of secure tools—thus helping, for instance, prevent "weak link" problems such as those identified in recent studies with regard to third-party outsourcing of state government IT work or hardware development. It is also critical, however, to ensure state-of-the-art *management* and *coordination*. The private sector is good at keeping up to speed with technology, but the overall cybersecurity *system of systems* still suffers weaknesses in overall information-sharing and coordination among private entities and between the private and public sectors. Michigan can play a role in improving such sharing and coordination, both within its borders and between state entities and the outside environment.

Michigan can also continue to play a leading role—as it has, for instance, with the EINSTEIN programs—in partnering with federal authorities having deep expertise in the field. Key federal agencies have much experience with cybersecurity issues, and in many cases actively seek closer partnership relations with state institutions. Michigan leadership and agility in this realm can keep the state at the forefront of cooperative cybersecurity.

Michigan can also continue to improve the safety and resilience of its own networks, as well as the ability of state systems to continue or restore critical services notwithstanding disruptive attack. This can include not only keeping state networks up to date with "perimeter defense" systems and intrusion detection but also improving data management practices to protect information integrity and implement methods to ensure service survival or reconstitution. By keeping its own networks secure and improving its ability to function as a cyber "first responder" in cooperation with other authorities—much as is currently done with *physical* disasters—Michigan can maximize demonstrate itself to be an attractive location for cyber-related business and a reliable partner in cybersecurity relationships.

Cybersecurity Talent Enhancement

One of the key ingredients necessary to the growth of Michigan's cybersecurity industry is talent. We need to develop, attract, and retain technology professionals with highly-specialized cybersecurity skills in order to support the growth of existing and new cybersecurity companies in Michigan.

Critically, Michigan's human capital development effort for cybersecurity should be a multidisciplinary one—focused not just upon technical knowledge but also upon the development of a "cyber-managerial skillset" of a sort not stereotypically associated with computer expertise. Technical skills are always greatly in demand, but—as noted—cybersecurity also relies increasingly upon inter-institutional partnerships and coordination relationships. This ensures that collaboration, communication, managerial, and even "political" skills are also essential. (As recent studies have emphasized, this is most acutely true at the senior most levels of IT-related personnel, where one needs not only to understand advanced network technologies but also to develop and implement broad solutions within complicated bureaucratic, political, and budgetary environments, and skillfully to "herd cats" in productive public-private partnerships. To a very real extent, however, such "non-technical" skills are also increasingly in demand deeper in to the ranks, for it is at such levels that effective operational interactions need to occur—especially in a crisis.) Responding to this need, Michigan's cybersecurity human capital effort should focus upon both technical *and* managerial skills, aiming to provide a unique talent pool of "full-spectrum" cybersecurity professionals.

Through the Michigan Economic Development Corporation, Michigan has developed several creative talent initiatives to grow this base of expertise locally. Cybersecurity will serve as a key aspect of the following Talent Enhancement programs:

- Shifting Gears, a career-transition program for seasoned corporate professionals who want to pursue Michigan job opportunities in business growth sectors where they can leverage their business knowledge and experience in new ways

- MichAGAIN, a campaign with the message, "Now is the perfect time to come back home." MichAGAIN helps talented individuals and growing businesses connect—and reconnect—with Michigan, sponsoring events in Boston, Chicago, Washington, DC, Cincinnati, and San Francisco, with more to follow.

- Global Michigan, working to find new ways to encourage immigrants with advanced degrees to come to Michigan to work and live.

- LiveWorkDetroit, an MEDC program that connects Michigan's college graduates to new opportunities in Detroit and promotes the city as a post-graduation talent destination.
- Additional talent programs are under development by the Talent Enhancement team, including "boot camp" programs to retrain IT professionals in emerging specialty areas like mobile applications and cybersecurity. Improved coordination with Michigan's

Economic Development Job Training (EDJT) effort and with the Michigan Technical Education Centers (M-TECs) may also be needed to improve their ability to provide relevant technical *and* "full-spectrum" multidisciplinary training.

Entrepreneurial Support

Through the MEDC, Michigan has significantly increased support for our domestic entrepreneurial ecosystem, making Michigan a hot spot for innovation and entrepreneurial activities. Key programs that will benefit cybersecurity start-up ventures include:

- The Michigan Mentor Network, a program designed to match entrepreneurs with experienced mentors in the private and academic sectors.

- The Michigan Small Business and Technology Development Center (MiSBTDC) offers Michigan's most comprehensive entrepreneur and small business development program. Jointly funded by the MEDC and the U.S. Department of Commerce, MiSBTDC provides counseling, training, research and advocacy for new ventures, existing small businesses, and innovative technology companies. Services include technology counselors to provide more in-depth support and a roadmapping tool that helps clients evaluate the direction of their technology, to departmentalize concepts, and to chart strategic direction.

- A network of Smartzones and Business Incubators, including several with specific focus on high-tech growth industries.

Access to Capital

Michigan offers a wide range of programs to enable business to gain access to the capital they need to grow through the various stages of their development. These programs will be critical to the growth of both start-ups and existing cybersecurity companies. Programs include the Michigan Capital Access Program, Collateral Support Program, and Loan Participation Program, as well as a variety of equity-based financing programs.

Michigan Defense Center

As home to key defense and military procurement facilities, Michigan companies are perfectly and uniquely positioned to interact with the US Armed Forces in cybersecurity. The Michigan Defense Center's team of seasoned professionals, with their combined military backgrounds and government contracting experience, stand ready to help Michigan companies tap into the in-state market for military cybersecurity and other advanced technologies. This team works closely with a network of Michigan Procurement Technical Assistance Centers (PTACs) to prepare Michigan businesses to compete for government contracts and by educating them regarding the opportunities, requirements and processes involved with becoming successful government contractors.

Product Beta Test Program

Small start-up cybersecurity companies start with a great idea that they prove in a lab/development environment, but often lack the resources required for real-world testing prior to commercial launch. Michigan will fill this gap by piloting a "Beta Test" program for cybersecurity products. The State will work with start-up company staffs to deploy the pre-release products in segments of the State's IT infrastructure, providing critical quality, suitability, and effectiveness data that will accelerate the product release cycle.

State-Federal Partnership

Building on its leadership role in partnering with DHS on the EINSTEIN 1 and 2 programs, Michigan is well positioned to do more in collaborating with federal authorities to provide state-of-the-art cybersecurity in its own networks and for businesses in the state.

DHS continues to seek state partners for advanced cybersecurity cooperation, and may be amenable to doing more with savvy partners such as Michigan. DHS's Homeland Security Grant Program (HSGP) also provides a mechanism for states to apply for federal funding for cyber-related activities under various component programs, and DHS is reportedly working to increase the cyber-security role of the various data fusion centers it has helped establish for information-sharing and analysis between different levels of government. DHS is planning to undertake assessments of state cybersecurity in the autumn of 2011, which will presumably play a role in allowing the Department to evaluate state strengths and needs. Michigan should work to ensure that it continues to be perceived as an enthusiastic and valuable partner in state-federal relationships.

DHS, for instance, is presently beginning to deploy EINSTEIN 3 in selected federal networks. This system encompasses not merely traffic flow analysis and "signature" detection but now also some capability automatically to "disrupt" inbound attacks. DHS apparently does not plan to deploy this particular system nationally, but is working with the MS-ISAC (in New York) to develop and deploy a new system for such purposes, known as ALBERT. Based upon its prior successes with DHS, Michigan may be well positioned as a pilot state for this effort.

Since February 2010, moreover, DHS has been implementing a pilot program for information-sharing with Chief Information Officers (CIOs) and Chief Security Officers (CSOs) in the corporate world, as well as with state and local government officials—all of whom participate in quarterly secure teleconferences and get DHS threat and security briefings. Some provision is also reportedly made to give these participants access to classified DHS networks in the event of a cybersecurity incident. Michigan should work to ensure that it remains at the forefront of state-level participation in such processes, both in order to keep its own networks secure and to help reassure actual or potential state businesses that Michigan "gets it" as enthusiastic and supportive cybersecurity partner.

In June 2011, the U.S. Defense Department (DOD) also began an innovative "Defense Industrial Base Cyber Pilot" program (DIBCP) for information sharing and coordination between defense contractors, DHS, and the National Security Agency (NSA). In an effort to get around longstanding concerns about NSA involvement in non-federal networks, DIBCP involves only voluntary information-sharing, in which participants and their Internet Service Providers (ISPs) are given some NSA data on sophisticated threat "signatures" so that ISPs to block attack that are still "inbound"—*i.e.*, before they actually reach the defensive "perimeter" of corporate IT systems.

At present, DIBCP is limited to a small number of participants, involving only 25 or fewer defense contractors and their ISPs. (The service providers AT&T, Verizon, and Century Link are reportedly participants, as well as defense giants such as Lockheed, CSC, SAIC, and Northrop Grumman.) According to DOD sources, however, the Cyber Pilot is proving very successful, and Pentagon officials are considering extending it to the entire U.S. defense industrial base.

Perhaps because some classified information is involved—and because NSA involvement entails political sensitivities—there has as yet been little talk of extending DIBCP beyond defense contractors (*e.g.*, to involve other private entities or state and local governments). DOD, however, does desire improved partnership relations in civilian-sector critical infrastructure protection, not only with DHS but also with state and private entities. Michigan could play a leadership role in helping build such relationships. (Precedents exist for handling classified information in counter-terrorist information sharing, and to the extent that private actors harbor continuing misgivings about cooperation with NSA, the role of state-level officials as participants and partners in such arrangements could even provide a kind of reassuring "third-party accountability" or privacy-protection "quality control" in such a process. A logical point to begin might be with General Dynamics Land Systems, a major defense contractor already located in Michigan.

Cyber-Resiliency

Michigan should also strive to ensure that state networks—and any private corporate systems that piggyback upon them (as for instance, in the GLITC) or coordinate with them—are as prepared as possible not simply to defeat cyber attack but to *survive* it and *reconstitute* services.

"Red teaming" and penetration exercises are a common tool of cybersecurity, which have been used (as in Colorado) to identify system vulnerabilities or (as in Texas) to evaluate software and hardware provided by state vendors by testing it against realistic attack scenarios. Even some municipalities have gotten into the game, with one city in Virginia, establishing a laboratory dedicated to simulating cyber attacks upon municipal systems. Michigan was one of 11 states (and 60 private companies) to participate in "Cyber Storm III," an exercise organized by federal authorities in September 2010 to simulate a massive attack upon U.S. networks with an eye to preparing participants for more effective responses in the event of a real one. This has provided valuable experience.

Such drills and training opportunities are critical not just for defense but for resilience. But they are valuable not simply for any familiarity they may bring with advanced technologies, but also, and perhaps more importantly, for the experience they provide in inter-institutional coordination and collaboration. Michigan could help improve its own cybersecurity and that of state businesses—thus making the state both a more attractive location for cyber entrepreneurship and a more reliable partner for established entities—by sponsoring exercises at the *state* and *local* level. This would help give participants experience in inter-personal and inter-institutional cooperation in the face of cyber-threats, providing them with reservoirs of contacts, understandings of comparative competences, and patterns of agile and adaptive behavior that are highly resistant to "book learning" but yet difficult and costly to acquire "on the job" in the event of a real attack. Such simulations help build the collaborative skills that will, in a crisis, be essential bridges across federal, state, local, and private-sector boundaries.

Finally, Michigan could preserve its leadership role by doing more—and in a very public way—to emphasize cybersecurity as a realm of emergency management equivalent to more established and traditional forms of disaster preparedness, consequence management, and recovery. It is a common finding of recent studies of cybersecurity management that state information security organs suffer from resource constraints and find themselves in a relatively worse position, enterprise-wide, than private-sector corporate counterparts. State organs also find themselves trailing the private sector in bringing systems within a consistent framework of network security standards. To the extent that it is within Michigan's means and legislative authority to upgrade the organizational posture of its cybersecurity organs, this would be both substantive useful and send an important signal that a "culture" of effective cybersecurity has taken root in the state.

Cybersecurity is a demanding business, a problem that demands an unprecedented degree of inter-institutional competence and coordination. Building a successful approach to cybersecurity—and making oneself a valuable partner in *and location for* relevant business development—lies not merely in technology but in managerial and collaborative competences: the coordination of adaptive responses across diverse institutional boundaries and the development of partnerships across multiple levels of government and the breadth of the private sector. With proven successes not only in internal cybersecurity management but in innovative public-private partnerships, Michigan is well-positioned for continued leadership. It can seize this opportunity through forward-leaning human capital development, the integration of an emerging cybersecurity culture with broader high-technology growth promotion, and continued openness to federal-state partnerships on the cutting edge of the field.

Border Security

Christopher Sands

The busiest section of the U.S.-Canadian border is the Great Lakes gateway encompassing the major crossings of Detroit and Port Huron in Michigan and the Buffalo and Niagara Peninsula crossings in New York, all connecting the U.S. industrial and agricultural heartland with Ontario, Canada's economic heart and home to 40 percent of the Canadian population and nearly half of Canadian GDP. At the eastern edge of the Great Lakes gateway, the crossing at Champlain, New York is the main connection between Montreal and New York City and the entire U.S. Atlantic seaboard. Unlike other sections of the border, geography limits the number of possible crossing points: the Great Lakes and rivers connecting them comprise most of the border in this region. As a result, traffic must cross over bridges and through tunnels, and is relatively concentrated. Of the major crossings in this gateway, only Champlain is a land crossing with room to expand inspection plaza areas to accommodate growth in traffic at a low relative cost. In all, 10 bridges and the Detroit-Windsor Tunnel carry motor vehicle traffic from Michigan and New York to Canada.

