Reimagining the Next Generation of Homeland Security

Booz | Allen | Hamilton

delivering results that endure

Table of Contents

A Message from Thad Allen

A remarkable sequence of events culminated 10 years ago in the creation of the US Department of Homeland Security (DHS). After President George W. Bush signed the Homeland Security Act on November 25, 2002, we had approximately 4 months to bring together 22 different departments and agencies into the new department. I recall the sense of urgency as I led a team that planned and executed the move of the Coast Guard from the US Department of Transportation to DHS. Legal deadlines pushed us together with little time for deliberate planning as to how the agencies would work together to fulfill our mission responsibilities.

Fast forward through a tumultuous decade and here we stand today, on the Department's 10th anniversary, looking back at our accomplishments but unable to resist peering ahead at the next 10 years. We are proud of the DHS' progress, but we also are keenly aware that homeland security is an evolving challenge.

We know we still need greater unity of effort.

At Booz Allen Hamilton, we've been thinking a lot about how we can help DHS realize the full dimensions of its capabilities and achieve its mission goals during its next decade. There is no single answer, no silver bullet; nevertheless, opportunity lies ahead. We are older and wiser. And 10 years of experience has provided valuable lessons to help guide the way forward.

To mark DHS' 10-year anniversary, Booz Allen is issuing a series of "viewpoints" that offer our insights into five levers the Department could pull as it looks forward to the next 10 years of securing our nation. These viewpoints are not the last word on these subjects, but instead provide starting points for meaningful discussion aimed at strengthening DHS' integrated mission capabilities and protecting our nation.

Among the new dimensions to homeland security, we will examine:

Adopting a "whole community" approach to resiliency. By re-thinking the roles and responsibility of US government, we can improve collaboration and facilitate a more unified involvement of federal, state, and local governments, businesses, community organizations, and households.

Marshaling enterprise-wide data for mission insights. DHS agencies can leverage cloud analytics to gain superior threat intelligence and predictive insight, but only by thinking of themselves as collective sources of information rather than separate parts of a larger bureaucracy.

Reimagining the border as a suite of interrelated mission functions. Modern border management requires a vision that transcends physical locations to achieve a broader, more integrated approach to managing trade and travel.

Creating a robust law enforcement network. To defeat today's highly networked, transnational criminals and terrorists, US law enforcement agencies must become a tightly knit, collaborative network that leverages their collective intelligence, analytic, and operational capabilities.

Building effective government-industry cybersecurity collaboration. Protecting the networks of our nation's critical infrastructure is a shared responsibility of government and the private sector, requiring their responsible collaboration.

DHS has made great strides and enjoyed many successes in its first decade. Booz Allen has proudly served as DHS' partner from the beginning, and we are ready to assist DHS as it continues to transform the aggregated enterprise into a unified force capable of meeting its evolving mission challenges today and into the future.

—Thad Allen, Senior Vice President, Booz Allen Hamilton

The Path Toward Resiliency

The Path Toward Resiliency

When it comes to natural and man-made disasters and emergencies, various levels of government continue to seek ways to better define and redefine the concepts of "whole community" and "resilience." While these concepts are not new, increasing numbers of state and federally declared disasters, greater damage and destruction, plus skyrocketing costs of cleanup, are placing a greater urgency on having those concepts better developed, more understood, and broadly accepted and adopted. Booz Allen Hamilton seeks to help reinforce those concepts by promoting mutually agreed upon definitions and developing mechanisms to measure progress toward helping the nation achieve greater resiliency.

The shift in real and perceived roles of government in preparedness is fueling the urgency for the responsibility of preventing, protecting, mitigating, responding to, and recovering from these events. Even though states and local jurisdictions are working hard to develop their own capabilities, a public view has emerged that the US federal government is the ultimate cavalry for rescuing devastated communities—that federal authorities will rush in and provide whatever resources are needed in order to restore normalcy. This is compounded by an escalation of approved pre- and post-disaster declarations, which have increased the costs to the federal government, and at a time when the nation can least afford it.

A re-emergence of a more holistic and inclusive approach and understanding of risk and resilience across the whole community—with shared roles and responsibilities and the commitment, effort, and resources for the five mission areas (prevention, protection, response recovery and mitigation)—will lead the nation to resiliency.

Our nation's ability to withstand and recover quickly from major disasters and emergencies is about a collective responsibility for making our communities, and ultimately the nation, more secure. When we can rebound quickly, with minimal damage and fewer losses of life, we are stronger and less vulnerable. To achieve this level of resiliency requires a unified involvement of federal, state, and local governments, businesses, community organizations, and individual households. To have everyone aiming in the same direction—toward resiliency—requires nothing short of changing a behavioral mindset. It also requires a generally accepted understanding of what "resilience" means and how it can be measured.

One of our biggest challenges is realizing the whole community approach. Communities defined by the sharing of goals, values, and institutions, are not necessarily bound by geographic boundaries or political divisions. Instead, they could well be neighborhood partnerships, advocacy groups, academia, social and community groups, and associations. Therefore, it is imperative to recognize that each community's composition, norms, and networks can be different. Another major challenge involves empowering the whole community with a tool or tools that yet exist. The right tool will illuminate cost/benefits, allow mapping to resources, provide insight to help leaders sort out priorities, and substantiate the value of resilience to further shift attitudes and culture.

Moving Toward the Whole Community

In Joplin, Missouri, after a series of devastating tornados, the actions and efforts from community leaders help demonstrate the benefits of forming the whole community ahead of when disasters strike. In May 2011, the deadliest tornado in more than

50 years touched down at suppertime in Joplin, leveling 25 percent of the city. Asphalt streets were peeled away, and large structures were shaken off their foundations while other parts of the city were leveled by 230 mph winds stretching over a mile. This was the third deadly tornado to touch down in Joplin in just 40 years.

The tragedy spurred a number of institutions to come together in a task force order to address resiliency. Mitigating the impact to local schools was the primary motivation of the task force getting together. But, their actions and results evolved into a series of return-on-investment decisions around the needs of the children and the services required to support them, their families, the businesses, and infrastructure. This activity was nothing short of a whole community and resilience in action, and demonstrated the results of optimizing the interests of all in preparation for future disasters.

The leaders made a number of recommendations based on public-private partnership, and a top-down/bottom-up approach that included structural and non-structural recommendations. The stakeholders used a disciplined process that was similar to what was outlined by a report released recently at a TISP (The Infrastructure Security Partnership) Conference called, "Infrastructure Partnership's Disaster Resilience: A National Imperative and authored by the National Academy of Sciences," for identifying risk, developing and implementing a strategy to deal with that risk, and keeping that strategy up to date.

Unfortunately, it was a string of tragedies that served as a catalyst for the community leaders coming together in Joplin. Our challenge is having leaders in the community self identify and commit time and energy to come together ahead of a disaster and to work toward planning and making decision concerning priority investments. It is a leadership responsibility to engage individuals in the imperative of building resilience. This requires no less than a behavior

shift that will only come about when leaders can demonstrate the benefits of resilience. In the near-term, a shift could be spurred on by incentives and disincentives.

Cultural Change for Behavior and Attitude Shift

Due to an inherent bias that bad things only happen to others, realigning behaviors is not insignificant and will require a generally accepted understanding of what resilience means and the consequences of rejecting resiliency.

As with other situations, cultural shifts in behavior and attitude can be often be leveraged using financial rewards and cost penalties. For instance, local governments might be aided through public-private partnerships to offer financial assistance for investments in priority situational impact areas for changing land use, such as helping identified individuals purchase hazard insurance, providing relocation costs, or the purchase of protective

boundaries. Short-term interest bearing loans could allow industries, businesses, utilities, and others to make necessary infrastructure improvements in order to accomplish expected mitigation results.

As a stakeholder, the federal government has an important role to play, offering tax credits for what is deemed proper investments. These actions should be in concert with whole communities to help empower them, bolster their impact, and provide the backing to substantiate their efforts. The US Department of Homeland Security (DHS), in particular, along with other granting agencies might want to establish criteria for its grants that require the use of the monies toward proper, approved resiliency, or to be granted to qualifying communities that have adopted resiliency as an incentive to adopt additional preparedness measures and take on more responsibilities. Disincentives can also be powerful, such as penalties and increased taxes for those who fail to purchase insurance, or when developers are found to be building with improper materials and methods. While this includes penalties, it may also portend the exclusion of grants to local jurisdictions or municipalities that are lax in enforcing resiliency tactics, and withholding certain aspects of federal disaster assistance to states that neglect resiliency obligations. Taxes might also be structured in the form of sin taxes, in which revenues from a stream of taxes are designated toward mitigation and preparedness.

Cost/Benefit Trade-offs of Resiliency: A Metrics Tool

The shift in behavior from top-down to bottom-up will require metrics for communities to: measure progress toward resiliency; understand and act accordingly on priority investments based on trade-offs; and, to gauge where other, similar jurisdictions rank in comparison for investments and payoffs toward resiliency.

Every day, we as individuals, business owners, workers, and government officials all make risk-based decisions. Whether we consciously realize it or not, we make decisions on a particular problem or activity based on whether it is in our best interest. This is the same concept as when banks and businesses calculate their return on investments. It's also how governments make decisions for allocating resources. This process is sometimes spelled out in procedures, and sometimes it is just intuitive. Either way, it is based on some value measurement that we put stock into. This is the essence of a trade-off between mitigation, protection, and preparedness, and the uncertain costs (including potential economic hardships) of clean up and recovery.

Our recommendation is to create a Resiliency Indicator—a proposed benchmark and progress-planning tool. We envision a Resiliency Indicator identifying baseline measures of preparedness with associated trade-offs showing, among other insights, the levels of investment required for degrees of resiliency. We recognize that one size does not fit all. Therefore, in addition to these standard metrics, the tool would be tailored for specific geographies, jurisdictions, and other defined situational environments.

The methodology behind a Resiliency Indicator is based on conducting a risk analysis that will identify assets, hazards, and risks, so that strategies can be formed (and policies developed) to align associated resources to the highest priority needs for a specific community. For example, areas with significant critical infrastructure assets would have different responsibilities and investments across its whole community to achieve resilience.

The tool would help map actions to cascading effects and results for various members of the community or organization for which it is designed. Each segment of the specific community would have responsibility for implementing a set of actions that have been determined to help improve resiliency based on the risk assessment and the objective for its role toward resiliency. An example could be extrapolated from a jurisdiction's business sector. Within this construct, the

driving goal would be to minimize down time and speed recovery to normalcy. In this scenario, stakeholders would assess the vulnerability of their business infrastructure, develop a measure of its value, and create strategies for how to manage risk and mitigate impacts.