The majority of U.S.-Canadian trade passes through the Great Lakes gateway, based on value. This is mainly due to the automotive industry. Detroit's automotive pioneers established partnerships and subsidiaries in Canada by 1910. The U.S. government signed trade agreements beginning in 1965 to remove barriers and allow the automakers to integrate car production across the continent. Today, Canada is responsible for nearly 20 percent of all North American vehicle production, and Canadian suppliers are closely linked to U.S. automotive supply chains. In recent decades, motor vehicles and parts have been the largest single component of bilateral trade, in what is famously the largest bilateral trade relationship in world history: generating more than $1.5 billion in cross border flows every day.

When the U.S.-Canada border was closed briefly on September 11, 2001, auto plants across the Midwest and as far south as Missouri were forced to shut down for lack of component parts. This is a consequence of just-in-time, or JIT, inventory management, a practice that coordinates the delivery of parts within hours or even minutes of when they will be needed so that companies do not need to maintain warehouses full of parts waiting for orders. In order to coordinate the logistics among suppliers and assemblers, manufacturers organize "supply chains" linking factories in a synchronized production process that is more efficient and therefore more competitive. JIT logistics are a major contributor to the growth in productivity in the auto industry and in other areas of the economy, from food processing to consumer electronics. A study by the Conference Board of Canada in 2007 identified the seven sectors most vulnerable to border disruptions of supply chains: (1) motor vehicle manufacturing; (2) basic chemical manufacturing; (3) computer and peripheral equipment manufacturing; (4) resin, synthetic rubber, and artificial and synthetic fiber manufacturing; (5) rubber product manufacturing; (6) seafood product preparation and packaging; and (7) electrical equipment and component

manufacturing.[9] Each of these is a sector that ships products via the Great Lakes gateway and Michigan's border with Canada.

Delays at the U.S.-Canadian border undermine the efficiency of JIT logistics, particularly unpredictable delays. Instead of sitting in warehouses, necessary components sit in trucks that are waiting to clear customs. Unexpected delays force assembly lines to slow down and in some cases stop when the parts they need have not arrived. Since such delays create a disincentive to purchase critical parts from suppliers on the other side of the border, the failure to address border delays can encourage companies to seek more expensive supplies in their own market. This in turn raises the cost of the product for the consumer, which can translate into lost sales and ultimately, lost jobs. As a result, the Blue Water Bridge and the Ambassador Bridge have among the highest rates of commercial traffic entered into the Free And Secure Trade (FAST) trusted traveler program at some 44 percent of all trucks crossing the border at these locations.[10]

In their analysis of U.S.-Canada trade data since September 11, 2001, Globerman and Storer found that in the Great Lakes Gateway, there is some evidence of negative effects on exports to Canada in 2001 and 2002 (and to some extent 2003) but the effects are more pronounced for exports by truck than for total exports. For imports from Canada, Globerman and Storer identified significant trade shortfalls that began to appear in 2002 and 2003.[11]

Just as important for the Great Lakes Gateway, Globerman and Storer found evidence of shifts in the trade shares of the port groupings. For U.S. exports to Canada, the share of the Great Lakes Gateway rises through 1998, hits a plateau around 2000, and then begins to decline. For imports from Canada, the share of the Great Lakes Gateway is fairly flat through 2000 and then begins to decline at an accelerating pace. The import share of Blaine rises through 1999 and falls thereafter.

The Globerman and Storer analysis also found trade disruption effects that seemed to be of shorter duration in the Great Lakes Gateway than in the Blaine/Cascadian Gateway. The authors speculate that the difference could be due to the greater utilization of programs such as FAST in the Great Lakes Gateway.

In recent years, the priority in the Great Lakes gateway has been to increase infrastructure. A new railway tunnel, the St. Clair Tunnel, was expanded south of Port Huron to accommodate larger rail cars in 1995. A second, twin span of the three-lane Blue Water Bridge between Port

---

[9] Danielle Goldfarb *Reaching a Tipping Point? Effects of Post-9/11 Border Security on Canada's Trade and Investment* Conference Board of Canada report (June 2007) Available at www.internationaltransportforum.org/2009/pdf/CDN_TippingPoint.pdf

[10] "Trade and Travel patterns at the Canada-U.S. Border: Policy Implications" *Border Policy Brief* Volume 4, Number 1 Border Policy Research Institute, Western Washington University (2009) Available at www.wwu.edu/bpri/files/2009_Winter_Border_Brief.pdf

[11] Steven Globerman and Paul Storer *The Impacts of 9/11 on Canada-U.S. Trade* (University of Toronto Press, 2008)

Huron, Michigan and Sarnia, Ontario was opened in 1997.[12] Together these investments helped to make Port Huron one of the busiest crossings on the Canadian border as other crossing points were in the process of building new infrastructure to keep up with the space requirements for new security measures instituted by U.S. and Canadian customs authorities and with demands caused by traffic volumes.

At Detroit, there is a bridge crossing, a vehicle tunnel, and a rail tunnel. The Detroit-Windsor Vehicle Tunnel was opened in 1930 and is nearly one mile long, passing underneath the Detroit River. Commuter buses, tour buses, cars and trucks pass through the tunnel on a regular basis, but traffic is easily congested because the entry and exit from the tunnel flows to downtown streets in both cities, and the space available to customs is limited by nearby office buildings. As a result, the tunnel is generally avoided by long-haul commercial traffic.

The rail tunnel at Detroit-Windsor opened in 1910, and continues to move freight although traffic through this tunnel diminished after the St. Clair Rail Tunnel opened in 1995. The Detroit River Tunnel Partnership proposed turning the former rail tunnel into a high capacity rail tunnel as well as a commercial truck crossing with up to six lanes of roadbed, but the plan failed to win approval from local authorities.[13] A second attempt was initiated in June 2010, dubbed the Continental Rail Gateway and backed by a coalition that included the Windsor Port Authority, the Canadian Pacific Railway, and Borealis Infrastructure Incorporated.[14] This new effort would build an entirely new tunnel capable of handling double-stacked trains and improving the throughput of the Detroit border crossing, and promises to generate and sustain 1,700 local jobs.

The Ambassador Bridge has long been the busiest crossing on the U.S.-Canadian border. Privately-owned and operated by the Detroit International Bridge Company (DIBC), the Ambassador Bridge carries more trade between the United States and Canada each year than flows between the United States and all of Europe and Japan combined. The Michigan Department of Transportation has undertaken a $230 million expansion of the Ambassador Bridge customs plaza to improve traffic flow and enhance access to Interstate 75 and Interstate 96, as well as to ease traffic problems affecting adjacent city neighborhoods. The DIBC has proposed a privately financed $1 billion second span for the Ambassador Bridge that is pending regulatory approvals.[15]

At the same time, a new crossing between Detroit and Windsor is being planned. Initially referred to as the Detroit River International Crossing (DRIC) and now known as the New

---

[12] "History of the Blue Water Bridge" Michigan Department of Transportation Available at: http://www.michigan.gov/mdot/0,1607,7-151-9618_11070-22062--,00.html

[13] For more on the Detroit River Tunnel Partnership, see: http://www.detroitchamber.com/index.php?option=com_content&view=article&id=232%3Adetroit-river-tunnel-partnership&catid=13%3Apolicy-and-legislation&Itemid=178

[14] For more on the Continental Rail gateway, see: http://www.crgateway.com/home.aspx

[15] *Connecting Neighbors: The Ambassador Bridge Gateway Project* Michigan Department of Transportation (August 2007) Available at http://www.michigan.gov/documents/mdot/MDOT_Amb_Bridge_gateway_newsletter_0807_206463_7.pdf

International Trade Crossing (NITC), this bridge would handle vehicle traffic from a crossing point roughly two miles downriver from the Ambassador Bridge. The NITC would connect Interstate 75 and Ontario's Highway 401 while bypassing Huron Church Road, which passes through the City of Windsor and is subject to congestion and delays. It would require the construction of additional customs inspection space in both countries, additional customs personnel, and a new three-mile long highway to connect the bridge to Highway 401 via the E.C. Row Expressway on the Canadian side. Planning for this connector began in 2006, and a route and design have been approved.

Planning and permitting for improvements at the Detroit-Windsor crossing involve the two federal governments, the governments of Michigan and Ontario, the counties of Wayne (Michigan) and Essex (Ontario), the cities of Detroit and Windsor, and neighborhood groups on both sides. Despite growth in traffic from 1989 onward, governments willing to invest in additional crossing infrastructure after the September 11, 2001 terrorist attacks, and an organized business and labor constituency lead by the auto industry supporting additional infrastructure, the delays have been considerable and frustrating to local residents.

The International Bridge connecting the cities of Sault Ste. Marie Michigan and Sault Ste. Marie Ontario is the northern terminus for U.S. Interstate 75, and is the only vehicle crossing between the Pigeon River Bridge (connecting Ontario and Minnesota) and the Blue Water Bridge. It carries modest annual traffic volumes, but remains an important link between the United States and Canada due to its location.

The land linkages for motor vehicles and rail are focal points for trade and border security efforts, but emphasis on these vital connections obscures the importance of the maritime border between the United States and Canada formed by the Great Lakes, specifically Lake Superior, Lake Huron, Lake Erie, and Lake Ontario and the rivers and canals that connect these lakes. The lakes are connected to the Atlantic Ocean by the St. Lawrence Seaway, a 2,500 mile route that opened in 1959. The U.S. Coast Guard, part of the U.S. Department of Homeland Security, maintains stations along the Michigan shoreline border with Canada, including stations at Belle isle, Harbor Beach, Port Huron, Saginaw, St. Clair Shores, and Tawas.

Not to be overlooked, the United States is connected to Canada by air linkages. There are approximately 243 airports operating in Michigan, many of which are small general aviation facilities or public use air strips. Detroit-Wayne County Metropolitan Airport is the busiest passenger airport in the state with more than 16 million passengers passing through its gates each year and a U.S. Customs presence for international flights and air cargo inspection. In addition, Michigan is home to two military airports with the Department of Homeland Security present in the form of the U.S. Coast Guard. The U.S. Coast Guard Air Station at Traverse City has an area of operations and patrol that includes all of Lake Michigan, Lake Superior, and most of Lake Huron.

Lower Lake Huron, Lake St. Clair, the St. Clair and Detroit rivers and western Lake Erie are patrolled by the U.S. Coast guard Air Station Detroit, which is co-located with U.S military and

National Guard operations at the Thomas Selfridge Air National Guard Base (ANGB) in Harrison Township, not far from the Canadian border.

Selfridge ANGB, established in 1917, has been home to U.S. Air Force and Navy detachments, and presently hosts the U.S. Department of Homeland Security's Operational Integration Center (OIC), a fusion center that links video, radar and satellite imagery with DHS, U.S. military, and federal, state and local law enforcement assets for rapid response. The Selfridge OIC supports integrated border security efforts across the Northern Border's Detroit Sector, which covers 863 miles of mixed land and maritime boundary and is the largest operational sector on the U.S. border with Canada.

Although the largest item in U.S-Canada trade has generally been motor vehicles and parts, in recent years energy has been the fastest growing category. And although the automotive trade has been a mutual exchange of imports and exports that attains a stable equilibrium, the energy trade heavily favors Canada, which has become the largest foreign energy supplier to the United States.

In 2008 Canada supplied seventeen percent of all U.S. oil imports, and U.S. refineries process most of this product (sustaining high-paying U.S. jobs). Canada also supplied eighteen percent of overall U.S. natural gas demand. Both oil and natural gas enter the United States from Canada through established pipelines, making this trade different from other goods crossing the border. The pipeline infrastructure must be inspected and secured, but the oil and gas cross the border without interruption. Building new pipelines involves some of the same problems as building other infrastructure that crosses the border, with multiple and overlapping permitting processes that make progress slow.

Canada is also a major supplier of electricity to the United States. In 2006, Canada exported 41.5 billion kilowatt hours (Bkwh) of electricity to U.S. markets, and imported 23.4 Bkwh that same year due to seasonal variations in domestic energy demand for electricity in Canada and the proximity of some U.S. supplies to Canadian consumers. Canada is the second largest generator of hydroelectricity in the world (after China, which leapt ahead with the completion of the Three Gorges Dam project). The Obama administration's plans to build a national Smart Grid for electricity transmission is intended to help alternative electricity generators to reach larger markets, but has the ancillary benefit of allowing Canada to export electricity across more states and sell to markets further away from the northern border. Although there are environmental concerns related to the flooding of land associated with hydroelectric dams, the carbon content of hydroelectricity once a dam is built compares favorably with other modes of electricity generation and imports from Canada will be attractive to many states and metropolitan regions seeking to replace coal-fired plants.

Canada is also the largest generator of nuclear power in North America, and the source of one-third of worldwide uranium ore production. This has led to support in Canada for the establishment of one or more nuclear waste reprocessing and storage facilities as a gesture of responsible environmental stewardship: as an exporter of uranium, some in Canada argue that it

should become an importer of the waste byproduct of its use for energy production. The Canadian Shield, an 800,000 square kilometer bedrock formation that stretches across most of the Canadian land mass provides ideal geology for safe storage of nuclear waste material.

The largest source of Canadian energy potential is the oil sands deposits located principally in the western provinces of Alberta and Saskatchewan. The carbon expenditure involved extracting bitumen from oil sands is high, and has led the Alberta provincial government to invest $2 billion in oil royalties in researching methods for effective carbon capture and sequestration (CCS). The Obama administration pressed Congress for $3.4 billion for CCS research with a view to addressing the carbon emissions from coal-fired plants in the United States which was subsequently approved as part of the stimulus legislation in February 2009. The Canadian federal government has promised to invest an additional $1 billion in CCS research as well in 2009. The research challenge is to develop ways to capture carbon emissions, after which storage is relatively simple. However, the same vast expanses of Canadian geography that provides locations for the safe storage of nuclear waste could also provide safe storage for captured carbon if CCS research bears fruit.

This suggests the potential for U.S. exports of nuclear waste and even captured carbon for storage in Canada. Although currently there are significant shipments of ordinary garbage from Metro Toronto to landfills in border states such as Michigan (although the volumes have recently been decreasing due to the opening a new landfill in Woodstock, Ontario that now handles most of Toronto's trash), energy-related waste shipments would create new challenges at the northern border.

At DHS, energy trade across the U.S.-Canadian border has been addressed most directly as a challenge of critical infrastructure protection and preparation for emergency response. Since this is an area where DHS collaborates well with state and local government, first responders including police and fire services have learned about current cross-border infrastructure and its vulnerabilities and energy firms that own this infrastructure or the energy that utilizes it have been in close contact with public sector officials at all levels in both countries. Participation in tabletop exercises and drills has deepened the mutual awareness of capabilities and knowledge of procedures and contingencies across the public and private sector alike. This is an area of border security management and trade facilitation between the United States and Canada that has worked remarkably well.

Michigan is at the heart of the growing U.S.-Canadian energy trade due to the infrastructure that connects the state to Canadians supplies of electricity, oil, and natural gas. Energy transportation infrastructure is by nature critical infrastructure that must be protected against terrorist attacks. The Michigan Public Service Commission Department of Licensing and Regulatory Affairs has looked carefully at the interconnections of the Michigan and Canadian grids in light of the August 2003 blackout. In addition, the July 2010 breach of Enbridge's oil pipeline, which contaminated the Kalamazoo River, led to new attention to the vulnerability of such transmission systems to accidents. Michigan has three nuclear power plants: Cook (in Bridgman, near the Indiana border on the Lake Michigan shore), Fermi II (on the shores of Lake Erie, near the Ohio

border) and Palisades (in South Haven, 40 miles further north on the Lake Michigan shore from Cook). Taken together, Michigan is a critical nexus of U.S. energy security and energy trade with Canada.

Border Security Dynamics and Trends

In the aftermath of the September 11, 2001 terrorist attacks on the United States, there was a significant effort undertaken by the U.S. and Canadian federal governments to upgrade border security. This upgrade occurred in three broad and overlapping phases, and a fourth phase is currently underway. Each phase was associated with a different set of opportunities for the private sector to win DHS business.

Phase 1 consisted of a remedial investment in infrastructure and staffing. As part of negotiations with the U.S. Congress to secure the ratification of the North American Free Trade Agreement (NAFTA), the Clinton administration agreed to transfer one third of customs and border patrol personnel from the northern border to the southern border in anticipation of an increase in border crossing volumes following the implementation of NAFTA. This was justified by the increase in border crossing volume on the northern border following the ratification of the Canada-United States Free Trade Agreement (CUFTA) five years before. However, this left the northern border understaffed through 2001.

In addition, the United States had neglected investments in northern border infrastructure habitually since the completion of the St. Lawrence Seaway in 1959. Facilities and inspection equipment were inadequate for the task, and proposals for electronic documentation and processing—which amounted to submission of paperwork to U.S. Customs by fax at that time—were slow to be implemented, causing significant frustration among commercial shippers.

The phase 1 investment in new facilities, transportation infrastructure to connect to the new facilities, new inspection equipment and vehicles, and new personnel began with bipartisan congressional support in 2002 and has continued to the present. With a few notable exceptions (the NITC stands out in this regard) the major border infrastructure projects inaugurated by the U.S. government since 2001 are nearing completion. There will undoubtedly be future opportunities for private sector contracts for new infrastructure, but these will not be likely to return to the scale witnessed in response to the 2001 terror attacks.

In addition, phase 1 saw the hiring of large numbers of new federal personnel for US Customs and Border Protection, the Transportation Safety Administration, the Border Patrol and other border agencies. Recruitment and training presented a surge in additional opportunity for the private sector, particularly in higher education (from universities and community colleges to for-profit professional training institutions). While major recruitment activity has now settled into a more normal pace, the ongoing need for training provides continued potential for non-governmental educators.

Phase 2 If the first phase of border security changes after 2001 involved catching up to where security investments and infrastructure ought to have been, the second phase involved modernizing border security and inspection through the deployment of advanced technology. Modernization of the border included the acquisition and installation of a range of new devices, from radiation detectors to license plate readers, from databases and passport scanners to unmanned aerial vehicles and remote sensing equipment.

Many of the technologies acquired in phase 2 provided new and more effective solutions for extant missions; other technologies offered entirely new capabilities to enhance mission effectiveness. In both categories, DHS benefitted from innovation in the private sector, which responded dynamically to meet DHS needs at the border.

Phase 3 involved an extension of the modernization of border technology and infrastructure to facilitate cooperation and collaboration with international partners, and Canadian border security agencies were among the first and most enthusiastic of these partners. There were opportunities for the private sector as friendly partners sought to procure technologies compatible with or identical to U.S. systems, and DHS in some cases sought the assistance of the private sector in resolving challenges related to intelligence sharing, communication, and data processing with foreign customs and border security agencies. In the land border security realm, DHS frequently sought technologies that would be used at both the northern and southern borders of the United States (despite differences in terrain and conditions), for example as part of the Secure Border Initiative (SBINet) program.

The United States has recently entered Phase 4 wherein efficiency is becoming paramount: efficient identification of identity for faster clearance of goods and people at the border, efficient threat assessment and dissemination of credible intelligence, and efficient use of resources, from personnel to equipment in pursuit of DHS missions. Behind the drive for efficiency is the growing pressure of fiscal constraints in the United States. In establishing DHS and upgrading border security, Congress was prepared to generously fund the new department and its agencies. Ten years after the September 11, 2001 attacks and with an unprecedented national debt burden, DHS is facing new resource constraints.

This will create new opportunities for the private sector in two respects. First, efficiency and productivity solutions will be highly appealing to DHS and its international counterparts as they seek to do more with less. Second, it is likely that DHS agencies will seek to shift certain burdens and tasks onto trusted shippers and travelers, and thereby “shrink the haystack” in which it is searching for the “needle” of a terrorist threat. As a result, firms engaged in cross-border trade will seek new products and services that will lower the compliance burden associated with border security measures.

Raising efficiency will also increase pressure on DHS to decrease inefficiencies and address problems in coordination with other federal, state, tribal and local law enforcement agencies. A

December 2010 report by the U.S. General Accounting Office highlighted problems in these areas specific to the U.S. northern border.[16]

Proposed Northern Border Policy Changes

On February 4, 2011 U.S. president Barack Obama and Canadian Prime Minister Stephen Harper issued a declaration on the northern border at a summit in Washington, D.C. entitled *Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness*.[17] It includes a set of principles, identifies specific areas where bilateral cooperation could be improved upon, and sets up a binational working group to provide oversight to the process.

Principles: For the most part, the principles set out in the Washington Declaration on the U.S.-Canadian border are salutary and intended to address the charges being leveled by Harper's domestic political critics. The Declaration pledges respect for each country's respective constitutions, the virtues of cooperation, the valuable contributions of many partner agencies that are non-federal in each country, respect for the sovereignty and independence of each country, and openness to working with other countries around the world.

More substantively, the Washington Declaration emphasizes an ongoing commitment by both countries to the risk management approach to border and supply chain security. This approach was adopted by the United States soon after 2001 and has been central to DHS planning and operations. It also requires intelligence gathering and information collection on a massive scale in order to assess risk. Canada has joined the United States in accepting this approach, and on consequence of this is that an increased amount of data sharing among the agencies of the two governments will be required. Canadian opposition critics have flagged citizen privacy concerns where increased information sharing has been proposed in the past—as have European countries during negotiations on the visa waiver program. Canada currently shares less than many visa waiver program partners of the United States—a concern raised by former DHS Assistant Secretary for Policy Stewart Baker in his memoir.[18] Information sharing, specifically, the exchange of individual entry records, will be central to a future deal on entry-exit information.

The Washington Declaration also emphasizes the commitment of both governments to improving the resilience of each country's critical infrastructure; that is, its ability to bounce back after an attack or disruption due to a natural disaster. A high degree of interconnectedness characterizes U.S. and Canadian energy, transportation, public health, telecommunications and other systems and several recent incidents, from the 2003 SARS outbreak in Toronto to the 2007 electricity blackout affecting the U.S. Midwest and Northeast, have served to underscore this

[16] The GAO report, *Border Security: Enhanced DHS Oversight and Assessment of Interagency Coordination Is Needed for the Northern Border* (GAO-11-97) is available here: http://www.gao.gov/new.items/d1197.pdf

[17] Executive Office of the President. "Declaration by President Obama and Prime Minister Harper of Canada - Beyond the Border" February 4, 2011. Available here: http://www.whitehouse.gov/the-press-office/2011/02/04/declaration-president-obama-and-prime-minister-harper-canada-beyond-bord

[18] Stewart A. Baker, *Skating on Stilts: Why We Aren't Stopping Tomorrow's Terrorism* (Hoover Institution Press, 2010)

fact. While both governments have been publicly committed to improving emergency response and preparedness, the Washington Declaration notes the role that private sector owners and operators of critical infrastructure must be prepared to undertake. At a time when automotive manufacturing, public health and energy sectors are facing significant new regulatory mandates in the United States, the hortatory call for action here may not be enough to prompt an adequate response. Still, in the wake of the U.S. experience during the BP oil spill in the Gulf of Mexico, it is significant that the two governments are recognizing here the limits of their ability to prepare for emergency response without private sector contributions. For now at least, the private sector is being urged but not required to invest in greater resilience.

Key Areas of Cooperation: The Washington Declaration on the U.S.-Canadian border citers four areas where the federal governments of Canada and the United States intend to improve their cooperation: addressing threats early; trade facilitation, economic growth and jobs; integrated cross-border law enforcement; and critical infrastructure and cyber-security.

The United States and Canada intend to improve their pre-emptive threat actions in the areas of natural disasters and what the Obama administration refers to as "man-made threats, including terrorism." In this section of the Washington Declaration, the governments agree to improve cooperation in emergency preparedness and response explicitly for future pandemic outbreaks and post-disaster recovery. Because this builds on similar pledges at North American leaders summits in Montebello, New Orleans and Guadalajara as well as the *U.S.-Canada Agreement on Emergency Management Cooperation*[19] (most recently updated in 2008) it is significant here mainly as a confirmation that the two countries intend to proceed to enhance bilateral cooperation where they had previously made such pledges in a trilateral framework.

In the area of counterterrorism cooperation, the two governments pledge to identify, prevent and counter violent extremism in both countries. This recognition of the rising concern over domestic "home-grown" terrorism follows recent al Qaeda statements on recruiting Americans and other western citizens to commit acts of terrorism since international law enforcement and military efforts have made it more difficult (though not impossible) for foreigners to infiltrate western countries to engage in terrorism. The two governments intend to work together at the community level, which will provide greater intelligence on the linkages between extremist groups in each country. This prompts the two governments to state that they will develop joint privacy and human rights protections to safeguard the constitutional rights of persons of interest and innocent bystanders who fall under surveillance. This enhanced depth of cooperation is both welcome and necessary, but the emphasis that the two governments have placed on civil rights reflects the challenges of action as well as expanded cooperation in this area.

Part of the early assessment of threats and the risk management approach that are central to the Washington Declaration on the U.S.-Canadian border is better information on border crossers. The two governments expressly pledge cooperation on entry-exit record keeping, noting its

[19] The full text of the *Agreement Between the Government of the United States and the Government of Canada on Emergency Management Cooperation* is available here: http://www.state.gov/documents/organization/142916.pdf

importance (a departure for Canada) and also calling for new standards for common technical standards to support identification documents required for border crossing. It is rumored that the Harper government is considering implementing a passport requirement for Canadians returning home from the United States, a policy that mirrors the U.S. approach and this pledge in the Washington Declaration is consistent with this possibility.

The identification of trade facilitation, economic growth and jobs as a key area for improving cooperation between the two countries is a reflection of the lagging economic recovery in the United States, which affects Canada as well through lower export revenues even though Canada's recent economic performance has been much improved since the downturn began in 2008. Canadians have often been criticized in the United States for their perceived focus on trade facilitation at the expense of security, but the times augur for the Canadian approach acknowledged here. Significantly, the two governments emphasize facilitation here in terms of reductions in compliance costs and border crossing delays; this formulation is more compatible with the security mission and is more likely to win support within DHS and the U.S. Congress.

Infrastructure at the border is much improved since September 2001, but the two governments pledge in the Washington Declaration to address some of the remaining chokepoints where traffic is vulnerable to congestion and room for inspections by border officials is constrained. The two governments also pledged to explore opportunities for shared facilities at lower-traffic crossings such as those built at Sweetgrass, Montana and Coutts, Alberta and at Alburgh, Vermont and Noyan, Quebec.

Perhaps the most promising new pledge in the Washington Declaration on the U.S.-Canadian border from an economic point of view has the governments establishing bi-national point of entry committees—a step strongly endorsed in the Brookings-Canadian International Council study *Toward a New Frontier: Improving the U.S.-Canadian Border*.[20] These committees would include the local business community and other stakeholders and give them input on port operations. This will provide Customs port directors with valuable intelligence on traffic fluctuations and generate ideas for improvements and pilot projects to test future improvements. The port of entry committees also introduce at least potentially an element of flexibility in border crossing management that could allow adaptations to local conditions rather than a rigid adherence to the "One Border" approach.

The Washington Declaration's commitments to binational cooperation in integrating cross-border law enforcement and protecting critical infrastructure and providing cyber-security are understandably less specific. There is already an extensive amount of cooperation among the responsible agencies in the United States and Canada in these areas and so this brief mention is either an acknowledgement of the importance of ongoing cooperation or a signal of further deepening of collaboration that will become clearer in time.