The Resiliency Indicator would help to identify the investments and resources for such things as protecting assets and maintaining the vitality of the supply chain, while ensuring backups for power and access to communications. Leaders would then have insight and more confidence for deciding the investments to cover gaps considered priorities. The indicator would generate a rating based on the implementation of the investments and actions identified. Over time, by tracking mitigation and preparedness costs and action, and collecting best in class experiences, the Resiliency Indicator would be increasingly reliable and useful to decision makers. In a time when demonstrating value and benefits from investments is so critical, a high rating could be marketed by a community or organization for drawing positive attention to the community, gain the support of local and national leaders, and for possibly retaining or increasing funding for key homeland security initiatives. It is conceivable that demonstrating resiliency through the Indicator would attract more businesses and residents to a community, or more customers for business—thus boosting the economy. The benefits of this tool could be exponential. Communities often use measures or ratings like this to attract business are common across the country. For example, many of us are familiar with rankings such as "Best Places in the Country to Live" or "Cities with the Most Business Growth." Conceivably, the Indicator could create an opportunity to market a community or organization with a superlative such as "Gold Star Resiliency Ranking." Many communities promote to the business world the value of their local emergency services, the local and regional governmental support and infrastructure all as a way to promote development and growth.

At the macro view, to know one's risks, and to know the resources available to apply to those risks, begins to unravel the complexities and to help decision makers decide how best to apply scarce resources to meet cost/benefit criteria of resiliency. Ownership from the whole community will allow these difficult decisions to be made in the interests of all.

Where to Begin

Not all disasters should be complete surprises. Focusing attention on those locations prone to threats could allow us to gather important information and best practices and, hopefully, give us real examples to show the benefits of resiliency.

Today, for instance, due to rising water levels we can predict a reasonable likelihood of floods to a large swath of the nation's low-lying coastal areas. We should help these communities in segments become more resilient. It would allow us to test methods and approaches along the lines of forming whole communities and then within their jurisdictions, assess assets, invest in mitigation actions, accomplish structural and non-structural best practices, and then see how those efforts stack up against subsequent damage, cleanup, and recovery.

The data accumulated, and the relationship of the data, can be used for algorithms that will improve the Resiliency Indicator. The results of accumulated data and non-data experiences will further support needed policies and recommendations. The output could provide the coordinating principles that federal, state, and local governments to then use to incentivize whole communities to form and to adopt strategies and the required investments for resiliency for all.

Over time with inputs and outputs, plus monitoring feedback, and incorporating other communities' experiences through a variety of disasters, a patchwork of resiliency will emerge across our nation. Within each whole community, one would find a bottom-up and top-down responsibility and energy around shared, mutual interests toward resiliency.

Conclusion

Most of us recognize that what defines a secure nation is changing and evolving. During the past decade, we have been witness to devastating disasters that can strike with, and without, warning. Therefore, we all bear degrees of responsibility to assure the security of our families, communities, and the nation. It's vital to our economy, our livelihood, and no less our preservation.

To be sure, with an evolving notion of security, a parallel paradigm shift must occur that requires no less than a rebalance of attitudes, ownership, and with it—risk. The impetus for this shift, we believe, is demonstrable proof that resiliency has measurable and immeasurable payoffs. Those will be recognized in reducing harm, damage, and a faster pace for returning to normalcy. We are all stakeholders in resiliency, either directly or indirectly, and we must collectively work toward this goal. Our nation's security depends on it.

Contacts

Marko Bourne
Principal
bourne_marko@bah.com

Megan Clifford
Principal
clifford_megan@bah.com

MaryAnne McKown
Lead Associate
mckown_maryanne@bah.com

Marshaling Data for Enterprise Insights

A 10-Year Vision for the US Department of Homeland Security

Marshaling Data for Enterprise Insights

A 10-Year Vision for the US Department of Homeland Security

As owners of one of the most comprehensive data environments in the US federal system, the US Department of Homeland Security (DHS) has an asset like no other for conducting its basic mission of safeguarding America's citizens, infrastructure, and borders. The information it collects is as diverse as the missions of the many agencies and offices under its purview, ranging from the Transportation Security Administration (TSA) to the Federal Emergency Management Agency (FEMA), US Customs and Border Protection (CPB), Immigration and Customs Enforcement (ICE), the US Secret Service, and the Coast Guard.

Because the mission of DHS is so broad and all consuming, it is challenged with ushering in the kinds of changes that its data regime needs to render new insights and drive down costs. Each of the extensive data sets that DHS and its components maintain supports specific mission needs and exists under established legal and regulatory authorities. Their owners naturally strive to improve the efficiency and effectiveness of data analysis for their intended purposes. But even when users recognize the mission benefits of sharing data and conducting analysis across multiple data sets, they too often run into technical, procedural, legal, and cultural barriers to shared analysis.

These barriers are preventing DHS from realizing the full potential of the data it has as its disposal. Intelligence and law enforcement analysts searching for terrorists, and other threats, need the ability to paint a comprehensive picture that considers all kinds of data at once—such as travel and entry and exit records, evidence that ties suspected terrorists or criminals to illicit shipments of cash or contraband, or involvement of specific individuals or groups in diverse criminal activities, from weapons trafficking to cyber crime. The need to learn from and capitalize on multiple sources of data is no less urgent for DHS teams responsible for responding to emergencies, enforcing trade agreements, combating transnational criminal organizations, managing the flow of people through US borders, protecting intellectual property rights, and safeguarding America's critical infrastructure.

Over the coming years, DHS will need to master the ability to marshal its tremendous repository of data while still living up to its manifold day-to-day responsibilities. These tasks are mutually dependent—the bridge must be rebuilt while remaining open to traffic. We believe it will be easier for DHS to manage its transformation into a data-enabled enterprise if it attacks the problem from a mission perspective and taps emerging cloud-based analytics to gain new insights from the information it already has at its disposal. Through this effort, DHS can significantly elevate its role in the nation's homeland security ecosystem, position itself as a valuable and insight-driven partner to other crime enforcement agencies, and increase the efficiency of its mission-support functions.

Opening the Aperture

When Michael Chertoff became the second secretary of homeland security in 2005, one of his first priorities was to change a departmental policy of only taking two fingerprints from each person either wanting a visa to come into the country or for those traveling without visas. Chertoff reasoned that by only taking two fingerprints—one from each index finger—homeland security personnel were potentially missing scores of

latent fingerprints, or the fingerprint residue collected all over the world at crime scenes, in safehouses where terrorists plan, and even on battlefields. By expanding the information collected from travelers to 10 fingerprints, Chertoff said that the DHS significantly enhanced its capability to identify those who weren't included on watch lists but "left a little piece of themselves somewhere and some place that suggests we ought to take a closer look."[1]

Chertoff's policy change was predicated on the belief that information is power. By opening the department's aperture to collect more information, he reasoned that the department was strengthening its powers to detect bad actors before they performed bad deeds.

This premise is at the heart of all homeland security efforts, and yet, there are real and significant constraints to expanding the amount of pertinent data that each DHS entity has at its disposal. The most significant constraint is rooted in the department's origins—bringing 22 different agencies under one organization necessarily meant bringing their legacy information technology systems with them. While considerable progress has been made in improving these systems over the last 10 years, too little has been done to address the challenges of sharing data and conducting analysis across these systems. As a result, DHS has limited the usefulness of its data. Users have to mine a number of databases to find answers to problems identified at the policy level or pursue particular cases, and these efforts have historically been susceptible to redundancy and lack of coordination. In addition, the people operating at the collection end of those stovepipes have little incentive to acquire information that isn't directly relevant to their own priorities, even though it might be very important to others.

But the issue also goes to a lack of awareness that data exist in the first place. In the homeland security setting, the real power of data is not limited to helping you solve problems identified elsewhere—it's

identifying new problems so you can get ahead of them. Information sharing relies on the owner of that information to recognize its value to others, and this is very seldom the case. As a result of this shortcoming, information just stays where it is, where it has no value at all. It's as if 10 different DHS entities were each collecting a print sample from a different finger, but nobody could ever put them together because there was no mechanism for matching them up.

These organizational and other barriers are particularly problematic for homeland security leaders trying to secure the nation's borders, keep ahead of criminal organizations, enforce and facilitate trade and travel, and plan for emergency response. For instance, Customs and Border Protection has developed reasonably effective processes for physically and virtually screening cargo shipments by analyzing trade data supplied by shippers and other information on the flow of goods into and out of ports of entry. But it is difficult to link that data to information on individuals who may be involved in those shipments, the past

[1] Remarks by Michael Chertoff, www.tsa.gov/press/happenings/2007_chertoff_remarks.shtm

histories of the conveyances used in the shipments, and the money and data flows that accompany all movement of goods—whether legal or not.

Part of this difficulty stems from the fact that different agencies relying on different databases are responsible for different aspects of securing and facilitating the movement of people, goods, money, and data. A data point as plain as a phone number on a bill of lading could be associated with a known terrorist, but it won't be flagged for follow-up if nobody inside CBP understands its value and those outside of CBP remain unaware that this information is even being tracked. Only by revealing the presence of data in the first place can DHS and its partners expect its analysts at the edge to make these critical connections.

More Tooth, Less Tail

DHS faces the added challenge of evolving into a data-centric organization at a time when every cost is being scrutinized. While mission challenges remain high, the department is facing budget constraints unprecedented in its 10-year history.

As in the military, concern is growing that the "tail" of back-office functions has grown too big and unwieldy to support DHS' mission in a timely and cost-effective manner. One of the biggest complaints coming from inside the organization is that staffers have to supply the same data to five or six different entities. That level of duplication is expensive and ties up valuable resources. This spending seems particularly out of synch when analysts working at the edge of the enterprise have a limited view of the information the back-office support groups are helping to maintain.

Our view is that DHS has the opportunity to become a leaner, more productive organization in the future if it harnesses the power of the data it already collects today to support its many mission objectives. In 10 years' time, we see DHS components thinking of themselves as collective sources and sharers of information rather than separate parts of a larger bureaucracy. DHS must tap the potential of its data much in the way that retailers, banks, and healthcare providers of today are tapping every available piece of information about their customers to predict their behavior and help set strategy. Investigators, inspectors, and analysts in the field will know what kinds of data are being collected across the organization, so they know where to go to mine for information and learn more about the cases they are pursuing. Ultimately, this capability will be extended from mission data to mission-support activities to help DHS more efficiently manage its personnel, property, fixed assets, and finances.

Mining Big Data for Insights

The first step in developing this capability and transforming DHS into a data-enabled enterprise is to embrace a new method of keeping track of and accessing information—one specifically designed for big data that is distributed in a classified or law enforcement environment. The emergence of cloud computing technologies has paved the way for organizations to unlock new insights by coupling technological infrastructure with analytical tools to gain better access to all of the data they have at their disposal.

To support this new capability, DHS must have a full and working knowledge of all the types of data its many entities collect on a regular basis. As it stands now, a DHS analyst is only able to locate the information he or she needs if they know precisely where it is housed—in one database or another. But DHS' experience reveals that this is seldom the case; users move from database to database, searching for specific information that may or may not be there. If users want to ask different kinds of questions, they often have to reengineer both the databases and the analytics involved—a process that can be prohibitively long and expensive. This tends to limit both the complexity of the questions that are asked and the utility of the results.

What DHS needs to derive actionable insights from its data is to evolve toward a platform where the data can be staged for advanced analytics. Cloud-based technology solutions now avail organizations with an effective and efficient way to load, store, and access multiple data sources to enable multivariate analytics in a mission-specific setting. The evolution will systematically convert the DHS' collection of individual databases into a consolidated and connected pool of information—or "data lake"—making all of it readily accessible for all types of analysis.