[20] Christopher Sands. *Toward a New Frontier: Improving the U.S.-Canadian Border* (Brookings Institution and Canadian International Council, 2009)

By shifting northern border management to allow for more local variation, stakeholder input, public-private partnership, and pilot projects to test new approaches, the United States and Canada are relying on a greater degree of local input and experimentation than ever before. This will put additional pressure on relationships among federal agencies with border security responsibilities and between the federal, state, local and tribal governments and law enforcement agencies whose missions overlap. In addition, it will add to the already powerful fiscal incentives toward public-private partnerships in border security such as the Free And Secure Trade (FAST) program and the Customs-Trade Partnership Against Terrorism (C-TPAT).

Michigan's Competitive Strengths

The trend toward enhancing security by leveraging networks of public and private, U.S. and Canadian border players, combined with an efficiency-solutions emphasis in DHS thinking about border security, and a similar shift among border users, will play to Michigan's competitive strengths.

The State of Michigan offers a variety of terrain including the largest maritime segment of the northern border; firms and communities large and small that are all affected, though in different ways, by changes in border operations; high-volume border crossings and low-volume crossings, including the busiest commercial land crossing in the world (Ambassador Bridge) and significant numbers of individual border crossers engaged in tourism, service trade, education, and family visits. The variety and scope of the Michigan segment of the northern border makes it the ideal place to pilot, test, and introduce new technological solutions aimed at making border security more efficient and effective.

The established federal presence in Michigan is another important advantage. Under pressure from Congress and the White House prompted by the GAO report, DHS will seek to improve coordination among its component agencies and with other federal, state, tribal and local agencies such as the federal Drug Enforcement Agency (DEA), state police, and local stakeholders. Testing new technology, information systems and procedures in Michigan can capitalize on the presence of DEA, the FBI, CBP, the Border Patrol and Coast Guard, Michigan National Guard and State Police.

Easy air connections to Washington, DC and DHS headquarters make the incorporation of DHS leadership in pilot projects in Michigan feasible. The proximity of Michigan to Ontario—the heartland of the Canadian economy with more than 40 percent of the Canadian population and much of Canada's trade with the United States—as well as easy air connections to Ottawa, the Canadian capital, provide a similar benefit for demonstration project with new technologies and other pilot projects developed and implemented in this region.

When it comes to innovation, Michigan has more than 350 transportation-related research and development facilities that have the ability to test products and new technology. Within the North American auto industry, Michigan has the largest concentration of research and development as well as applied engineering facilities and specialists. According to research by

the Michigan Security Network the range of testing that these companies can do includes but is not limited to:

- Noise, vibration, and handling (ride quality)
- Aerodynamics
- Emissions
- Thermal and climatic performance (cold, hot, wet, etc.)
- Antenna (power, range, etc.)
- Durability and reliability (components and wholes)
- Strength (e.g., of materials)
- Software (stability, bug free, etc.)
- Security (e.g., of devices and data)
- Cost-weight analysis, and
- Structural integrity.

In addition, Michigan has a strong university-based research and development capacity with extensive experience with public and private sector collaboration. The heart of any pilot or demonstration project is data collection and analysis, and from laboratory to real-world setting the universities and community colleges in Michigan offer significant potential for partnership with DHS and other border security agencies in the United States and Canada.

Commercial customers for homeland security applications, from software to physical security technology, represent the next wave of market growth for DHS suppliers in this sector. The presence of sophisticated supply chains in the auto industry as well as for other manufacturing and agrifood (perishable product) businesses should draw firms to locate in the Michigan area interested in a critical mass of private sector customers. Since threats posed by terrorism and smuggling are constantly evolving, supply chain security measures must continuously adapt as well, creating a steady demand for innovation and new business. For similar reasons, DHS should find Michigan an attractive location to test and pilot new security measures and equipment. This will add positive public-private synergy to the list of Michigan advantages for the homeland security sector.

This is not a speculative assessment; Michigan has been the source of successful public-private homeland security collaboration and innovation in the past. Even before 2001, U.S. Customs, working with General Motors, Ford Motor Company, and Chrysler Corporation began work on the precursor to the FAST program, known as the National Customs Automation Program (NCAP) as a pilot project. NCAP was part of the Automated Customs Environment (ACE) initiative, and was intended as a remedy for congestion at major crossings including principally Detroit, Port Huron, and Laredo (on the southern border). Despite NCAP's origins as a facilitation program, its success led U.S. Customs officials to propose expanding this program as a response to post-2001 security concerns, renaming the program FAST.

Border Security Economic Development Strategy

There are a number of additional steps Michigan can take to ensure that it retains a continued leadership role and becomes an ever more attractive location for border-related business development.

Pilot Projects Capitalizing on the new interest in pilot projects to enhance security and adapt to local conditions or commercial sector concerns, Michigan should help to coordinate among local firms, governments and public safety agencies to develop specific proposals to solve local needs and address local concerns and problems. This might include (though would not be limited to): convening stakeholders in border security charettes in order to identify and develop ideas; building consensus and participation among relevant organizations in support of the experiment; and possibly financing or subsidizing early stage development or negotiating a cost-sharing arrangement with DHS to make locally-developed pilots attractive to DHS given fiscal constraints. Despite Michigan's natural advantages, other states and northern border regions such as New York and the Pacific Northwest are likely competitors for such projects and the economic benefits that accrue from a successful pilot effort.

Trusted Traveler/Trusted Shipper Programs The Great Lakes gateway with Michigan at its heart has the largest enrollment in trusted shipper (FAST and C-TPAT) and traveler (NEXUS) programs. As the most intensive users of these programs, Michigan residents ought to be the best at using them; the reality is that participation in these programs is highly-concentrated. This presents Michigan with a valuable opportunity: to leverage the experience of a relative few firms and individuals participating in these programs intensively to train logistics managers, business travelers, truck drivers and even occasional border crossers in how to enroll and maximize their benefit from these programs. Initially, this might involve training for shipping managers and those responsible for border-related paperwork and filings. Over time, this could foster a skilled workforce capable of expediting border transactions at the lowest possible compliance cost. Since Canada is the United States largest export destination, the ready availability of these skills could prove attractive to small and medium sized businesses for which a Michigan location would boost Canadian sales.

Northern Border Security Test Bed DHS has used a number of locations to test new technologies and systems, procedures and personnel. Michigan should work with DHS to attract more test bed activity in close proximity to the firms and geographic conditions that the state has to offer. In practice, the challenge is to facilitate the participation of local firms and governments; when all of the necessary collaboration is predisposed to work with DHS and any firms involved, the prospects of a successful test are thereby improved. DHS has the choice of numerous offers from regions hoping to attract test bed activity, and a "Team Michigan" approach will make Michigan competitive.

Northern Border Center of Excellence The DHS Science and Technology Directorate has developed a Centers of Excellence network, drawing together consortia of university research and expertise in areas relevant to DHS missions. The National Center for Border Security and

Immigration (NCBSI)**,** led by the University of Arizona in Tucson (research co-lead) and the University of Texas at El Paso (education co-lead), was established and charged with developing technologies, tools, and advanced methods to balance immigration and commerce with effective border security. Yet the differences between the conditions at the northern and southern borders of the United States suggest that DHS should allow for two such centers, networked together but devoting attention to distinctive problems and solutions. The establishment of a Center of Excellence on the northern border could also foster university research collaborations with Canadian universities and researchers; their participation will make Canadian government buy-in for new technologies more likely, and add an additional benefit to DHS. Michigan, especially its congressional delegation, should work toward the establishment of a National Center for Northern Border Security and Immigration (NCNBSI) to complement the existing Center of Excellence on the southern border and enhance U.S. national security innovation.

Expansion of Selfridge OIC The U.S. Department of Homeland Security's Operational Integration Center (OIC) at Selfridge ANGB has a limited range of current monitoring capacity that should be expanded to include the entire Detroit sector through the installation of additional cameras and the deployment of additional UAVs to this location. Working with DHS and the US Department of Defense, Michigan should seek to contribute to the information collection and analysis underway at the OIC and foster its expansion, as well as innovation in the use of OIC data and coordination among federal state, tribal and local law enforcement and first responders.

Regulatory Cooperation Demonstration Projects In addition to border security pilot projects, Canada and the United States are committed to pursue greater regulatory cooperation through a new Regulatory Cooperation Council announced by President Obama and Prime Minister Harper on February 4, 2011.[21] Given the significant private sector interaction with regulatory compliance via border inspection, Michigan should foster the development of demonstration projects in regard to regulatory and inspection procedures by responsible agencies of the U.S. and Canadian, as well as state and provincial governments. This work would benefit from the capacity to include front line inspectors and leading companies present in Michigan, and might also foster employment in the product testing and compliance fields.

Energy Corridor Security Michigan is at the center of a network of energy transmission, via pipelines and powerlines, to and from Canada, the United States' largest foreign energy supplier—our number one source of imported electricity, oil, natural gas, and uranium. In addition, Canadian proposals to establish nuclear waste storage and disposal facilities could lead to nuclear waste trans-shipment across Michigan. Michigan should seek to work with its energy companies, local utilities, local first responders and federal regulators to enhance the security of these energy transmission systems through interagency exercises, scenario planning, monitoring and enforcement. Pilot programs and new initiatives should be proposed to the U.S. Department of Energy and the Federal Energy Regulatory Commission as well at to DHS. Michigan should

[21] For more on the Regulatory Cooperation Council initiative, see Christopher Sands *The Canada Gambit: Will It Revive North America?*(Hudson Institute, 2010) available at: http://www.hudson.org/files/publications/Canada%20Gambit%20Web.pdf

create a fund for the development of innovative security technologies to safeguard pipelines and powerlines, as well as generation stations. State-led efforts to upgrade the electrical grid to a "smart grid" should include security measures, and the interoperability of these measures with the Canadian grid interconnections. On the front lines of U.S. energy imports from Canada, Michigan and its companies should lead in securing energy infrastructure.

Trade Corridor Coordination It is a persistent irony of border security that the jurisdictions adjacent to the border are not the only jurisdictions affected by changes at the border—communities in the interior of the country benefit or suffer as well. Yet when it comes to the advocacy for border security investments and reforms, border jurisdictions are typically alone in leading the charge. Michigan should seek to engage the participation of state and local governments along exiting trade corridors that connect far-flung parts of the United States and even Mexico to Michigan border crossings with Canada. This effort starts with raising awareness, but leads to joint lobbying for infrastructure and federal investments that benefit trade and travel for everyone along the specific corridor. Michigan should not have to advocate for its segment of the northern border alone, and given the fiscal constraints in Washington, DC Michigan will prove less successful alone that it might with a wider coalition.

In addition, many firms and citizens whose livelihood and profitability is connected to border access remain unaware of this fact and therefore disinterested in contributing to solving border challenges. Michigan should lead the effort to bring together border stakeholders and encourage regional cooperation on northern border issues.

Workforce Development Analysis

Hanns Kuttner

While Michigan's geographic location creates a natural advantage for innovation in homeland security, Michigan's ability to make the most of that advantage depends on the human capital available in Michigan. If Michigan workers do not have the skills required, the work will take place elsewhere. Human capital is one constraint Michigan faces in trying to make the most of its border position.

The homeland security challenge has created two separate sources of workforce demand. One derives from activity to provide the goods and services required by the federal government to create and implement the tools, techniques and procedures to meet the homeland security challenge. The other source is everything but the federal government, including other levels of government and the private sector. Unlike defense, where the federal government is the primary source of demand, there are many sources of demand for the goods and services that make up the homeland security market. Each layer of government has a preparedness responsibility. Each firm that ships goods across national borders must manage border risk. Each person and organization who connects to the Internet takes on risk from the less savory elements that troll the Internet, searching for vulnerabilities in order to carry out activities that range from mischief to criminal acts to espionage.

Seen as an "industry," homeland security, then, is both concentrated and diffuse. The concentrated components include the firms and organizations that supply goods and services to the federal government. Some may primarily be in the business of fulfilling government contracts, but many also supply other levels of government, the private sector, and individuals. These firms and organizations make up the homeland security sector, analogous to the defense sector that more narrowly supplies the Department of Defense.

The diffuse component is much larger. It includes both identifiable parts of larger organizations, such as those within firms who carry out the shipping and traffic function and are responsible for moving goods both within the US and across its borders. It is also one responsibility of multi-purpose organizations. For example, local public health departments must be prepared to deal with outbreaks caused by novel infectious agents whether the agent arises through natural processes or is introduced in a bioterror incident. Similarly, those within an organization who have responsibility for computer security have responsibility both for repelling intruders conducting industrial espionage as well as intruders who might be deployed as part of cyberwarfare.

The risks that arise from the homeland security challenge are one of many risks every organization must manage. Users must decide whether to make or to buy risk management; do we create our own security tool or do we buy a software product from an outside vendor? The

make/buy decision determines where the jobs are located. A decision to "make" means that the job gets counted as part of the sector to which the "make" firm or organization belongs. It could be a hospital, a utility, or Tier 1 auto supplier. A decision to "buy" means the job is more likely to be in a firm that is more closely part of the homeland security sector. Still, the diffuseness of the homeland security sector means the job will be in a firm that is classified as a provider of computer software and services or a logistics company. The standard classification schemes used by the federal statistical agencies do not include a category specifically for firms and organizations that focus on homeland security.

The Homeland Security Sector

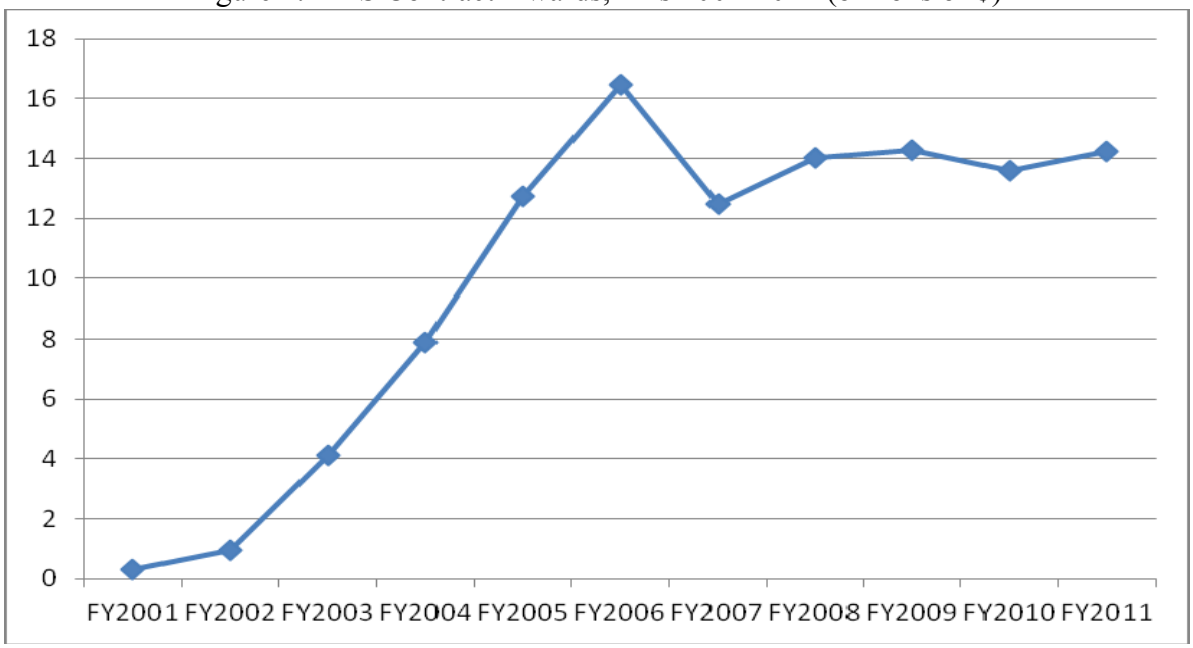
The federal government is a directly observable source of demand. The most direct workforce demand is people who work for the federal government. While the creation of the Department of Homeland Security (DHS) concentrated the federal government's responsibilities and functions in one organization, it did not create as singular a focus as the Department of Defense has in the defense area. For example, responsibility for developing medical countermeasures to public health medical emergencies rests with the Department of Health and Human Services. The Federal Bureau of Investigation has become an important homeland security agency and is in the Department of Justice. Because federal employment statistics are available by agency, not function, DHS employment is the best approximation of the federal homeland security workforce. DHS employment should be viewed as a lower bound on the number who are the federal homeland security workforce. Overall, DHS employed 180,000 workers in 2010. No state-by-state breakdown is available.

The federal government enters into contracts to obtain goods and services it has decided to buy rather than make. Those who work for contractors are also part of the homeland security workforce supported by the federal government. Again, the available data is organized by government agency, not function.

The dollar amount of DHS contracts rose rapidly following 9/11 but in more recent years has been at a plateau.

DHS contract data shows that federally-supported work is concentrated in regional clusters. In some industries, geographic clustering of businesses and their suppliers emerges. Southeast Michigan knows about this phenomenon through the clustering of automotive-related activity. For DHS, clustering has occurred around Washington, DC. About one-third of all DHS contract dollars in FY 2011 went to firms and organizations in the District of Columbia, Virginia, and Maryland.

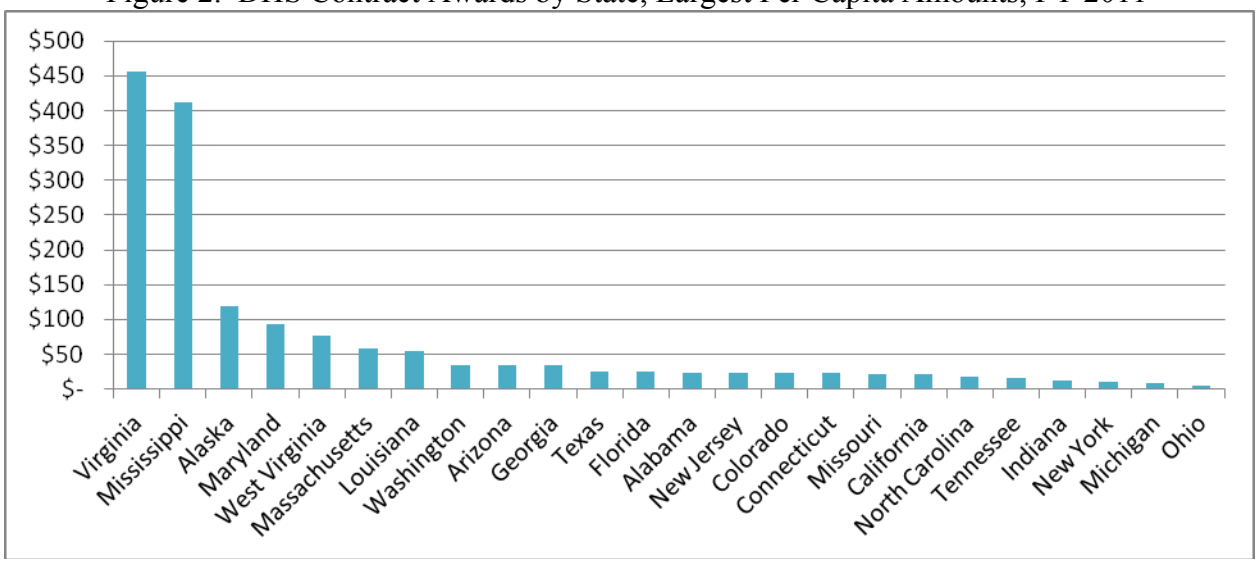
Figure 1. DHS Contract Awards, FYs 2001-2011 (billions of $)



Source: Hudson Institute analysis using data from usaspending.gov

Figure 2 shows the dollar amount of DHS contracts awarded in FY 2011, taking into account the relative size of states by dividing contract awards by state population yielding per capita amounts. (It omits the District of Columbia, where DHS contracts per capita were, by far, the largest: $4,515.) Michigan, with $7.93 in contract awards per capita, falls in the middle of the distribution. Even if Michigan contractors doubled their dollar volume of DHS contracts, Michigan would only move up four places in the per-capita rankings. DHS contracts would have to increase five fold in order for Michigan to be among the top ten states ranked by per capita contract awards.

Figure 2. DHS Contract Awards by State, Largest Per Capita Amounts, FY 2011



Source: Hudson Institute analysis using data from usaspending.gov

The per capita data reflects some of the underlying patterns of DHS procurement. Mississippi does very well because a Mississippi shipyard received contracts to build ships for the Coast Guard. Alaska's standing reflects in part the status Alaska Native Regional Corporations have, a status that makes it easier to use them as contracting intermediaries, leading to sub-contracts for work in other states.

DHS contracts are a very small part of Michigan's economy. The $78.4 million in FY 2011 contract awards amounted to less than .1 percent of Michigan's total economy. (Contracts are not the only source of DHS economic impact on Michigan. Grants added an additional $56.1 million. Still, the two together remain less than .1 percent.)

However, the structure of DHS contracting data makes it difficult to discern the actual impact on the state. For example, in the computer service area, the firm that received the largest number of DHS contracts for work in Michigan has a New Mexico address. The federal government does not collect data to show what share of the work under the contract is done in Michigan and what share in New Mexico.

DHS contracts reflect the wide scope of activities that fall under the jurisdiction of DHS. For example, the single largest contract award to Michigan went to Computer Sciences Corporation in Southfield. Under this contract Computer Sciences Corporation provides support for the National Flood Insurance Program, one of the many components of DHS.

This focus on DHS omits what is likely the largest homeland security-related contract activity in Michigan. Emergent Biosolutions produces anthrax vaccine stockpiled by the federal government from a facility in Lansing. Emergent Biosolutions received contracts for $125 million in FY 2011, making it the largest homeland security contractor in Michigan.

Homeland Security in Other Sectors

Michigan has not yet become one of the leading states for federal homeland security contracts. However, federal contracts are only one facet of the homeland security sector.

Some activities must, by definition, take place at the border, and the border is one thing that cannot be taken from Michigan. Yet in many cases the workforce required can be met by tapping into the national labor market. Someone moving to Michigan to take a homeland security job means someone already in Michigan did not benefit from that opportunity.

More importantly, much of the homeland security-related workforce can be anywhere. Software used in cybersecurity can be written anywhere. Lab work that cannot be done by Michigan workers can be sub-contracted to organizations that have people with the required skills in other states. While Michigan has an advantage, location is in very few places a guarantee that the human capital requirement will be met by creating opportunities for workers who already are in Michigan.

Only a portion of the human capital required for the homeland security challenge is specific to homeland security. Most is "dual purpose." Much of the work can be done by people who have skills and experience that is valued both in the homeland security sector and also in other sectors of the economy. However, some employment settings require workers who have security clearances, and the relative scarcity of this factor may keep some opportunities from Michigan workers.

Following the structure of the report overall, this workforce analysis looks at human capital needs in biodefense, cybersecurity, and border security.

1. Biodefense

Products. Biodefense is the area where Michigan does best in homeland security-related federal contracts, all thanks to one firm. The primary provider of anthrax vaccine stockpiled by the United States government, Emergent Biosolutions, produces the vaccine it supplies to the federal government in Michigan. A look at the firm's current openings shows the skills required in biodefense are "dual use," producing a product for biodefense using skills that are also in demand outside biodefense.[22] On the science side, the firm wants to recruit PhD-level researchers in the fields of cellular and molecular biology and immunology. Other staff are required who have the skills to execute standard laboratory procedures such as Western blot and ELISA (enzyme-linked immunosorbent assay) and use cell culture techniques. All of these skills and fields of knowledge are widely used outside biodefense. Biodefense is an area where the highly-skilled graduates of programs in the biosciences offered by Michigan's colleges and universities may find work.

[22] "Current Job Openings," https://jobpostings.ebsi.com/prdcss/JobPostings.html. Accessed January 16, 2012.

Other skills are the same as would be required in any life sciences manufacturing environment. Some of these are specific to life sciences, such as understanding the requirements of the good manufacturing practices required by the Food and Drug Administration (FDA.) Other skills are those required in any manufacturing company; those of a buyer, for example.

Because Michigan's performance in this area is tied to one firm, future labor force requirements will depend on how well that one firm does at retaining and obtaining new federal contracts.

Public health preparedness. A public health workforce that has the training and readiness to confront a terror incident is an important part of overall readiness. Without an effective public health response, the consequences of any event are likely to be greater.

Michigan had been in the lead in this area. The University of Michigan School of Public Health received support from the federal government's Centers for Disease Control and Prevention to provide training for the public health workforce. It appears that training in this area depends on dollars from the federal government. When the federal government decided to shrink the training network, Michigan lost out. The University of Michigan Center for Public Health Preparedness closed in August 2010.[23]

This experience offers a reminder that much of the demand for border security services at other levels of government comes from the federal government. As relative funding priorities for the federal government changes, so, too, will the opportunities that Michigan can pursue.

2. Cybersecurity

The cybersecurity job market in Michigan has two components, employers already in Michigan with cybersecurity needs, and cybersecurity service providers. Developing a workforce with federal security clearances and specialized certifications as prerequisites for employment for both components is a significant challenge.

Employers already in Michigan. Every organization with at least one computer or device that connects to the Internet has a cybersecurity challenge. Viruses, intrusions, and password security are issues that arise as soon as an Internet connection has been made. In the world of cybersecurity, physical location is not important. Each node on the Internet is equally vulnerable.

How organizations manage the challenge depends on their scale. In a one-person organization, cybersecurity is one of too many challenges. In organizations large enough to have one or more persons dedicated to information technology (IT), cybersecurity can be a component of one person's job or, in larger organizations, require one or more persons dedicated to cybersecurity.

This function combines an awareness of what the organization's requirements are with creating or buying the software and services that meet the organization's security requirements. For

[23] "Who We Are," http://practice.sph.umich.edu/micphp/index.php. Accessed January 13, 2012.

software and services, physical proximity is not important. The physical location of the software supplier is largely irrelevant and support is usually provided through call centers which, again, can be anywhere. Michigan-based staff procures software from vendors that may or may not be in Michigan. In the largest organizations or organizations with particular security concerns, cybersecurity is its own activity with dedicated staff. Some organizations have chosen to address cybersecurity needs for parts of their organization outside Michigan from a Michigan base.

As we noted in the report's discussion of talent enhancement in the cybersecurity chapter of this report, the most difficult challenge in cybersecurity needs may be individuals with a "cyber-managerial skillset," people who both understand the technical challenges and have the credentials to demonstrate to outsiders that they know what best practice demands and who have the managerial skills to develop the relationships outside the IT chain-of-command to bring about the institutional culture that meeting the cybersecurity challenge requires. Training programs that produce well-credentialed individuals are much easier to design and implement than those which produce the soft skills required for effectiveness at the top of the cybersecurity function. These key figures atop organizations are a small part of the overall cybersecurity job market.

The breadth of the cybersecurity challenge has created requirements for a cybersecurity function in many firms and organizations. The Bureau of Labor Statistics says job growth in this area can be expected to be much faster than average.[24]

To assess the total needs in this job market, we gathered a sample of 30 online job postings from late 2011 and early 2012 for cybersecurity-related jobs in southeast Michigan. Figure 3 shows the skills, experiences, and credentials most frequently mentioned in the postings.