With the data lake, users can easily tap all of the available data in a variety of constantly changing ways. A key feature of the data lake is that information is no longer defined strictly by its location. Specific pieces of supporting information—known as meta-data, or "data about the data"—are identified by embedded "tags" that allow for sorting and identification. In the shipping container example illustrated above, the user could find the phone number listed on the bill of lading simply by searching for it, regardless of which DHS agency captured the information. The process of tagging information is not new—it is commonly done within specific datasets or databases. What is new is using the cloud in combination with the technique to make it available to a wide array of users. This is an important distinction, as an important advantage of the data lake is there is no need to build, tear down, and rebuild rigid data structures.

The most transformative aspect of a cloud analytics reference architecture that incorporates a data lake is that users do not need to have the possible answers in mind when they ask questions. Instead, they can let the data talk to them. The ability to make complex inquiries, easily switching in and out any number of variables, allows users to look for patterns, and then follow them wherever they may lead. This is particularly important in predictive analytics, when people may not know exactly what they are seeking. This capability strengthens the power of inquiry by empowering data to help reveal new or broader questions and correlations, expanding insight into scenarios and challenges. Importantly, a data lake also helps draw from unstructured and streaming data, which exist in forms that cannot be directly placed in structured databases and data sets.

Our prior work with another intelligence-driven organization shows that a data lake can be employed even when classified information is at issue by putting appropriate levels of security and authorization in place. The solution called for predictive analytics to use existing data to forecast potential events and detect anomalies in order to extract potentially significant information and patterns. Our design focused on keeping transactional-based queries in the current relational databases, while doing the "heavy lifting" in the cloud and outputting the results into relational data stores for quick access.

The new cloud solution provided immediate and striking improvements across the increasing volume of structured and unstructured data using aggressive indexing techniques, on-demand analytics, and pre-computed results for common analytics. By combining sophistication with scalability, the solution helped move the organization from a situation in which analysts stitched together sparse bits of data to a platform for distilling real-time, actionable information from the full aggregation of data.

Many such opportunities now exist in Homeland Security. For example, the National Cybersecurity and Communications Integration Center (NCCIC) faces the challenge of making full use of the numerous data feeds it receives from a variety of government, private-sector, and other organizations. Because much of the data is unstructured, or resides in discrete data sets that are difficult to connect, NCCIC may get only a partial, delayed picture of cyber and communications incidents. Booz Allen Hamilton's Cloud-based Services would enable NCCIC to consolidate all its available data—of every type, from all sources—and then automatically search through its entirety for important correlations and patterns. With this ability to put all the

pieces together and see the full picture, NCCIC could better respond to incidents in real time, and provide more accurate situational awareness to stakeholders.

In another example, Cloud-based Services would enable DHS and the Department of Justice (DOJ) to integrate the intelligence they gather in their shared Southwest border mission. Currently, the critical ability of the two agencies to gain a common operating picture is hampered not just by the wide range of structured and unstructured data collected, but also by the various restrictions, authorities and security issues around storing, managing and accessing that data. Through Cloud-based Services, DHS and DOJ can create a common operating picture while maintaining the different sets of rules for the data—all in one system, rather than in many. This ultimately frees the mission operators and the IT organizations supporting them from the need for proprietary solutions, and from the resource-depleting operations and maintenance costs tied to those solutions.

Cloud-based Services would also allow DHS to break through major cost barriers with a shared data environment for the department's component agencies. Currently, agencies often share space at data centers. Cloud-based Services takes a major step forward by creating an environment in which the agencies share a common data pool, as well as reusable analytic and visualization software that taps into the pool. What occurs is a decoupling of the data from the software, substantially driving down costs and creating previously unobtainable economies of scale.

Oversight and Backing

Of course, DHS will need to maintain adequate governance of its data to help decide which information is included in the data lake and who is authorized to access it. To this end, DHS will need a dedicated team to provide this level of governance. Many commercial enterprises have turned to a chief data officer (CDO) to serve this function and increase the transparency of their data. This idea, or something like it, could serve DHS well. The CDO and their staff should not be confused with a chief information officer or chief technology officer. Where these other two functions provide general infrastructure support to the rest of the organization in a commercial setting, CDOs work much more closely with the lines of business to tap data for specific objectives.

Financial services firms, among the first to create such a position, have turned to CDOs to drive their data management strategy and establish a data governance structure to determine who owns and manages the information. Their experiences could be particularly instructive in a homeland security setting, given the vast array of data they collect, as well as their need to safeguard sensitive information.

Indeed, this last consideration has proved problematic for DHS in the past; it's easier to protect information when security is at stake than risk exposing it to someone without the proper authorization. A critical part of the CDO's role would be to define the parameters for data ownership and stewardship. The CDO would also help determine legal restrictions on the use of data. When certain data are combined, it can create a collision of legal authorities. On its own, one piece of information may not be classified or law enforcement sensitive, but combining that information with other data may yield insights that need to be protected for national security or prosecutorial reasons.

A strong governance function may also be influential in securing support from outside the organization. Whether the solution takes the form of a data lake or some other vehicle, it likely won't go far without a legislative mandate. The legacy structure of its seven operating components and other agencies has supported a view that information is a commodity that must be protected, and only disseminated on a need-to-know basis. The agency will also face the reality of convincing incoming political leaders to make short-term investments for long-term gains. Change

management is tough enough for private companies—it is that much more difficult for federal agencies whose senior leaders are in a state of constant flux. Even the best-laid plans can get disrupted or derailed when those who call the shots inevitably change.

Without a legislative or statutory mandate to serve as a forcing event, DHS will not likely be able to foment the degree of change that is needed—at least not at an acceptable rate. In some ways, the position DHS finds itself in now is not dissimilar to that faced by the US Treasury Department in the aftermath of the credit crisis. At the time, it was clear that the financial services industry had major gaps in trying to get its hands around all of the risks being taken with the advent of credit default swaps and other advanced financial derivatives. The Treasury Department needed financial data that was actionable and would support decision-making at the highest levels within the department.

To help fill these gaps, Congress created an Office of Financial Research (OFR) within the Treasury Department through the Wall Street Reform and Consumer Protection Act of 2010 ("Dodd-Frank"). The law created two units within OFR—a data center and a research and analysis center—to continually gather up and analyze detailed financial information collected from a variety of banks and other financial firms. One of its first steps was to issue a request for proposals on an industry utility to create and generate identification codes to help it obtain more granular data on counterparty risk, long and short positions, collateral and collateral calls, and derivative positions.

Given the complexity involved with the effort, and the reliance on private sector contributions, OFR would not have been possible were it not provided for in statute. It may be too early to judge whether OFR will be a success or not, but it does show the power of a mandate to force organizational change where the availability of information is restricted.

Conclusion: A Data-Driven Future

The political feasibility of winning such a mandate for a data-driven approach at DHS is an open question. To win support for such a mandate, it will be critical that DHS and its components present the opportunity to be more effective and cost-efficient in real terms. DHS will continue to collect and store data regardless of whether such a mandate exists. The cost of those efforts will not go away. The question is whether DHS is empowered to make better use of those resources by increasing its awareness of the information that exists. After all, you can't fight an enemy you don't know. And, creating new channels to share information only works if you know what information you have at the ready.

The enterprise insights that come from these early efforts will likely produce some quick victories and attract the necessary buy-in to build incrementally from there and start developing a data repository with actual answers—not just questions. By thinking big, acting small, and going methodically step-by-step, DHS has the capability to lead where others continue to squabble. Information is the key to this transformation. Treated as a commodity, it will continue to be stockpiled and stored away. Viewed as an asset, it will strengthen the nation's homeland security enterprise and help DHS deliver on its many far-reaching mandates.

Contacts

Suzanne Storc
Principal
storc_suzanne@bah.com

Mike Delurey
Principal
delurey_mike@bah.com

Reimagining the Border

A Functional View of Border Management

Reimagining the Border

A Functional View of Border Management

Globalization and international trade bring benefits as well as risks. To maximize the benefits of trade and travel while mitigating risks, a nation must facilitate cross-border movement of legitimate goods and people, while simultaneously enforcing trade and travel regulations and limiting the movement of illegal or dangerous things and people. However, managing these sometimes competing functions grows increasingly difficult due to the complex flows of goods, people, conveyances, data, and money across multiple territorial boundaries and jurisdictions. The existing border management infrastructure and processes struggle to keep pace with evolving demands, particularly as terrorists, criminals, other threats become more adept at exploiting cyber technologies and the maze of separate authorities and systems to avoid detection. Addressing these challenges by simply buying more sophisticated equipment or expanding the number of agents and officers is not the answer, nor is it even possible in this budget-constrained era. To maximize available resources, modern border management needs a vision that transcends physical locations and often stove-piped authorities to achieve a broader, more integrated approach to managing trade and travel. By reimagining the border as a suite of interrelated mission functions, our nation can make better use of information and modern analytical capabilities to improve border management up and down the supply chain, strengthening the individual missions of each authority and the overall economic well-being and security of the nation.

Viewing the border through the lens of the key functions of border management—facilitating trade and travel, enforcing regulations, and preserving physical and cybersecurity—gives agencies a clearer, more holistic appreciation of how goods, people, data, and conveyances flow through domains and across boundaries in the modern global environment. This view also enables a more comprehensive accounting of money flows that support trade and travel. Most importantly, the flow of data that underlays virtually every international transaction can be the core enabler to efficiently and effectively manage the mission functions of facilitation, enforcement, and security. Conveniently, this view opens the possibilities for using the vast amount of trade and travel data that already exists to both speed and secure international travel and commerce.

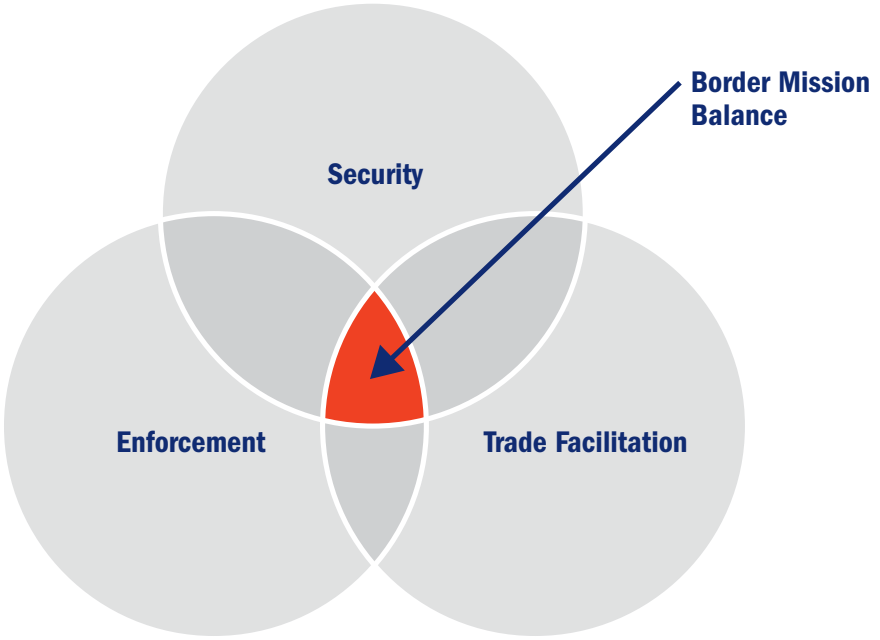
Envisioning the Future

The overall border mission is to maintain a balance among sometimes competing functional areas:

- **Enforcement** to ensure compliance with trade and immigration laws, regulations, and international agreements; collect duties; and protect health and safety
- **Security** of people, cargo, conveyances, and infrastructure to prevent the import or export of anyone or anything that could be used for nefarious purposes and to protect the international transportation infrastructure itself
- **Facilitation** of trade and travel to keep cargo and people moving to expedite commerce and enhance freedom of movement

The mission is exercised across land, maritime, air, and cyber domains, including at legal ports of entry and between them. Well-run borders are a prerequisite for vibrant border regions as they allow for efficient flow of workers, tourists, and shoppers, as well as regional social and political interaction. Any solutions

Exhibit 1 | Border Mission Balance



Source: Booz Allen Hamilton

or changes to the mission approach must be made while, at least, preserving today's mission performance.