[24] Bureau of Labor Statistics, Occupational Outlook Handbook, 2010-2011 Edition.

Figure 3. Mentions in Southeast Computer Security Job Postings, 2011-2012

Hardware/software/products	
Cisco networking products	14
Virtual private network (VPN)	11
Firewalls	10
Local area network/wide area network (LAN/WAN)	9
C/C++ programming language	4
Java programming language	4
Transmission control protocol/Internet protocol (TCP/IP)	4
HyperText Markup Language (HTML)	2
Linux operating system	2
Credentials	
Cisco Certifications (any)	5
Cisco Certified Network Associate	4
Cisco Certified Security Professional	1
Certified Information Systems Professional (CISSP)	4

We found two overall patterns. First, employers for whom cybersecurity is an ancillary activity use credentials and certifications as a tool to identify who is likely to have the skills they need. Second, employers whose focus is cybersecurity and who provide cybersecurity services used by other organizations want particular IT-related skills more than demonstrated skill that is specific to cybersecurity. Their strategy appears to be one of using people who have particular skills, usually skill with specified programming languages, and then using learning-by-doing to build the knowledge that is specific to their cybersecurity-related products.

The credential most frequently requested in the job postings after one of the certifications offered by Cisco for its networking products is CISSP, Certified Information Systems Professional. The CISSP credential requires at least five years of full-time professional experience in two or more of the domains addressed by the credential. Individuals who have no experience can begin by the process of becoming an Associate of the International Information Systems Security Certification Consortium, Inc. (ISC2). After one year of cumulative experience an individual can progress to the SSCP (Systems Security Certified Practictioner) credential.[25]

To become an Associate or obtain one of the credentials, an individual must pass either of the CISSP or SSCP examinations. These examinations cover a range of domains that are determined by job studies that look at what people in the field do. The domains include access control, telecommunications and network security, cryptography, business continuity and disaster recovery planning, security architecture and design, and physical security. The domains are

[25] "Steps for Certification," https://www.isc2.org/steps-for-certification.aspx. Accessed January 3, 2012.

periodically updated. For 2012, for example, a new topic under security architecture and design is distributed systems (e.g., cloud computing.)

Course enrollment that covers the domains addressed in the CISSP and SSCP examinations is available through community colleges. For example, an individual who received a Certificate in Information Technology - Networking Specialist - Network Security Professional or Certificate in Information Technology - Networking Specialist - Information Assurance would take courses that addressed the examination domains.

Figure 4. Information Security Examination Domains and Related Community College Offerings

Domain	Course
Access controls - Methods to specify what users are permitted to do, which resources they are allowed to access, and what operations they are able to perform	ITIA-1200 - Introduction to Information Systems Security
Security operations and administration - Identification of information assets, documentation required for implementation of policies to ensure confidentiality, integrity, and availability.	ITIA-1300 - Information Security Safeguards ITIA-1400 - Building an Information Protection Program
Monitoring and analysis - Methods of identifying security events, ability to determine if system operation complies with policies and procedures.	ITIA-2300 - Information Systems Threat Assessment
Risk, response, and recovery - Identification, measurement, and control of loss associated with adverse events. - Business and disaster recovery plans, techniques and concepts.	ITIA-2700 - Computer Forensics
Cryptography - Methods to manage and modify information to ensure integrity, confidentiality, authenticity, and non-repudication. - Digital signatures, public key infrastructure and certification	ITIA-2600 - Principles of Cryptography
Networks and Communication - Network structure, transmission methods, transport formats, and security measures.	ITNT -1500 - Principles of Networking
Malicious code and activity - Understand the concepts of malicious and mobile code, types of malicious code threats, how malicious code is introduced, and protection and recovery methods.	

Source: Systems Security Certified Practitioner Candidate Information Bulletin (effective 2/1/2012); Catalog 2011-2012, Macomb Community College

The close relationship between the examination domains and course titles suggests students who complete the coursework should be well prepared for the examinations. Data about pass rates would help students determine how well the courses do in fact prepare students.

While the CISSP credential is the one most often cited in Michigan cybersecurity job postings, other credentials cited are Certified Ethical Hacker (CEH), Cicso Certified Network Associate (CCNA), Certified Information Security Manager (CISM), and Certified Information System Auditor (CISA.)

Cybersecurity focused employers. Michigan is home to or one of several locations for employers which provide software and services that help organizations meet their cybersecurity challenge, producing products and services that organizations all across the country buy. These employers require both workers who have skills that are specific to cybersecurity as well as skills that are broadly used in the information technology sector.

Cybersecurity-focused employers can be anywhere. This fact was brought home by one employer that advertised for a particular set of skills and indicated the employer would be equally satisfied by having the individual work at the firm's Massachusetts or Michigan locations.

Skills sought included:

- Scripting language experience: Perl, Python, PHP, and Bash
- Familiarity with TCP/IP, SMTP, HTTP, and SSL protocols.
- Skill in the "C" and Java programming languages.

Again, this list shows that cybersecurity firms want workers who have "dual purpose" skills, skills that could be put to work both in and out of the cybersecurity world.

Security clearances. The cybersecurity challenge is a high priority for the federal government. The challenge takes two forms. One is to defend the cyberborder using the best available tools. The second is to increase the government's capacity to defend cyberspace.

The focus of this activity is the national defense and intelligence communities. The workforce dedicated to meeting this challenge includes individuals in federal agencies and in contractors doing work for those agencies.

Those who work in the national defense and intelligence communities doing cybersecurity work typically hold national security clearances. This "credential" creates a separate job market within the cybersecurity job market. In the national security sector, a government security clearance is a must. In the civilian sector, it is unknown.

Not surprisingly, this federal government-focused workforce has concentrated around Washington, DC. Only two of twenty network security openings in Michigan we examined said that candidates with a current or recent federal security clearance were preferred or required. In contrast, only two out of ten in Fairfax County, VA, just outside Washington, DC, did not require or prefer candidates with current or recent security clearances.

The concentration of the government cybersecurity labor market around Washington, DC reflects both wanting to be proximate to the customer as well as agglomeration effects. The agglomeration effect reflects the tendency for niches of economic activity to become concentrated in particular geographic areas. The concentration of the auto industry in Michigan is an example of how agglomeration effects lead to particular industries becoming geographically concentrated.

Agglomeration creates a broad and deep labor market for particular skills. However, as the discussion of the supply side of the cybersecurity market noted, much of the labor demand from firms that focus on cybersecurity is not for skills specific to that sector but for more general skills (computer language familiarity and experience; web site development.) However, the requirement for security clearances puts a fence around the national security sector.

One source of workers who have the requisite security clearances is individuals who separate from the armed forces. A Michigander who acquires both a security clearance and network security skills while serving in the armed forces and who then separates from the armed forces would find both attributes valued in the Washington labor market.

Focusing on Michigan residents who separate from the armed forces could be the basis for more national security-related projects taking place in Michigan. Two strategies to increase the importance of Michigan to national security-related cybersecurity are:

1. Encourage organizations with Washington and Michigan locations that do national security-related work to enter the cybersecurity space

2. "Michigan champions," following the Barracuda Networks model (see Figure 5). The latter strategy looks to people who know Michigan and who are decisionmakers to take the leap and open up an outpost in Michigan to tap an additional labor market.

Figure 5: The Barracuda Networks Example

Barracuda Networks provides tools that help users manage the Internet security challenge. These include spam and virus firewalls and web filters, tools to keep the "bad guys" away from the user's computer resources. Barracuda emphasizes the ease with which its products can be put to work, requiring no special expertise from users and its ability to be up-and-running in 15 minutes.[1]

It is a classic Silicon Valley company, headquartered in Campbell, CA, a short drive up I-880 to the San Jose airport, the Grand Central Station of the northern California IT industry. The company was founded by Dean Drako, a graduate of the University of Michigan's engineering school.

Given Drako's Michigan ties, it is not surprising that Barracuda decided to open a Michigan office, something it did in 2007, within five years of its founding. Drako knew this: Michigan's colleges and universities produce quality graduates. Many would want to stay in Michigan if they found jobs that used their skills. He also knew that a start up IT company in Silicon Valley faced ferocious competition for workers, with constant poaching of each other's workers.[1]

Drako saw a Michigan office as part of the solution for his problem. It allowed tapping a new labor pool. It would also be a less frenetic environment, increasing the chances that workers would stay longer.

As of mid-2011, Barracuda Networks employed 100 workers in Michigan. They staff an engineering center that helps Barracuda develop products and also a customer support center that helps Barracuda maintain its 24/7 commitment to its customers.

Barracuda's presence in Michigan is the result of having a "Michigan champion" in a key decisionmaking role -- someone who has been in Michigan, who knows Michigan, and when it is time to make a decision about where to locate, chooses Michigan. If Barracuda Networks did not have a Michigan champion, its first office outside Silicon Valley might have been in Champaign-Urbana, IL or Boston.

Specialized Training and Certification. The federal government has taken steps to promote training that will help form the workforce required to meet information security challenges.

The National Security Agency and Department of Homeland Security jointly sponsor the designation of National Centers of Academic Excellence in Information Assurance Education (CAE/IAE) and Center for Academic Excellence-Research (CAE-R.) While the designation does not bring direct funds to institutions, it does allow students to apply for Department of Defense Information Assurance Scholarships and the Federal Cyber Service Scholarship for Service.[26]

[26] "National Centers of Academic Excellence," http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml. Accessed December 23, 2011.

Five educational institutions in Michigan are among the 164 which have achieved designation as a National Center (Davenport University, Eastern Michigan University, Ferris State, University of Detroit, and Walsh College).[27]

Two-year institutions can now participate as well, designated as National Centers of Academic Excellence in Information Assurance - 2 year (CAE2Y). Two cohorts of two-year institutions have received the CAE2Y designation, one in 2010 and the second in 2011.[28] Five of the twelve are in Maryland. None are in Michigan. Those in the Midwest are Owens Community College, across the Michigan border in northwest Ohio, Moraine Valley Community College in Illinois, and Inver Hills Community College in Minnesota.

In order to be designated, CAE institutions have shown that their course offerings map to training standards established by the Committee on National Security Systems (http://www.cnss.gov/). Evaluation of applications relies on a points system that addresses six criteria: information assurance (IA) partnerships, IA student development, IA as a multidisciplinary subject, IA outreach, IA faculty, and the institution's own practice of IA.

Having one or more two-year institutions that have the CAE2Y designation would broaden Michigan's ability to train individuals who can show that they have the skills appropriate for the cybersecurity workforce, particularly for opportunities working for the federal government or federal contractors. However, because the CAE2Y category is new, there is no evidence to show whether those who complete programs at these institutions will be able to make a better labor market match than those who complete similar coursework at institutions that do not have the CAE2Y designation.

3. Border Security

As in the case of cybersecurity, there are two components of the border security workforce in Michigan: existing Michigan employers with border security compliance obligations, and public sector law enforcement including federal agencies with a presence in Michigan. Both groups recruit nationally, but improvements to the relevant skills and certifications of the southeastern Michigan workforce make local hiring attractive.

Employers already in Michigan. Following the September 2001 terrorist attacks on the United States, U.S. Customs established the Customs-Trade Partnership Against Terrorism (C-TPAT).[29] Participants in the C-TPAT program agree to undertake at their own expense certain security measures to ensure that their shipments are not tampered with or infiltrated by unauthorized individuals. Its primary purpose is countering terrorist efforts to use legitimate cross-border

[27] "Centers of Academic Excellence - Institutions," http://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml. Accessed December 23, 2011.
[28] "CAE, CAE2Y, and CAE-R," http://www.cyberwatchcenter.org/index.php?option=com_content&view=article&id=67&Itemid=166. Accessed December 23, 2011.
[29] For more information on this program, see http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/

commercial traffic as a cover for attacks or illicit activities. The Government of Canada established a similar program in 1995 called Partners in Protection.[30] Customs officials of the governments of the United States, Canada and Mexico linked C-TPAT certification and validation to similar Canadian and Mexican trusted shipper programs as part of an initiative named Free And Secure Trade, or FAST, in 2002.[31]

Participation in these programs requires application, certification by customs officials, and annual validation of regular reporting by the firm on its ongoing security measures. For C-TPAT, companies must take action to secure their operations, facilities and links to other companies as well as collect data and maintain records available for inspection by U.S. Customs and Border Protection (CBP). The criteria or guidelines encompass the following areas: Business Partner Requirements, Procedural Security, Physical Security, Personnel Security, Education and Training, Access Controls, Manifest Procedures, Information Security, and Conveyance Security. (A short description of the compliance requirements is included in Figure 6). U.S. Customs and Border Protection assigns an individual C-TPAT Supply Chain Security Specialist (SCSS) to work with firms applying to participate, and regular validation emphasizes a review of company self-assessments, rather than audits.

In order to maintain status in the C-TPAT program, companies must have personnel trained to ensure and document compliance with security requirements. This is particularly important for firms in supply chain relationships, since the loss of certification as a C-TPAT member can jeopardize the C-TPAT status of all of the other members of the supply chain, with consequent loss of business. Smaller firms have relied on security compliance services provided by customs brokers and freight forwarders, but many firms seek to perform these functions in-house for security reasons.

There are roughly 10,000 firms participating in the C-TPAT program, including the vast majority of firms working in the automotive sector. The Department of Homeland Security is working to expand the number of participating firms to 40,000 over the next five to seven years, doing so with a small staff of 200 C-TPAT Supply Chain Security Specialists.[32] In addition, the governments of Canada and the United States.