Geographic borders define international trade and travel. Goods and people flow in and out of a nation's sovereign space through multiple domains. Nations attempt to manage those flows through international agreements, laws, and regulations bringing to bear the authorities and resources given their border enforcement agencies. In the United States, border management functions are carried out by multiple agencies within the Department of Homeland Security (DHS) as well as other parts of the federal government. Each is governed by authorities tied to its mission responsibilities and is resourced accordingly. Depending on their core missions, some work across all domains; some focus on only one. Together, these agencies strive for smooth entrance/exit of approved traffic while denying entrance/exit to unapproved traffic.

Many of the trade and travel facilitation, enforcement, and security procedures currently in place—manifests, bills of lading, passports, and visas—are modern versions of legacy practices and business rules dating to long before the information age. While these processes have been "modernized" through the application of information technology, much of that effort has focused within separate domains, procedures, or agency programs. To this point, no one has fully reimagined how trade and travel could be managed in a technologically enabled, more mobile, and highly networked world.

A functional view emphasizes three essential elements: cooperation among agencies with complementary

geographic responsibilities, missions, and authorities; more effective information sharing and operational coordination across functions, domains and modes of transportation; and application of advanced analytical techniques to enhance coordination and decision making. The result is greater unity of effort across all border functions and a better allocation of resources to focus on intelligence-based priorities.

Important precursors for this approach are already coming into place. On trade, modern customs administrations worldwide possess technical capabilities and technologies that greatly enhance their abilities to perform inspections, process import and export declarations, and collect duties and fees. For example, US Customs and Border Protection (CBP) have capabilities to perform targeting analysis and selectively make determinations on admissibility and compliance with export regulations. In addition, this capability is carried out on behalf of more than 60 US government agencies. Similarly, US Immigration and Customs Enforcement (ICE) and the Transportation Security Administration, together with the State Department and the intelligence community, are cooperating to screen passengers against watch lists as well as verify the status of legal travelers seeking to enter the country.

A reimagined view will require stakeholders from border-responsible agencies to think outside current mission and authority-imposed stovepipes. It will require that they work together and leverage opportunities to improve information sharing and operational coordination, and they adapt their own processes and resources to achieve greater unity of effort. In some cases, the evolution has begun with the implementation of "virtual border" programs and regional cooperation efforts. These programs, meant to push the notion of the physical borders out and away from the geographic boundaries of the nation, mark the beginning of the evolution towards a more information-driven border.

Advanced Analytics—From Information to Intelligence

This new way of thinking about the border encourages timely collection of data throughout the supply chain rather than primarily at the border. This sets the stage for more efficient management and decision making at the borders themselves and helps offset infrastructure and process constraints at points of entry. It also provides an overall architecture for sharing and analyzing information so that agencies with border missions have a clearer understanding at both the transactional and strategic levels of movements of goods and people. This enables agencies to be more efficient at their particular missions and promotes multi-jurisdictional cooperation.

There is an opportunity to enhance border management by making more effective use of the vast amounts of data already available on the international movement of people and commodities. For example, existing programs such as the Immigration Advisory Program (IAP), Container Security Initiative (CSI), the Customs and Trade Partnership Against Terrorism (C-TPAT), and Advanced Passenger Information System (APIS) rely on data collected well before shipments or travelers reach ports of entry to enable timely screening and targeting decisions. However, these programs focus on different aspects of the overall flow of goods and travelers; and they are based on separate authorities, jurisdictions, capabilities and competencies largely isolated within individual agencies. Viewing the various border missions as an aggregation of functions across physical and virtual domains could provide a more integrated operational picture of the total flow of people, cargo, and conveyances through all domains, thus enabling agencies to act more effectively across the total trade and travel environment.

The functional border approach enables agencies with border responsibilities to more fully exploit advanced analytical techniques and emerging "Big Data"

capabilities. All legitimate trade and travel, as well as much illicit trade and travel, generates data—financial transactions, bills of lading, purchases of airline tickets, classification of goods, flight plans, etc.—to meet normal business and regulatory requirements. Governments already collect much of that data for customs, immigration, health and safety, and security purposes. With improved information sharing and the application of sophisticated data analytics, agencies can build a more comprehensive picture of legitimate trade and travel, and then highlight anomalies that warrant deeper investigation. Advanced biometrics and other tracking and sensing technologies can indicate when and where travelers and cargo are during transit, bringing essential geographic context to the data. The vast majority of trade that is legitimate can be tracked, screened where necessary, and monitored for trade compliance, duties, and other purposes—and done so, if necessary, at the level of the individual pieces of freight. People generate similar data trails when they travel internationally, which can also be used to facilitate freedom of movement, enforce travel and immigration laws, and identify illegal intent. While privacy and civil liberties considerations must be taken into account, information needed for advanced analytics that will improve identification of illicit activities and movement is already lawfully collected and available.

Also, anomalies identified in legal trade and travel can raise red flags pointing to possible illegal activity, particularly when those anomalies occur over time. In addition, most illicit trade and travel have financial motivations and rely on criminal networks. A security strategy using data analytics to uncover illicit networks, transactions, and flows of people and property can help law enforcement agencies halt and seize dangerous goods and people as they cross geographic borders or, in some instances, well before borders are crossed. The accurate and timely analysis of information on legal movement will make it more

difficult for criminals to conceal illegal transactions in the normal flow of trade.

Much of the data needed to support the analytic foundation of the functional border approach already exists. But the data must be located, shared, appropriately protected, and analyzed. These are primarily cultural, leadership, and policy challenges—and only secondarily a technology issue—that will require components to embrace unity of effort as a strategic goal. Strengthened public-private information sharing arrangements will also be necessary to exploit data analytics, as well as measures to protect privacy and sensitive business information. Improvements in processing speed and reduced administrative costs to shippers will spur increased information sharing, as will improved cooperation among key US agencies with direct responsibilities at the border.

Conclusion

Fully adopting this approach will not require agencies to relinquish mission responsibilities or jurisdictional authorities. Rather, it will require them to relinquish the belief that they alone are responsible for certain functional activities or possess all the information and capabilities needed to achieve their mission objectives. It is recognition that all border-related mission performance across the enterprise is improved through more efficient and effective use of the vast amounts of data flowing through various agencies and systems.

At the tactical level, border agents and officers will always retain responsibility for keeping the border secure at their entry points, but those agents and officers will be supported in these efforts by information and analysis drawn from all domains and from all points in the global supply chain. The primary change under the functional approach is not to redraw organizational roles and responsibilities, but to achieve unity of effort through better information sharing and more powerful analytics. This also helps alleviate budget challenges by acting as a force multiplier because it better prioritizes where we focus and allocate limited resources.

The cause for information-supported unity of effort grows more compelling with the increasing sophistication of global threats, complexity of international networks and trade, and severe budget constraints facing our nation. DHS has no higher priority than removing barriers to information sharing and improved operational planning and execution. This will improve the overall performance of DHS and its component agencies in carrying out their inter-related homeland security mission functions, and it will support unity of effort within the department and across the homeland security enterprise.

Contacts

Rick Saunders
Vice President
saunders_richard@bah.com

Dan Dreyfus
Principal
dreyfus_dan@bah.com

Appendix 1

The following three scenarios illustrate how better utilization of information, across domains and functional areas, can improve border mission performance. The scenarios suggest a new way to think about the future of border protection. This future requires changes not just in how we use information, but how we think about information. It requires us to think about information more broadly and establishes a critical need for better collaboration across information sources. Now is the time to set a path for this future. Over the long term, this path is the only affordable option that can optimize the sustained balance between ensured security, strong trade facilitation, and effective law enforcement.

Scenario 1: Megawati Sukarnoputri travels to Chicago

Megawati Sukarnoputri, an Indonesian citizen, is a successful industrial parts manufacturer and distributer. Over the past 2 years, he has actively managed US domestic business activities and has taken several business trips to America. Mega, as his American employees call him, owns an industrial supply distribution warehouses in Baltimore, land in Idaho, and he owns a distribution business in St. Louis. Today, he's traveling independent of business activity.

Mega is traveling on a visitor visa to Chicago. He bought an airline ticket from Indonesia to Amsterdam seven days ago. Interestingly, he has a friend in Illinois who, just yesterday, bought a reverse ticket in Mega's name (Amsterdam, Chicago, back to Amsterdam). As a frequent traveler, Mega is not on the do not fly list. Beyond his travel to Chicago, there are no domestic travel purchases or other reported travel itinerary.

Within the past month, his St. Louis business just obtained licensee to transport hazardous materials. Oddly, while records show that there have been three recent hazardous waste pickups, but no reported deliveries to hazardous waste disposition centers.

Current information process and exchange regarding this scenario

A review of a traveler's information occurs upon the purchase of a ticket, when the carrier creates a Passenger Name Record (PNR). All commercial airlines are required to make their PNR systems and data available to Customs and Border Protection (CBP). The PNR is provided to CBP up to 72 hours in advance of travel, which permits CBP to conduct research and risk segmentation on all travelers including US citizens and non-US citizens. The PNR includes:

- **Full name (last name, first name, middle name if applicable)**
- **Gender**
- **Date of birth**

- **Nationality**
- **Country of residence**
- **Travel document type (normally passport)**
- **Travel document number (expiry date and country of issue for passport)**
- **[For US travelers] Address of the first night spent in the US (not required for US nationals, legal permanent residents, or alien residents of the US entering the US)**

The data is fed to CBP Automated Targeting System (ATS) and NTC-P database and targeting of passenger list is automatically evaluated. The ATS data is sent back to CBP on all passengers and flags passenger of interest (if any). When the passenger arrives in the United States, he is subject to inspection by CBP officers. Upon application for admission to the United States, this inspection begins with CBP officers scanning the traveler's entry document and performing a query of various CBP databases for exact or possible matches to existing lookouts, including those of other law enforcement agencies. The system queries the document information against the APIS manifest information previously received from the carrier and provides any enforcement information about the traveler to the officer for appropriate action.

Questions for consideration

- **Would, if assimilated, Mega's business activity information raise a flag to meet and question him upon his arrival in Chicago (all the information above would be available through the IRS and Department of Commerce. Recent activities in St. Louis might be known by local law enforcement and state and federal environmental reports)?**
- **Is it possible Mega has plans for that recently acquired toxic waste that diverge from his normal business interests?**

Case 2: Takeshi Watanabe makes a new friend

Takeshi Watanabe is a certified C-TPAT shipper. He's been shipping automotive parts (axles and brake parts for resale) for over eight years. He usually ships from Singapore to Long Beach, CA. Takeshi enjoys a comfortable life as a successful, independent Japanese businessman living on Mali. Of course, he has visions of greater business success and even greater luxuries and comforts in his future. As he obtained and maintained his C-TPAT certification, he's had no issues on any shipments (his shipments have progressively been assessed as low risk).

Four months ago, Takeshi was approached by Vladimir Petrenko with a very lucrative business proposition. Vlad, who is also interested in getting into the automotive parts business, offered to purchase Takeshi's next shipment while it was en route to the US, Vlad told Takeshi that his customer base paid top dollar and he offered cash money giving Takeshi three times his usual profit. Takeshi couldn't help but accept. Vlad later contacted Takeshi and told him the deal resulted in great success and was definitely a "win-win." Vlad suggested they do business again in the future.

Two weeks ago, Vlad called Takeshi and asked if he could add some of his goods to containers that might not be at capacity. Vlad assured Takeshi that the manifest of materials was thorough and he would take care of all the additional requirements of loading. Takeshi reviewed the manifest and found it all legal. Once again, Vlad's

financial offer was one of the best deals Takeshi's had ever seen (it even surpassed the deal he made with Vlad a few months back). While Takeshi found it somewhat troubling when Vlad suggested that Takeshi remain sole owner on the paperwork, Vlad assured him that it was only because the cost savings (limited inspection) associated with Takeshi's C-TPAT certification that could make the deal possible.

Current information process and exchange regarding this scenario

Twenty-four hours before cargo is loaded on the vessel a 10 + 2 file is sent to CBP—the following 10 data elements are required from the importer:

1. **Manufacturer (or supplier) name and address**
2. **Seller (or owner) name and address**
3. **Buyer (or owner) name and address**
4. **Ship-to name and address**
5. **Container stuffing location**
6. **Consolidator (stuffer) name and address**
7. **Importer of record number/foreign trade zone applicant identification number**
8. **Consignee number(s)**
9. **Country of origin**
10. **Commodity Harmonized Tariff Schedule number**

From the carrier, two data elements are required:

1. **Vessel stow plan**
2. **Container status messages**

Prior to departure and also during transit ATS and NTC-C targeting will provide and update a score. The score is based upon threat criteria. If the score indicates a national security threat, a do not load order is sent. Otherwise a load order is sent. The threat profile is updated as more information is received during transit.

Questions for consideration

- **How could import agents and officers become aware of this transaction?**
- **Is it possible to automate historical container weights with current imports on frequent shippers? Do current data searches compare invoice paperwork with reported weights?**
- **Would non-intrusive inspection capabilities be applicable in this case?**
- **Is it possible Vladimir put something in those containers not wanted within US borders?**

Case 3: Marcos Castro takes a drive to San Ysidro

Marcos is a recent hire working for Maquia Trucking. He's been hired to haul supplies through the US border. Two days ago, Marcos was on holiday traveling to Laredo. Prior to joining Maquia, Marco was a gardner for a very wealthy Mexican businessman who is under DEA investigation due to his ties to known members of the Sinaloa drug cartel.

He was stopped at the border and denied entry because his sentry card had expired. Today, Marco was on duty driving a load of textiles to San Ysidro. When stopped at the border, Marco presents a current FAST card. The border agent lets Marco cross.

Current information process and exchange regarding this scenario

Two hours before entry into the US, the trucker is required to submit a manifest (which is transmitted for NTCC clearance):

- **Crew/passenger data**
- **Shipment/cargo data**
- **Conveyance information**
- **Equipment data**

When the trucker arrives, he undergoes a review with the CBP officer. The CBP officer provides clearance upon his onsite review and NTCC clearance. He as the following courses of action:

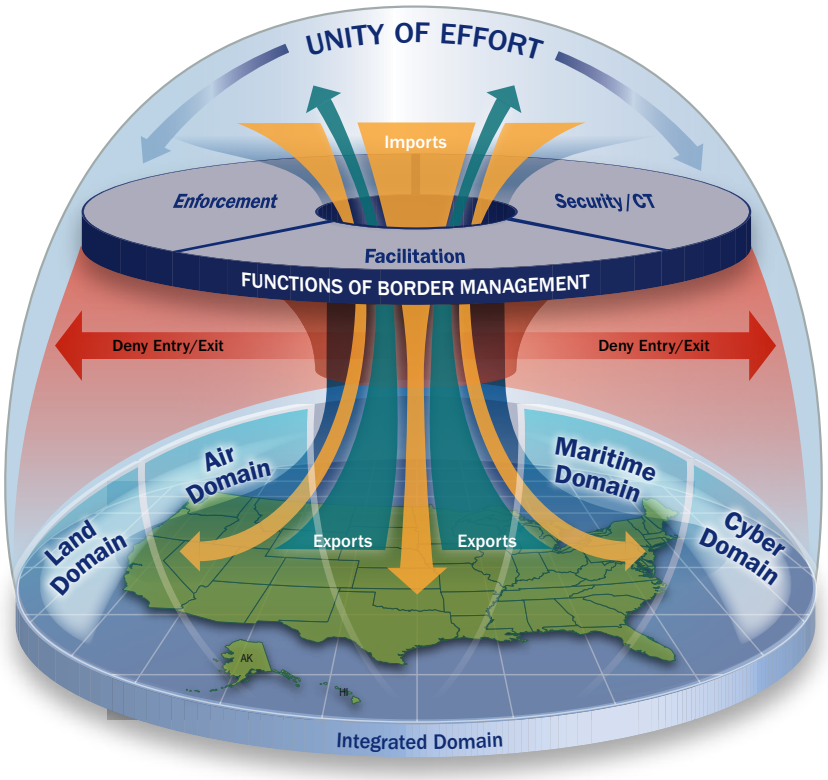
- **Agent lets truck through, or**
- **Agent sends to secondary inspection with options of:**
  - **Strip the vehicle**
  - **100 percent tear-down**
  - **Disassemble**
  - **Let go**

Questions for consideration

- **Could Marco's recent travel activities be made available to the border agent at San Ysidro?**
- **Could known recent and current employees of his previous employer be part of DEA files and available to the border agent?**
- **Is that truck really just full of textiles?**

Reimagining the Border: Functional Border Management

Reimagining the Border as a Balanced Suite of Interrelated Mission Functions. Modern border management requires a vision that transcends physical locations and often stove-piped authorities to achieve a broader, more integrated approach to managing trade and travel. By viewing the border through the lens of the key functions of border management, we can make better use of advanced analytics to improve border management and strengthen the individual missions of each component authority, as well as the overall security of the nation.



Security/Counterterrorism (CT):
Identifying and interdicting the movement of goods, people, or conveyances that have a nefarious intent or possible nefarious use

Enforcement:
Ensuring compliance with laws, regulations, and international agreements

Facilitation:
Keeping cargo and people moving while ensuring compliance, security, collection of duties, and maintaining officer/agent/citizen safety

Cybersecurity:
Screening, inspection, targeting, biometrics, data analysis, identity management, C4ISR, HUMINT, data and systems integrity

The Challenges: Enforcing, facilitating, and securing flows of people, goods and conveyances in and out of the United States—and the movements of money and data that support those flows; dealing with the special challenges of migrants and refugees; identifying and seizing contraband; neutralizing human trafficking; and identifying and destroying invasive species.

Trade/Cargo
- 64,483 Containers/Day
- 23.5 Million Containers/Year
- 329 Ports of Entry
- $20 Billion in Duties/Fees
- Rules and Regulations of 60+ Agencies

Travel/People
- 340 Million Travelers/Year
- 932,456 Travelers/Day
  - Pedestrians
  - Air Travelers (259,191)
  - Cruise Ship Passengers (48,000)
- 5,000 Miles of Land Border
- 9,000 Miles of Coastal/Littoral

Transport/Conveyances
- Aircraft
- Automobiles
- Pipeline
- Trucks
- Trains
- Vessels

Source: Booz Allen Hamilton

Enabling Agility in Law Enforcement

Leveraging Collective Intelligence, Analytics, and Operational Capabilities to Optimize Mission Performance

Enabling Agility in Law Enforcement

Leveraging Collective Intelligence, Analytics, and Operational Capabilities to Optimize Mission Performance

By nearly every measure, the threat from Transnational Organized Crime (TOC) grows stronger every day. The National Intelligence Council, within the Office of the Director of National Intelligence, recently estimated that TOC generates these staggering annual revenues from its criminal activities:[1]

- **Money Laundering –** US$1.3 trillion to US$3.3 trillion (2-5 percent of world GDP)
- **Narcotics Trafficking –** US$750 billion to US$1 trillion
- **Counterfeited and Pirated Products –** US$500 billion
- **Human Trafficking –** US$21 billion (2.4 million victims)
- **Credit Card Fraud –** US$10 billion to US$12 billion

Perhaps most alarming are the growing interlinkages between TOCs, terrorists, and insurgency groups. Increasingly, TOC organizations are employing terrorist-like violence to spread fear and exert influence and control, while terrorists and insurgents are using criminal activities to help fund their political violence. Insurgent networks such as Colombia's FARC and the Afghan Taliban have become so deeply involved in smuggling narcotics, kidnapping, and extortion that crime has essentially become their raison d'être. Similarly, TOCs from Mexico's Sinaloa Cartel to the D-Company gang in Pakistan have adopted terrorist tactics to intimidate law enforcement and government officials as well as rivals. Collaboration between criminal groups and anti-state organizations is also growing more common. Although the motivations of TOCs and terrorists-insurgents are decidedly different—one's primary motive is financial gain, while the other's is political power—their activities are increasingly alike. The melding of these threats across national and international borders has blurred the distinctions between national security, criminal justice, and homeland security. There are no borders in the fight against transnational criminals, terrorists, and insurgents. National security, law enforcement, and homeland security missions have become intertwined.