[30] Details available from the Government of Canada here: http://www.cbsa.gc.ca/security-securite/pip-pep/menu-eng.html

[31] A brief description of the program is available here: http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/fast/us_mexico/fast_fact.ctt/fast_fact.pdf

[32] Former U.S. Customs Commissioner Alan Bersin made this announcement in April, 2011. Available here: http://www.c-tpat.com/ctpat-blog/files/82717b862b3a9cf9aa0af3dc48bea94f-3.html

Figure 6: C-TPAT Business Partner Requirements[33]

Importers must have written and verifiable processes for the selection of business partners including manufacturers, product suppliers and vendors.

Security procedures
For those business partners eligible for C-TPAT certification (carriers, ports, terminals, brokers, consolidators, etc.) the importer must have documentation (e.g., C-TPAT certificate, SVI number, etc.) indicating whether these business partners are or are not C-TPAT certified.
For those business partners not eligible for C-TPAT certification, importers must require their business partners to demonstrate that they are meeting C-TPAT security criteria via written/electronic confirmation (e.g., contractual obligations; via a letter from a senior business partner officer attesting to compliance; a written statement from the business partner demonstrating their compliance with C-TPAT security criteria or an equivalent WCO accredited security program administered by a foreign customs authority; or, by providing a completed importer security questionnaire).Based upon a documented risk assessment process, non-C-TPAT eligible business partners must be subject to verification of compliance with C-TPAT security criteria by the importer.

Point of Origin
Importers must ensure business partners develop security processes and procedures consistent with the C-TPAT security criteria to enhance the integrity of the shipment at point of origin. Periodic reviews of business partners' processes and facilities should be conducted based on risk, and should maintain the security standards required by the importer.

Participation / Certification in Foreign Customs Administrations Supply Chain Security Programs
Current or prospective business partners who have obtained a certification in a supply chain security program being administered by foreign Customs Administration should be required to indicate their status of participation to the importer.

Other Internal criteria for selection
Internal requirements, such as financial soundness, capability of meeting contractual security requirements, and the ability to identify and correct security deficiencies as needed, should be addressed by the importer. Internal requirements should be assessed against a risk-based process as determined by an internal management team.

have begun negotiations on simplifying compliance obligations under C-TPAT that they hope will result in expanded participation by firms.[34] These ambitious plans suggest that the demand for C-TPAT compliance support skills will grow dramatically in the coming years

Although southeast Michigan is a major hub of C-TPAT activity due to the presence of the automotive industry and the fact that C-TPAT was introduced for U.S.-Canadian trade before it

[33] Excerpted from information provided by CBP at http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/security_criteria/criteria_importers/ctpat_importer_criteria.xml

[34] See *The United States –Canada Beyond the Border: Action Plan* (December 2011) Available online here: http://www.dhs.gov/xlibrary/assets/wh/us-canada-btb-action-plan.pdf

applied to trade with many other countries, the C-TPAT program is available for shipments around the world with an increasing number of U.S. trading partners. The growth in the C-TPAT program and the presence of experienced professionals in southeast Michigan adds to the attractiveness of the region for global logistics management. The development of training in C-TPAT procedures and compliance, building on available resources such as the U.S. CBP Supply Chain Security Best Practices Catalog[35] and drawing on the expertise of local professionals as instructors would enhance the capacity of southeast Michigan to meet the needs of global business and secure supply chains.

The U.S. government's trusted shipper program, C-TPAT, places requirements on participating firms that have changed the nature of several job classifications in terms of the skills required. As examples, three areas are profiled below: human resources, logistics, and facility security and maintenance.

Human Resources: C-TPAT rules state that human resources staff must enforce policies and practices that ensure that prospective hires, current employees, and contractors meet security standards:

> "Processes must be in place to screen prospective employees and to periodically check current employees. Pre-Employment Verification: application information, such as employment history and references must be verified prior to employment. Background checks / investigations: consistent with foreign, federal, state, and local regulations, background checks and investigations should be conducted for prospective employees. Once employed, periodic checks and reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position. Personnel Termination Procedures: Companies must have procedures in place to remove identification, facility, and system access for terminated employees."[36]

While many firms maintain systems meeting or exceeding these requirements, HR personnel at C-TPAT participating facilities must be prepared to document compliance routinely.

Logistics: C-TPAT rules state that cargo handling procedures and documentation must be in place at participating firm job-sites to ensure compliance:

> "Security measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo in the supply chain. Documentation Processing: Procedures must be in place to ensure that all information

---

[35] Available online here: http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/ctpat_members/ctpat_best_practices.ctt/ctpat_best_practices.pdf

[36] Excerpted from information provided by CBP at http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/security_criteria/criteria_importers/ctpat_importer_criteria.xml

> used in the clearing of merchandise/cargo, is legible, complete, accurate, and protected against the exchange, loss or introduction of erroneous information. Documentation control must include safeguarding computer access and information. Manifesting Procedures: To help ensure the integrity of cargo received from abroad, procedures must be in place to ensure that information received from business partners is reported accurately and in a timely manner. Shipping & Receiving: Arriving cargo should be reconciled against information on the cargo manifest. The cargo should be accurately described, and the weights, labels, marks and piece count indicated and verified. Departing cargo should be verified against purchase or delivery orders. Drivers delivering or receiving cargo must be positively identified before cargo is received or released. Cargo Discrepancies: All shortages, overages, and other significant discrepancies or anomalies must be resolved and/or investigated appropriately. Customs and/or other appropriate law enforcement agencies must be notified if illegal or suspicious activities are detected - as appropriate."[37]

These requirements add to the work that must be performed within a facility, at the loading dock, and by truckers or other transportation providers. As with human resource changes, the key is not only to make procedural changes but to document compliance thoroughly in preparation for DHS audit.

Facility Security and Maintenance: C-TPAT rules state that participating firms must establish and maintain physical access controls and heightened security awareness and training at all company facilities:

> "Physical Access Controls Access controls prevent unauthorized entry to facilities, maintain control of employees and visitors, and protect company assets. Access controls must include the positive identification of all employees, visitors, and vendors at all points of entry.
> Employees: An employee identification system must be in place for positive identification and access control purposes. Employees should only be given access to those secure areas needed for the performance of their duties. Company management or security personnel must adequately control the issuance and removal of employee, visitor and vendor identification badges. Procedures for the issuance, removal and changing of access devices (e.g. keys, key cards, etc.) must be documented. Visitors: Visitors must present photo identification for documentation purposes upon arrival. All visitors should be escorted and visibly display temporary identification. Deliveries (including mail): Proper vendor ID and/or photo identification must be presented for documentation purposes upon arrival by all vendors. Arriving packages and mail should be periodically screened before being disseminated. Challenging and Removing Unauthorized Persons: Procedures must be in place to identify, challenge and address unauthorized/unidentified persons.

[37] Information provided by CBP at http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/security_criteria/criteria_importers/ctpat_importer_criteria.xml

Security Training and Threat Awareness
A threat awareness program should be established and maintained by security personnel to recognize and foster awareness of the threat posed by terrorists at each point in the supply chain. Employees must be made aware of the procedures the company has in place to address a situation and how to report it. Additional training should be provided to employees in the shipping and receiving areas, as well as those receiving and opening mail. Additionally, specific training should be offered to assist employees in maintaining cargo integrity, recognizing internal conspiracies, and protecting access controls. These programs should offer incentives for active employee participation. Physical Security: Cargo handling and storage facilities in domestic and foreign locations must have physical barriers and deterrents that guard against unauthorized access. Importers should incorporate the following C-TPAT physical security criteria throughout their supply chains as applicable. Fencing: Perimeter fencing should enclose the areas around cargo handling and storage facilities. Interior fencing within a cargo handling structure should be used to segregate domestic, international, high value, and hazardous cargo. All fencing must be regularly inspected for integrity and damage. Gates and Gate Houses: Gates through which vehicles and/or personnel enter or exit must be manned and/or monitored. The number of gates should be kept to the minimum necessary for proper access and safety. Parking: Private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas. Building Structure: Buildings must be constructed of materials that resist unlawful entry. The integrity of structures must be maintained by periodic inspection and repair. Locking Devices and Key Controls: All external and internal windows, gates and fences must be secured with locking devices. Management or security personnel must control the issuance of all locks and keys. Lighting: Adequate lighting must be provided inside and outside the facility including the following areas: entrances and exits, cargo handling and storage areas, fence lines and parking areas. Alarms Systems & Video Surveillance Cameras: Alarm systems and video surveillance cameras should be utilized to monitor premises and prevent unauthorized access to cargo handling and storage areas."[38]

As evident from this excerpt, the C-TPAT requirements for security raise the standard for private security by participating firms and require that upgraded security measures be documented, verified and auditable by CBP.

In each of these areas, the risk to the firm of employees who through ignorance or negligence fail to fully comply and document compliance with C-PAT requirements is that C-TPAT designation may be withdrawn by CBP. In cases where this happens, the firm is no longer eligible to participate in C-TPAT compliant supply chains – the security breach by one firm endangers the C-TPAT record of all firms in the supply chain. This may be cause for termination of contracts and loss of business. In some cases, CBP may resolve a breach with fines and additional audits, and while firms in this circumstance may not lose existing business, the costs of additional audits and fines are not immaterial.

[38] Excerpted from information provided by CBP at http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/security_criteria/criteria_importers/ctpat_importer_criteria.xml

Michigan firms that have joined the C-TPAT program have generally adapted to the evolution of program requirements with existing staff, providing internal training to staff on compliance. However, as more companies seek to join C-TPAT (at the urging of the governments and of customers already C-TPAT compliant) we expect that there will be demand for individuals already familiar with the requirements of C-TPAT for business. This provides an opportunity to add to existing skills training programs, and should sufficient demand warrant, the establishment of a certification of C-TPAT knowledge and capability that workers were prepared to meet the needs of firms participating in, or applying to participate in this program.

Public Sector Law Enforcement. The surge in hiring by federal and local law enforcement agencies in response to the September 2001 terrorist attacks is now past, and hiring by these employers has stabilized. In the case of federal agencies, including the Border Patrol, U.S. Coast Guard, and Customs and Border Protection, recruitment for positions in southeastern Michigan is national and successful hires are trained by the employer.

Border security changes have affected the employment market for nonfederal law enforcement and public safety jobs (including fire and emergency service personnel). The United States and Canada now operate joint Integrated Border Enforcement Teams linking counterpart personnel and foster cross-border emergency response planning in border areas. Southeast Michigan law enforcement priorities such as narcotics trafficking and human smuggling also lead to interactions with border security agencies of the U.S. and Canadian governments.

For these reasons, education and training for law enforcement personnel such as that provided by the Criminal Justice Training Center at Macomb Community College could be adapted to include an orientation to border security agencies and procedures in both the United States and Canada. The proximity of the border would permit student visits to border facilities and guest presentations by border security personnel. The rising importance of interagency cooperation and coordination for public safety and law enforcement across Michigan and along the U.S.-Canadian border would give graduates with an understanding of the current border security environment a skills advantage in the employment market.

Appendix 1: Skills Inventory for Homeland Security Workforce Needs

This appendix provides the Department of Labor/ETA O*NET job profile for the job that most involves cybersecurity-related functions, **Information Security Analyst**.

Information Security Analysts
DoL/ETA O*Net code: 15-1122

Description: Plan, implement, upgrade, or monitor security measures for the protection of computer networks and information. May ensure appropriate security controls are in place that will safeguard digital files and vital electronic infrastructure. May respond to computer security breaches and viruses.

Sample of reported job titles: Information Technology Specialist, Data Security Administrator, Information Security Analyst, Information Security Officer, Computer Specialist, Information Security Specialist, Information Systems Security Analyst, Computer Security Specialist, Information Security Manager, Information Technology Security Analyst

Tasks

- Encrypt data transmissions and erect firewalls to conceal confidential information as it is being transmitted and to keep out tainted digital transfers.
- Develop plans to safeguard computer files against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs.
- Review violations of computer security procedures and discuss procedures with violators to ensure violations are not repeated.
- Monitor use of data files and regulate access to safeguard information in computer files.
- Monitor current reports of computer viruses to determine when to update virus protection systems.
- Modify computer security files to incorporate new software, correct errors, or change individual access status.
- Perform risk assessments and execute tests of data processing system to ensure functioning of data processing activities and security measures.
- Confer with users to discuss issues such as computer data access needs, security violations, and programming changes.
- Train users and promote security awareness to ensure system security and to improve server and network efficiency.
- Coordinate implementation of computer system plan with establishment personnel and outside vendors.

Technology used:

- *Authentication server software* — Akoura SmartToken; Diameter ; IBM Tivoli Identity Management TIM; Remote authentication dial-in user service RADIUS software
- *Internet directory services software* — Active directory software; Berkeley Internet Domain Name BIND software; Domain name system DNS software; Network directory services software
- Network monitoring software — Cisco Systems CiscoWorks; Hewlett-Packard HP OpenView software; Quest BigBrother; Sun Microsystems NetManage
- *Network security or virtual private network VPN management software* — Intrusion prevention system IPS software; Network and system vulnerability assessment software; Network security auditing software; Snort intrusion detection technology
- *Transaction security and virus protection software* — Anti-spyware software; Honeypot; McAfee VirusScan; Stack smashing protection SSP software

Knowledge

- Computers and Electronics — Knowledge of circuit boards, processors, chips, electronic equipment, and computer hardware and software, including applications and programming.
- Telecommunications — Knowledge of transmission, broadcasting, switching, control, and operation of telecommunications systems.
- Administration and Management — Knowledge of business and management principles involved in strategic planning, resource allocation, human resources modeling, leadership technique, production methods, and coordination of people and resources.
- English Language — Knowledge of the structure and content of the English language including the meaning and spelling of words, rules of composition, and grammar.
- Education and Training — Knowledge of principles and methods for curriculum and training design, teaching and instruction for individuals and groups, and the measurement of training effects.
- Engineering and Technology — Knowledge of the practical application of engineering science and technology. This includes applying principles, techniques, procedures, and equipment to the design and production of various goods and services.
- Public Safety and Security — Knowledge of relevant equipment, policies, procedures, and strategies to promote effective local, state, or national security operations for the protection of people, data, property, and institutions.
- Communications and Media — Knowledge of media production, communication, and dissemination techniques and methods. This includes alternative ways to inform and entertain via written, oral, and visual media.
- Customer and Personal Service — Knowledge of principles and processes for providing customer and personal services. This includes customer needs assessment, meeting quality standards for services, and evaluation of customer satisfaction.