These converging TOC and terrorist networks threaten US national security and economic interests in multiple ways. Powerful illicit networks from South Asia to West Africa to Latin America to the Former Soviet Union are destabilizing the regions where they operate, undermining state authorities, disrupting business and trade, and fueling migration. The worldwide expansion of trafficking in drugs, weapons, and humans has spurred a concurrent rise in violence that spills onto US soil. In Mexico, the criminal cartels have become so entrenched that the Calderon Administration enlisted more than 45,000 military troops to assist police, while spending billions of dollars in domestic funding and foreign aid under the Merida Initiative. However, as yet, the Mexican government has been unable to break the power and impunity of the criminal syndicates. Not simply traditional drug cartels, TOCs, many with terrorist links, are also escalating the number and sophistication of their cyber attacks on businesses and individuals to steal intellectual capital, hack into private bank accounts, perpetrate fraud, and commit other cybercrimes that go undetected for months and even years. For example, Central European cybercrime networks alone defrauded US citizens or entities of an estimated US$1 billion in a single year.[2] Legitimate businesses suffer enormous losses and compete at a disadvantage when their intellectual capital is stolen and their products are counterfeited and sold at reduced prices. They are likewise harmed

[1] National Intelligence Council, *The Threat to National Security Posed by Transnational Organized Crime*, www.dni.gov/index.php/about/organization/national-intelligence-council-nic-publications

[2] National Security Council, *Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security*, www.whitehouse.gov/administration/eop/nsc/transnational-crime, July 2011, p. 7.

by trade-based laundering, which distorts the prices of commercial goods, and by criminal enterprises that bribe and intimidate government officials worldwide to gain special treatment or access to markets. The global stakes are enormous. These highly sophisticated and well-financed TOC and terrorist organizations wield unprecedented political and economic power; and their potential to disrupt critical infrastructure, undermine markets, spread deadly viruses, and even obtain weapons of mass destruction poses a grave threat to the nation's security.

The task of tracking and halting TOC activities has become increasingly difficult due to a number of factors. TOC and related terrorist organizations are extremely adept at exploiting cyber technologies, not just to commit crimes, but also to escape detection and operate hidden from view. Their highly decentralized networks adapt quickly to countermeasures, disbanding when threatened and later reappearing in new locations and disguises to resume their criminal activities. Their ability to collaborate and share information with a wide range of criminal and anti-state actors also adds to their strength and agility. Moreover, their many diverse criminal enterprises make it difficult for law enforcement agencies to bring them down solely by focusing on just one or two activities, such as narcotics or weapons trafficking. At the same time, government agencies are facing budget constraints not seen since government downsizing in the 1990s. Law enforcement agencies simply do not have the resources to fight TOCs by adding large numbers of personnel or buying expensive solutions. The alarming success of TOCs, combined with the constrained budget environment, has sparked a growing recognition that law enforcement agencies must find ways to operate more effectively and efficiently. This requires that current methodologies and procedures be adapted to meet the modern TOC threat, which is much more agile, elusive, and dangerous than earlier incarnations. When he released the government's "Strategy for Combating Transnational Organized Crime," President Obama declared, "Despite a long and successful

history of dismantling criminal organizations and developing common international standards for cooperation against transnational organized crime, not all of our capabilities have kept pace with the expansion of 21st century transnational criminal threats."[3] The challenge for today's law enforcement community is building the strategies, tactics, organizational structures, processes, partnerships and tools to exploit modern digital technologies and shift the advantage back in our favor in the fight against transnational criminals and terrorists.

Creating Agile Law Enforcement

The need to adapt law enforcement capabilities to the realities of new technologies and criminal activities is not new. In the early 20th century, the automobile enabled criminal gangs to travel quickly from one jurisdiction to the next, helping them stay beyond the reach of local sheriffs. Their crimes became national as well as local problems. Consequently, the Federal Bureau of Investigation (FBI) was created to counter criminal activities that crossed state and local borders, prompting federal, state, and local law enforcement officials to create new ways of working

[3] National Security Council, *Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security*, www.whitehouse.gov/administration/eop/nsc/transnational-crime, July 2011, p. iii.

together to defeat the new brand of criminals. The same challenge exists today: the Internet and other digital technologies have provided criminals with dramatically new modes of operation and new ways to escape arrest and conviction, similar to the advent of the automobile. Today, law enforcement and security agencies must chase cyber criminals across virtual networks stretching into every region of the globe. It is absolutely imperative that federal law enforcement agencies find new ways to work together to combat this modern, burgeoning threat. Moreover, collaborative efforts should include all relevant instruments of national power, including the intelligence community, military commands, diplomatic authorities, and other US national security organizations, as well as international partners who have shared interests and responsibilities in defeating transnational criminals and terrorists. Law enforcement entities must not only become more adept at interacting with each other, but also at interacting with the entire national security system.

A good starting point is understanding that the very same technologies that gave rise to modern TOCs can also give law enforcement an edge in uncovering their activities and shutting down their operations. These criminal enterprises leave digital footprints, just as all enterprises do. Travel, money transfers, and communications (including phones, email, instant messaging) generate data that can be combined and analyzed to gain a greater understanding of the TOC networks and activities. In addition, these organizations have common characteristics—for example, in how their leadership operates, how they communicate, and how they move money. Consequently, mapping a foreign fighter network in Iraq, for example, could provide lessons that fuel operations against Mexican cartels.

US government agencies have unique access to the data sources that can shine a spotlight on TOC leadership and activities. Much of this information is collected by law enforcement and other agencies for enforcement and regulatory purposes, but the data also contain significant potential for combating TOCs and sophisticated terrorist groups. A large portion of that data currently resides in separate agency divisions and systems that have different legal authorities, policies, and data tools. The information is not readily shared, nor are agency processes structured to provide a unified view of TOC threats. This hinders their ability to leverage the vast storehouses of data to uncover criminal activities or respond quickly against suspected threats. The law enforcement community recognizes the need for new approaches, but the challenge is figuring how best to facilitate the required integration and collaboration among agencies in the pursuit of shared mission goals, particularly given current budgetary constraints.

No single action will instantly solve the problem. In working closely with multiple law enforcement agencies focused on TOC and terrorist threats, we have observed that the most successful organizations are characterized by several common capabilities and characteristics, the most important being the ability to share and analyze information with multiple partner agencies, and related ability to collaborate with those agencies in the pursuit of common missions. To defeat today's highly networked transnational criminals and terrorists, US law enforcement agencies must themselves become a tightly knit, collaborative network that leverages their collective intelligence, analytic, and operational capabilities to optimize mission performance. No agency can defeat these international threats on its own, but by strengthening their collaborative networks—with each other and with other national and international partners—they can become more agile, flexible, swift, and strong in achieving their mission goals.

Based on Booz Allen Hamilton's extensive experience assisting US law enforcement and Homeland Security agencies in countering today's converging criminal

and terrorist threats, we recommend the following actions for building collaborative networks among law enforcement agencies:

1. Build Out the Vision Outlined in the White House Transnational Crimes Strategy

Released in July 2011, the White House's Strategy to Combat Transnational Crimes provides guidance to "build, balance, and integrate the tools of American power to combat transnational organized crime and related threats to our national security—and to urge our partners to do the same."[4] It lays out the nation's strategic objectives in the global fight against crime, such as breaking the economic power of TOCs, defeating their networks, and building international cooperation in these efforts. The strategy also identifies actions the nation and law enforcement community should take to enhance intelligence and information sharing, disrupt drug trafficking, protect the financial systems, and achieve other goals. Overall, the strategy provides guidance to help agencies develop strategies and take stronger action against TOC networks. Government agencies need to implement the strategy's guidelines and enhance information sharing.

2. Align Entities with Their Missions (not with their agencies)

Numerous federal agencies have law enforcement missions, each with a specialized area for countering domestic and international criminal and terrorist threats. Unfortunately, current rules and bureaucratic practices often prevent these agencies from combining efforts against common threats that transcend their own "lanes in the road." Even within the US Department of Homeland Security (DHS), member agencies pursue distinct missions, maintain separate records, and are not rewarded for internal DHS collaboration. Consequently, while the government expends a lot of resources tracking people, money, and goods, it often does so in stove-piped missions; and when government agencies attack TOC networks, they often do so separately, rather than mounting a collaborative operation to defeat the targeted network. Too often, our law enforcement entities operate as bastions aligned to agencies rather than to missions.

However, there exist a growing number of examples demonstrating how agencies can combine resources and efforts to pursue common mission objectives. For example, the Drug Enforcement Administration (DEA) is leading an interagency effort at the Special Operations Division with the FBI and DHS that is disrupting Hezbollah drug trafficking and money laundering. Similarly, the FBI, CIA, and other agencies are working together at the National Counterterrorism Center for a common mission, bringing together instruments of national power inside and outside the law enforcement community. Joint efforts by the FBI and DEA working against the Colombian FARC resulted in the indictments of 50 principal FARC members on drug trafficking changes. These and other examples can provide lessons for developing the methodologies, doctrine, training, and tools for enabling agencies to work together toward shared mission goals.

3. Make Integrated Fusion Centers the Norm, not the Exception

As criminal and terrorist networks become increasingly interconnected and collaborative in their operations, so too must law enforcement organizations. An important way to strengthen the law enforcement network is by enhancing the operations of fusion centers. Currently, most fusion centers are a collection of representatives from various law enforcement agencies who are co-located in federal buildings across the country. Unfortunately, in most instances, officers have little authority to collaborate with colleagues; and few are rewarded for serving in such centers. As a result, fusion centers rarely reap the benefits of the collective staffing talent.

Designated fusion centers could make multi-dimensional operations—such as the kind necessary

[4] National Security Council, *Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security*, www.whitehouse.gov/administration/eop/nsc/transnational-crime, July 2011, p. iii.

to counter evolving transnational terrorist and criminal threats—their principal missions, with the necessary authority to enhance effectiveness. Well-run fusion centers can serve as models for future practice. For example, the Organized Crime Drug Enforcement Task Force Fusion Center (OFC) is an inter-agency intelligence and investigative support center that excels at information sharing. The center maintains a single fused repository containing the most sensitive investigative information from all of the federal investigative agencies, including information from open investigations involving undercover agents, informants and cooperating witnesses, court authorized communications intercepts, etc. The single, fused database makes it possible to conduct a number of sophisticated analytic functions and proactively generate targeting packages. The interagency workforce has had tremendous success in coordinating and targeting sophisticated crime syndicates. Based on the OFC's success, the center has added a new component, the International Organized Crime Center (IOC2), to target non-drug related international organized crime.

Another effective example is the El Paso Intelligence Center (EPIC), which provides time-sensitive information to law enforcement customers who typically act on the information immediately upon receipt. EPIC has a 35-year history and is expanding its portfolio beyond the traditional "pull" model where individual users ask for specific information, so that now EPIC is increasingly "pushing" information to border operators and policy makers in a proactive way. On the international stage, interagency fusion centers in Iraq and Afghanistan have provided real-time analyses of terrorist and insurgent networks in support of critical multinational operations in those nations. Giving all fusion centers these kinds of capabilities and authorities would support the integrated and "networked" law enforcement required to defeat today's TOC and terrorist-insurgent networks.

With regard to state and local fusion centers, the Senate Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations recently concluded that DHS' work with the more than 70 state and local intelligence fusion centers "has not produced useful intelligence to support federal counterterrorism efforts."[5] A bi-partisan subcommittee report said that DHS intelligence officers assigned to fusions centers rarely produced intelligence of any value for counter-terrorism, and that the centers lacked "must-have" intelligence capabilities. Clearly, this is an area where DHS must strengthen the collaborative law enforcement network by providing more oversight and training for both its own intelligence officers and the state and local fusion centers.

4. Reward Activities and Behaviors Aimed at the TOC Threat

It is well understood that police and other law enforcement personnel will pursue policies and goals that are actively encouraged and rewarded by their organizations. They will focus on seizures and arrests because they are graded on the number of seizures and arrests they make. Consequently, law enforcement organizations should establish incentives to encourage and reward collaborative efforts to defeat transnational criminal networks, rather than for simply seizing drugs and making arrests. To reinforce the seriousness of our commitment to counter evolving transnational threats, for example, federal and state agencies could require a "successful tour" working with interagency partners, such as at a fusion center, as a necessary condition for promotion beyond a certain grade. By devising measures and rewards to foster collaborative actions and behavior, law enforcement would also be ensuring more accountability in achieving desired outcomes.

5. Focus on Criminal Financial Transactions

The huge volumes of financial transactions that pass through the US banking system provide a valuable opportunity to spot anomalies, uncover criminal transaction, and identify the people behind them. As mentioned, DEA led a joint operation with DHS and the FBI that disrupted illicit drug trafficking and money laundering by Hezbollah. As a result of the investigation, US authorities seized US$150 million

[5] Homeland Security & Governmental Affairs Permanent Subcommittee on Investigations, *Federal Support For and Involvement in State and Local Fusion Centers*, www.hsgac.senate.gov/subcommittees/investigations, October 3, 2012, p. 1.

from the Lebanese Canadian Bank in Lebanon, which has been sanctioned and required to pay significant fines and penalties. Similarly, the Department of Treasury was recently given expanded financial regulatory authority to investigate and prosecute international crime syndicates operating in the United States, essentially giving Treasury the same tools to combat organized crime as it uses to combat terrorist financing networks.

6. Use Analytics to our Advantage

Powerful analytic algorithms can sift through data at fusion centers and other locations to quickly uncover patterns of behavior or connect the dots between seemingly unrelated information and events. In addition, cloud computing now eliminates many of the technological barriers to centralizing and sharing data, giving agencies far greater reach into federated data sets containing potentially valuable threat information. Data analytics could be applied in a variety of ways. For example, law enforcement agencies that use supply chain attack models can go beyond traditional approaches, which typically examine contraband and the people involved in trafficking the contraband, to instead map out all of the sophisticated processes, people, technologies, and flows associated with the illicit enterprise. This would allow agencies to identify points of weakness that can be targeted with the goal of causing cascading failures to the system. In an era of budget constraints, cloud analytics will also help agencies operate more efficiently and effectively.

7. Promote Information Sharing

Over 12 years have passed since 9/11 and many law enforcement agencies remain reticent to share data, creating information gaps readily exploited by sophisticated transnational criminal entities. However, many notable examples exist within government showing that agencies can effectively share and extract value from data while also keeping it secure, preserving privacy, and complying with federal regulations regarding the handling of data. For example, the FBI's Investigative Data Warehouse collects data from multiple law enforcement and intelligence community databases, and makes the data available to authorized personnel throughout the country. The Integrated Automated Fingerprint Identification System (IAFIS) is a national fingerprint and criminal history system that is widely available and used by local, state, and federal law enforcement officials to track and capture criminals and terrorists. Similarly, the OFC, mentioned earlier, contains the most sensitive investigative information from seven federal agencies, as well as other data sets, which are shared among agencies. And the CIA's Crime and Narcotics Center, which collects and analyzes information relating to international narcotics trafficking and organized crime, supports law enforcement as well as the US military, State Department, and other agencies, providing one model for information sharing across a wide spectrum of national security organizations.

A starting point for promoting information sharing is the creation of department-wide technology systems, rather than allowing individual agencies to create their own silos of excellence. Within DHS, for example, virtually all of the major component agencies, including the US Coast Guard, Immigration and Customs Enforcement, Customs and Border Protection, and the Transportation Security Agency, run their own separate IT systems. Regrettably, the agency specific systems are frequently incompatible with technology platforms used by other agencies within the same department. Creating a department-wide IT system would facilitate information sharing within the department, and made it easier to share information and collaborate with agencies outside the department.

Conclusion

The converging threats of transnational criminals, terrorists, and insurgents are not only exacting enormous costs on citizens and businesses, but they also pose a significant danger to national security with their growing potential to disrupt major government operations, distort or undermine economic markets, and proliferate weapons of mass destructions. No single law enforcement agency, acting alone, can

counter this threat. But collectively, agencies have the information and capabilities to identify, track, and dismantle these organizations. Countering today's emerging threats will require US law enforcement and security agencies to adapt new operating models that leverage new mission enabling technologies and foster significantly greater collaboration across the traditional boundaries of agency affiliation. The expanded collaboration must include not just other law enforcement organizations but also other US agencies and international partners whose shared mission responsibilities and complementary capabilities can provide valuable support in the global fight against transnational criminals and terrorists. The current environment of budget austerity makes this collaboration vital, while the emergence of well-funded hybrid organizations that facilitate both crime and terrorism argue for an increased sense of urgency. By creating collaborative mission-focused networks and using powerful new analytical tools, law enforcement organizations can operate more efficiently and effectively against sophisticated transnational adversaries. Networked law enforcement operations will provide the agility, flexibility, and strength needed to defeat these threats to our national security and homeland.

Contacts

David Rubin
Senior Vice President
rubin_david@bah.com

Bob Sogegian
Vice President
sogegian_bob@bah.com

Anthony Placido
Executive Advisor
placido_anthony@bah.com

Achieving "Unity of Effort" in Cybersecurity

How the Department of Homeland Security Can Strengthen the US Government's Cyber Partnership with the Private Sector

Achieving "Unity of Effort" in Cybersecurity

How the Department of Homeland Security Can Strengthen the US Government's Cyber Partnership with the Private Sector

The United States is facing a "pre-9/11 moment" for cyberspace.[1] No widespread economic damage or loss of life has been achieved by cyber attacks on the nation's critical networks and systems, but the warning signs are present. US government agencies face an onslaught of attacks, each day, as do other critical infrastructure sectors. In September 2012, distributed denial-of-service attacks allegedly initiated by Iran, disrupted operations at several major US banks. Terrorist groups and hacktivists also have the capability to inflict damage, as shown by the successful Anonymous attacks on the Israel Ministry of Foreign Affairs and Bank of Jerusalem during recent Middle East hostilities. In addition, human error can introduce unintentional threats and disruptions to US critical infrastructure, such as accidental data breaches exposing millions of sensitive records or accidental destruction of fiber optic cables or other equipment shutting down connectivity for entire regions.[2] While anecdotal or historical parallelism does not fully reflect the nature of today's cyber threat environment, the US does seem to only have a short window of opportunity remaining to prepare for major cyber incidents that, if successful, could be as physically and economically devastating as severe hurricanes or other natural disasters. "The urgency and the immediacy of the cyber problem—the cyber attacks that we are undergoing and continuing to undergo—cannot be overestimated," said Secretary of Homeland Security Janet Napolitano.[3]

The US government is pressing forward with changes to meet the cybersecurity challenge by strengthening cybersecurity-related policies to match the severity and urgency of the risks posed by the current cybersecurity environment. In mid-October, the president reportedly signed a directive laying out rules of engagement allowing the military to act more aggressively in countering cyber threats to the nation.[4] In addition, the Administration is poised to issue an Executive Order (EO) clarifying and strengthening the role of the government and industry entities in enhancing the cybersecurity and resiliency of US critical infrastructure. While some may view the anticipated EO as merely formalizing what is—or should be—the US Department of Homeland Security's (DHS) responsibilities, we believe it provides DHS with an opportunity to realize the department's cybersecurity mission. In this "pre-9/11 moment," DHS needs to be seen as the strategic leader and focal point for building unity of effort among public- and private-sector cybersecurity partners.

Enhancing DHS' Cybersecurity Role

The urgent need for stronger cybersecurity has increased dramatically in recent years, not just because attacks have grown more frequent and sophisticated, but because the nation's dependence on information and communications technology (ICT) has grown to a level that makes it inseparable from the physical infrastructure it traditionally has enabled. In short, the ICT elements of critical infrastructure have become just as important as critical infrastructure's traditional or physical aspects. A successful attack on the nation's power grid can occur by physical destruction of critical elements or nodes, as well as a successful and sophisticated cyber attack. An extended electricity outage could easily cascade to other sectors to cause widespread, long-lasting damage or serve as a force multiplier during physical attacks, impeding response and recovery efforts. The Administration's planned EO would strengthen cybersecurity by improving private and public sector information sharing about major cyber incidents, such

[1] Secretary of Defense Leon E. Panetta, in a speech titled "Defending the Nation from Cyber Attack," October 11, 2012; and Stephanie O'Sullivan, principal deputy director of the Office of the Director of National Intelligence, in an article by William Jackson, "In cyber's 'pre-9/11' moment, intell agencies turn to automation," *GCN*, October 30, 2012.

[2] See, e.g., *Help Net Security*,"Data breaches expose 94 million records in the government sector," September 10, 2012; Parfitt, Tom, *The Guardian*, "Georgian woman cuts off web access to whole of Armenia," April 6, 2011; and Field, Tom, *BankInfoSecurity.com*, "Insider Threat: 'You Can't Stop Stupid,'" July 28, 2010.

as breaches, stolen data, and disrupted or degraded networks; and it would help establish a minimum level of cybersecurity through the identification and adoption of practices that address each sector's unique needs. Improved information sharing and a more rigorous security environment would enable public and private sector entities to identify trends, anticipate attacks, and help infrastructure organizations protect and defend against cyber incidents. DHS already plays a central role in coordinating critical infrastructure protection, and as the one civilian agency with public-private sector cybersecurity coordination responsibilities, it possesses the unique ability to lead government's efforts to improve the protections and resiliency of privately held networks and systems.

Achieving these new mission goals will not be easy. Major disagreements between government and industry organizations about information sharing will need to be addressed so vulnerabilities and breaches can be managed in ways that capitalize on the authorities and role of government while respecting and acknowledging the important functions industry organizations perform. Disagreement also exists over how to implement standards, including the kinds of standards that should be adopted. Equally challenging, many industry officials are not yet persuaded of the business case for pursuing these activities. Consequently, DHS will have to find the right balance between empowering organizations to secure their networks and information voluntarily while also providing a meaningful direction to infrastructure sectors to establish a minimum level of security that preserves the nation's global economic and security prowess.

DHS is well positioned to carry out its new responsibilities, despite these challenges. The DHS Office of Cybersecurity and Communications (CS&C) is already working to enhance the security, resiliency, and reliability of the nation's critical infrastructure. Similarly, the agency has already gained valuable experience gathering and sharing cyber information within government and with industry through the National Cybersecurity and Communications Integration Center (NCCIC) and its other incident response

capabilities that are co-located within it. DHS has also been working to bolster its workforce of cyber professionals to improve its overall capabilities.

Booz Allen Hamilton has enjoyed a long and successful history of supporting the DHS' cybersecurity and infrastructure protection missions since its creation in November 2002. We have supported DHS in many of its strategically important cyber programs and initiatives. As DHS prepares to take on expanded cyber responsibilities, we draw upon our longtime partnership with DHS and our extensive cyber experience assisting government and industry to offer these axioms for addressing cyber challenges.