Skills

- Critical Thinking — Using logic and reasoning to identify the strengths and weaknesses of alternative solutions, conclusions or approaches to problems.
- Reading Comprehension — Understanding written sentences and paragraphs in work related documents.
- Complex Problem Solving — Identifying complex problems and reviewing related information to develop and evaluate options and implement solutions.
- Speaking — Talking to others to convey information effectively.
- Active Listening — Giving full attention to what other people are saying, taking time to understand the points being made, asking questions as appropriate, and not interrupting at inappropriate times.
- Writing — Communicating effectively in writing as appropriate for the needs of the audience.
- Judgment and Decision Making — Considering the relative costs and benefits of potential actions to choose the most appropriate one.
- Time Management — Managing one's own time and the time of others.
- Active Learning — Understanding the implications of new information for both current and future problem-solving and decision-making.
- Monitoring — Monitoring/Assessing performance of yourself, other individuals, or organizations to make improvements or take corrective action.

Education

Education Level Required	Percentage respondents
Some college, no degree	11
Bachelor's degree	65
Master's degree	23

Labor Market Information

Median wages , Michigan (2010): $34.28/hour; $71,300/year
(Data aggregated across three occupations: Information Security Analyst; Web developer; Computer network architect.

Employment outlook (national, 2008-2018): Much faster than average growth (20%+)

Appendix 2: About the Authors

Christopher Ford

Christopher A. Ford is a Senior Fellow at Hudson Institute, where he directs the Center for Technology and Global Security. His areas of expertise include cyber-security; arms control; intelligence oversight, law and policy; nuclear weapons; space security; cyber-warfare; and counter-terrorism.

Dr. Ford served until September 2008 as United States Special Representative for Nuclear Nonproliferation, and prior to that as Principal Deputy Assistant Secretary of State responsible for arms control, nonproliferation, and disarmament verification and compliance policy. Prior to joining the Bush Administration, Dr. Ford served as Minority Counsel and then General Counsel to the U.S. Senate Select Committee on Intelligence (SSCI) in the wake of the September 2001 terrorist attacks. His previous service on various Senate committee staffs included periods as Staff Director and Chief Counsel to the Permanent Subcommittee on Investigations, Chief Investigative Counsel to the Governmental Affairs Committee, national security advisor to Senator Susan Collins (R-ME), and an investigative lawyer for the investigation led by Senator Fred Thompson (R-TN) into campaign finance abuses during the 1996 presidential election campaign. Dr. Ford also served briefly as Assistant Counsel to the Intelligence Oversight Board at the White House in 1996. He is also an intelligence officer in the U.S. Navy Reserve, holding the rank of Lieutenant Commander, as well as an ordained chaplain in the Zen Peacemaker Order.

Dr. Ford is the author of *The Mind of Empire: China's History and Modern Foreign Relations* (University Press of Kentucky, 2010), as well as *The Admirals' Advantage: U.S. Navy Operational Intelligence in World War II and the Cold War* (Naval Institute Press, 2005). He is also the author of numerous articles on topics ranging from nonproliferation and disarmament to comparative law, from Chinese strategic culture to intelligence oversight, and from Islamic international law to international legal history. He is also a contributing editor to *The New Atlantis* magazine.

Dr. Ford received his undergraduate degree summa cum laude in Government/International Relations from Harvard in 1989, his doctorate from Oxford University in 1992, and his law degree from the Yale Law School in 1995. He was the recipient of several prizes and awards for academic excellence, including the Emerson and Scharps prizes at Yale, the Bonaparte, Hoopes, and Firth prizes at Harvard. Dr. Ford was also awarded a Rhodes scholarship.

Hanns Kuttner

Hanns Kuttner is a Visiting Fellow at Hudson Institute. His expertise includes labor market research and the design of employment skills training programs matched to local needs.

Mr. Kuttner's career spans the policy and research world. During the presidency of George H.W. Bush, he was part of the White House domestic policy staff with responsibility for health and social service programs. Most recently, he was a research associate at the University of Michigan's Economic Research Initiative on the Uninsured. He has also worked for the federal agency which runs the Medicare and Medicaid programs and advised the state of Illinois on restructuring its human service programs.

He has written extensively about issues relating to Americans' health insurance status and the potential for improving the American health care system. With Gail Wilensky and Joseph Antos, he wrote, "The Obama Plan: More Regulation, Unsustainable Spending," published in Health Affairs, the policy journal of the health sphere, in September 2008. His current research projects look at alternative ways to pay physicians and health insurance decisions by small employers.

Kuttner has an A.B. from Princeton University. His graduate training was at the University of Chicago, where he received an M.A. degree from the Irving B. Harris Graduate School of Public Policy Studies.

Christopher Sands

Christopher Sands is a Senior Fellow at Hudson Institute, and will serve as the principal investigator and team leader for Hudson working with the Michigan Security Network. A native Michigander, he specializes on Canada and U.S.-Canadian relations, as well as border security and North American economic integration. Dr. Sands is also a professorial lecturer at the Johns Hopkins University School of Advanced International Studies, an adjunct professor in Government at the American University School of Public Affairs, and lectures at the Foreign Service Institute of the U.S. Department of State and for the U.S. Department of Homeland Security.

In 1993, Sands began a long association with the Center for Strategic and International Studies (CSIS) where he focused on US-Canada relations and North American integration issues, including a major study with Sidney Weintraub of *The North American Auto Industry under NAFTA* (CSIS Press, 1998).

Following the September 11, 2001 terrorist attacks on the United States, Sands took part in a project at CSIS to identify priority action areas in addressing terrorism. This effort produced the book, *To Prevail: An American Strategy for the Campaign Against Terrorism* (edited by Kurt M. Campbell and Michele A. Flournoy. CSIS Press, 2001). Sands chapter identified the U.S.

northern border with Canada as a source of vulnerability and promise, given the high degree of bilateral trust and historic cooperation which would make rapid improvements in border security feasible.

From 2002 until 2007, Sands directed the CSIS Smart Border North Working Group to focus research on security threats, track changes in U.S. policies regarding the border, and develop recommendations for policymakers in both the United States and Canada. The CSIS Smart Border North Working Group also sponsored a series of Congressional Staff Study Tours of border facilities enabling first-hand assessments of program implementation. Tours were conducted of border facilities at Detroit-Windsor, Port Huron-Sarnia, Buffalo-Fort Erie, Niagara Falls, Lewiston-Queenston, and Champlain-St. Bernard La Colle.

From 2003 to 2006, Sands was the research director of the Quebec Border Security Initiative at CSIS, an effort to study state-provincial cooperation in homeland security, critical infrastructure protection, law enforcement cooperation, and coordination with federal efforts to improve border security and counter terrorism.

In 2005 the George W. Bush administration launched the Security and Prosperity Partnership of North America at a summit in Waco, Texas attended by Canadian Prime Minister Paul Martin and Mexican President Vicente Fox. Dr. Sands tracked the activity of its 20 trilateral working groups on coordinating inspection and regulation in areas of security and economic policy among the three countries as a member of the Advisory Committee to the U.S. Section, North American Competitiveness Council from 2006 to 2009, a business advisory panel contributing to the SPP process. Dr. Sands was the co-author (with Greg Anderson) of the Hudson White Paper, *Negotiating North America: The Security and Prosperity Partnership* (Hudson Institute, 2007).

In 2008, Dr. Sands was commissioned by the Metropolitan Policy Program of the Brookings Institution and the Canadian International Council to study northern border security. Published in 2009, *Toward a New Frontier: Improving the U.S.-Canadian Border* was launched in Buffalo, Toronto, Detroit and Chicago and helped to lay the groundwork for the northern border strategy developed by U.S. Customs Commissioner Alan Bersin and the February 4, 2010 launch of the U.S.-Canada Beyond the Border Working Group.

Dr. Sands holds a B.A. in political science from Macalester College in St. Paul, Minnesota, and an M.A. and Ph.D. in Canadian studies and international economics from the Paul H. Nitze School of Advanced International Studies at the Johns Hopkins University.

Tevi Troy

Tevi Troy is a Senior Fellow at Hudson Institute. His expertise includes bio-defense issues and medical emergency preparedness and response.

On August 3, 2007, he was unanimously confirmed by the U.S. Senate as the Deputy Secretary of the U.S. Department of Health and Human Services. As Deputy Secretary, Dr. Troy was the chief operating officer of the largest civilian department in the federal government, with a budget of $716 billion and over 67,000 employees. In that position, he oversaw all operations, including Medicare, Medicaid, public health, medical research, food and drug safety, welfare, child and family services, disease prevention, and mental health services. He served as the regulatory Policy Officer for HHS, overseeing the development and approval of all HHS regulations and significant guidance. In addition, he led a number of initiatives at HHS, including implementing the President's Management Agenda, combating bio-terrorism, and public health emergency preparedness. He also sponsored a series of key conferences on improving HHS' role with respect to innovation in the pharmaceutical, biomedical, and medical device industries. Dr. Troy has led U.S. government delegations to Asia, the Middle East, Europe, North America, and Africa.

Dr. Troy has extensive White House experience, having served in multiple high-level positions over a five-year period, culminating in his service as Deputy Assistant and Acting Assistant to the President for Domestic Policy, where he ran the Domestic Policy Council and was the White House's lead adviser on health care, labor, education, transportation, immigration, crime, veterans and welfare. At the White House, Dr. Troy specialized in crisis management, creating intra-governmental consensus, and all aspects of policy development, including strategy, outreach and coalition building. Dr. Troy spearheaded the White House's American Competitiveness Initiative, featured in the 2007 State of the Union Address. He also served as Special Assistant to the President and Deputy Cabinet Secretary.

Before coming to the White House, Dr. Troy served as the Deputy Assistant Secretary for Policy at the Department of Labor, where he was the Department's lead regulatory strategist. At Labor, Dr. Troy crafted the Department's new ergonomics policy, as well as plans for a compliance assistance strategy for the Department's regulatory and enforcement arms.

Dr. Troy has held high-level positions on Capitol Hill as well. From 1998 to 2000, Dr. Troy served as the Policy Director for Senator John Ashcroft. From 1996 to 1998, Troy was Senior Domestic Policy Adviser and later Domestic Policy Director for the House Policy Committee, chaired by Christopher Cox. Dr. Troy has also been a Research Fellow at the Hudson Institute and a Researcher at the American Enterprise Institute.

Troy has a B.S. in Industrial and Labor Relations from Cornell University and an M.A and Ph.D. in American Civilization from the University of Texas at Austin.

Dr. Troy is the author of *Intellectuals and the American Presidency: Philosophers, Jesters, or Technicians* (Lanham: Rowman & Littlefield, 2002), as well as numerous newspaper and magazines articles. He is a regular contributor for *National Review Online*, and appears frequently on TV and radio.

John Walters

As Chief Operating Officer and Executive Vice President, John Walters oversees the Institute's operations, including staff and research management. From December 2001 to January 2009, he was director of the White House Office of National Drug Control Policy (ONDCP) and a cabinet member during the Bush Administration.

As the nation's "Drug Czar," Mr. Walters guided all aspects of federal drug policy and programs--supporting efforts that drove down teen drug use 25 percent, increased substance abuse treatment and screening in the healthcare system and dramatically dropped the availability of cocaine and methamphetamine in the U.S. He also helped build critical programs to counter narcoterrorism in Colombia, Mexico, and Afghanistan.

From 1996 until 2001 Mr. Walters served as president of the Philanthropy Roundtable, a national association of charitable foundations and individual donors. His prior government service included work at ONDCP at its founding in 1989 as chief of staff and later deputy director of supply reduction. He was assistant to the secretary and chief of staff at the U.S. Department of Education during the Reagan Administration. He also served in the Division of Education Programs at the National Endowment for the Humanities from 1982-1985.

Mr. Walters has taught political science at Michigan State University's James Madison College and at Boston College. He holds a BA from Michigan State University and a MA from the University of Toronto.

Appendix 3: About Hudson Institute

Founded by the late geo-strategist Herman Kahn in 1961, Hudson Institute is one of America's premier policy research organizations. Hudson Institute provides policy research, insights, and analysis that advance national security, protect our liberty, and draw on the power of free markets.

Hudson Institute has 50 years of proven leadership in shaping critical domestic and international policies and opinion. Hudson's team includes renowned experts, many with experience at the highest levels of government or the private sector.

With offices in Washington and New York, associates in capitals around the world, and close ties to leaders in many countries, Hudson projects into an uncertain future a compelling voice of reason on the great issues of the day.

Hudson scholars are frequently called to testify before congressional committees, and Hudson's staff produces a regular series of op-eds, white papers, policy conferences, briefings, journal articles, and studies that are widely circulated on Capitol Hill and in the Executive Branch.

Hudson research garners press coverage in a wide spectrum of high-profile global print outlets and serves as a resource for citation and background in many national and international publications. Hudson scholars appear on every major U.S. news channel, and a variety of foreign outlets, to provide their expertise on pressing issues.