Axiom 1: Take Advantage of DHS' Public and Private Sector Collaboration Role

DHS' unique mission to lead government-industry collaboration in prevention and response activities is the lynchpin of enhanced resilience and cybersecurity across critical infrastructure organizations. DHS' mission has positioned it to be the US federal government's lead for engaging industry in maintaining the nation's infrastructure protection, cybersecurity, and response capabilities. DHS' role as a civilian

[3] Martinez, Jennifer, *The Hill*, "Napolitano: US financial institutions 'actively under attack'by hackers," October 31, 2012.

[4] Nakashima, Ellen, *The Washington Post*, "Obama signs secret directive to help thwart cyber attacks," November 14, 2012.

agency also enables it to lead implementation of domestic cybersecurity policy in ways that other national security agencies cannot.

As part of the nation's infrastructure protection strategy and planning activities, DHS has established a governance model that has been effectively used to plan for physical and cyber incidents. In addition, this model has recognized the cultural needs of sectors and organized them in a manner that allows them to address common issues and risks that face their partner organizations. The governance model has provided meaningful contributions to previous policy shaping activities, such as the Cyberspace Policy Review, which was led by senior Administration officials in 2008 and 2009. It has created forums, such as those supporting the Enduring Security Framework as well as sector-specific risk management activities, where technical- and policy-related problems are identified and addressed through trusted and collaborative discussions that DHS supports and leads with industry and government representatives.

DHS organizations have also already created effective processes, systems, and organizational cultures supporting collaboration in a crisis. The Federal Emergency Management Agency (FEMA) is an example of how DHS' engagement with industry and other government entities addresses physical disasters. In its role supporting public and private sector efforts to prepare for, protect against, respond to, recover from, and mitigate hazards, DHS works with partners at all levels of federal, state, and local government, both national and international, as well as with nonprofit and commercial organizations. FEMA plays an essential leadership and coordinating role to ensure that all relevant partners have the necessary information and resources to carry out their missions of mitigating physical disaster risks. DHS will need to respond with appropriate measures in the event of cyber incidents on critical infrastructure that have physical consequences and, to do so, it will need to better link and facilitate the response capabilities currently comprising the National Protection and Programs Directorate's warning centers, the NCCIC, and FEMA.

With enhanced organizational structures and integrated capabilities, DHS must rely more heavily on its partners and, where appropriate, seek to leverage—rather than replicate—capabilities and expertise. Expanding threats and constrained budgets will require all federal agencies to work as efficiently as possible by collaborating on shared mission responsibilities. By serving as a central hub for information sharing, DHS can carry out its missions of protecting critical infrastructure and federal networks, while also supporting the need of responding to current and emerging threats to the nation's critical infrastructure.

Axiom 2: Emphasize a Risk-based and Standards-based Approach that is Premised on Empowering Organizational and Sector-wide Resilience and Innovation, Rather than a Reactive Regulation and Compliance Regime

Adopting a strict regulatory approach in which the government seeks to enforce standards will create a focus on checklists and compliance rather than achieving genuine security. In contrast, a risk-based approach that uses standards to guide cyber activities will give government agencies and industry the flexibility to adopt measures that best suit each sector, as well as the flexibility to adjust to evolving threats, vulnerabilities, and risks. A focus on risk also helps companies to see the full spectrum of risks presented by cyber breaches, ranging from financial losses to damaged brands and reputations. And this, in turn, helps substantiate the business case for action.

The North American Electric Reliability Corporation (NERC) offers an example of how industry can create a sector-specific framework for self-regulation of cyber standards. NERC works with electric utilities to develop reliability standards and then enforces compliance with those standards. NERC also coordinates the physical and cybersecurity needs of its members, analyzes system events, identifies trends and potential reliability issues, and promotes a culture of excellence by identifying best practices and areas for improvement. Compliance is enforced through self-reporting by

companies and through audits, monitoring, and investigations by NERC, which assesses monetary and non-monetary penalties for noncompliance. NERC also sponsors a cybersecurity incident readiness exercise, called GridEx, which tests crisis response plans and provides insights to enhance collaboration and strengthen security processes and capabilities.[5] Booz Allen assists NERC in developing and conducting GridEx, which is modeled after DHS' Cyber Storm exercise.

DHS can provide valuable assistance to the critical infrastructure sectors by helping them establish cybersecurity rules and standards that are appropriate for each sector. DHS can also help identify best practices and promote the development of maturity models to benchmark cyber capabilities. Maturity models provide a clear, risk-based vision of the spectrum of cyber challenges that organizations face; and in this way, maturity models enable organizations to allocate cyber resources in the most efficient manner by showing the trade-offs between investment and risk. In fact, DHS and the US Department of Energy are already helping the electric power industry develop the Electricity Sector Cybersecurity Capability and Maturity Model to gauge industry readiness and provide policymaking guidance.[6] DHS can also promote collaboration and adoption of best practices in other critical infrastructure sectors through risk identification and management activities and cyber exercises and wargames. The bi-annual Cyber Storm could be adapted for this purpose, as it was for the electrical sector.

Axiom 3: Build the Right Cyber Skills and Address Surge Requirements

DHS lacks the workforce skills it needs to carry out its current cybersecurity mission responsibilities. A report by the Homeland Security Advisory Council CyberSkills Task Force, published in the fall of 2012, said the agency needs 600 additional employees with mission-critical cybersecurity skills, and advised DHS to establish a Cyber Reserve program of DHS cyber alumni and other experts to call upon in an emergency.[7] New cyber responsibilities will only exacerbate the agency's workforce shortfall.

DHS is aggressively pursuing programs to hire, train, and retain cyber employees. Secretary Napolitano said DHS has increased its cyber workforce by 600 percent over the last few years.[8] DHS should ensure that ongoing hiring efforts focus on acquiring needed skills in security engineering, malware analysis, advanced analytics, continuous monitoring, and other technical areas relevant to its evolving mission tasks. It is vital that DHS create other avenues for surge capacity, such as establishing contract vehicles providing access to the private sector's cyber expertise during a crisis. In the event of a cyber attack that has national security consequences, DHS will need to have immediate access to cyber talent outside the federal workforce.

Axiom 4: Accelerate Adoption of Advanced Data Analytics and Continuous Monitoring

The enormous volumes of data that DHS has access to related to the protection of government and critical infrastructure networks must be harnessed to identify future cyber trends and threats. However, DHS currently lacks the capability to fully process and analyze the terabytes of cyber data that exist. To address its new responsibilities, DHS will need to tap emerging cloud-based analytics that can analyze and glean insight from the additional stores of data. The department will also need to improve its information sharing capabilities, so public- and private-sector organizations can benefit from DHS' deeper analyses. By embracing emerging data analytics, DHS can elevate its role in coordinating government-industry cyber activities and partner with other agencies to protect the nation's critical cyber infrastructure.

Another key cyber capability is continuous monitoring. Given the dynamic nature of the cyber environment, the federal government is shifting from traditional compliance reporting to measuring security status on a more timely basis through continuous monitoring sensors, diagnosis, mitigation, and other tools. As part of its mission to protect government network domains, DHS is delivering Continuous Monitoring as a Service

[5] North American Electric Reliability Corporation (NERC), *NERC Announces Grid Security Exercise*, May 3, 2011.
[6] The maturity model is described in September 27, 2012, letter to Senator John D. Rockefeller IV from the heads of four electric power associations. www.nreca.coop/press/Testimony/Documents/ElecSectorResponsetoRockefeller.pdf
[7] US Department of Homeland Security, *CyberSkills Taskforce Report*, Fall 2012, p. 4.
[8] Miller, Jason, *Federal News Radio*, "Napolitano wants NSA-like hiring authority for DHS cyber workforce," October 31, 2012.

(CMaaS) to federal agencies under the department's Continuous Diagnostic and Mitigation program. Key to successful adoption of this program would be consistent implementation throughout the government and bi-directional sharing of continuous monitoring data to secure government networks.

By rewarding innovative and dynamic security practices in areas such as advanced analytics, continuous monitoring, and other emerging cyber technologies, DHS will empower its partners inside and outside government to bring forward new and more powerful solutions for addressing our evolving cyber risks.

Conclusion

Even as the Administration advances its cyber initiatives, it likely will continue pushing for legislative action to achieve changes requiring Congressional approval. But the trajectory of DHS' cyber roles and responsibilities is clear. The Administration wants—and the nation needs—DHS and agencies with a public-private sector partnership mission to step forward and establish a more meaningful presence in protecting the functions, networks, and systems of both the private sector and federal civilian agencies. Of all federal agencies, DHS is best positioned to serve as the focal point for coordinating, analyzing, and sharing data about attacks and breaches with industry and government entities. State-of-the-art data analytics tools, capabilities, and processes will enable DHS to glean insights that can help the nation prepare for and manage cyber incidents. DHS can also elevate its role by helping industry adapt standards and promote maturity models that are tailored to the requirements of each critical infrastructure sector. It can further its leadership by implementing new technical capabilities, such as continuous monitoring, to make government networks more resilient.

"Unity of effort" is the common theme that underlies these activities. This should not be surprising. The United States failed to untangle the clues to the 9/11 terrorist attacks of 2001 due to poor communication and haphazard information sharing among government agencies tasked with tracking terrorist activities. In this "pre-9/11 moment" for cyberspace, DHS has an opportunity to help government and industry get it right. Whether working with the private sector or other government organizations, DHS will depend on strong, collaborative relationships and innovative ideas from within government and across industry to perform its cyber missions successfully.

Contacts

George Schu
Senior Vice President
schu_george@bah.com

Lori Sparks
Principal
sparks_lori_l@bah.com

Marcia McGowan
Senior Associate
mcgowan_marcia@bah.com

About Booz Allen

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for nearly a century. Today, Booz Allen is a leading provider of management and technology consulting services to the US government in defense, intelligence, and civil markets, and to major corporations, institutions, and not-for-profit organizations. In the commercial sector, the firm focuses on leveraging its existing expertise for clients in the financial services, healthcare, and energy markets, and to international clients in the Middle East. Booz Allen offers clients deep functional knowledge spanning strategy and organization, engineering and operations, technology, and analytics—which it combines with specialized expertise in clients' mission and domain areas to help solve their toughest problems.

The firm's management consulting heritage is the basis for its unique collaborative culture and operating model, enabling Booz Allen to anticipate needs and opportunities, rapidly deploy talent and resources, and deliver enduring results. By combining a consultant's problem-solving orientation with deep technical knowledge and strong execution, Booz Allen helps clients achieve success in their most critical missions—as evidenced by the firm's many client relationships that span decades. Booz Allen helps shape thinking and prepare for future developments in areas of national importance, including cybersecurity, homeland security, healthcare, and information technology.

Booz Allen is headquartered in McLean, Virginia, employs approximately 25,000 people, and had revenue of $5.86 billion for the 12 months ended March 31, 2012. *Fortune* has named Booz Allen one of its "100 Best Companies to Work For" for eight consecutive years. *Working Mother* has ranked the firm among its "100 Best Companies for Working Mothers" annually since 1999. More information is available at www.boozallen.com. (NYSE: BAH)

To learn more about the firm and to download digital versions of this article and other Booz Allen Hamilton publications, visit www.boozallen.com.

Booz | Allen | Hamilton

Principal Offices

Huntsville, Alabama
Sierra Vista, Arizona
Los Angeles, California
San Diego, California
San Francisco, California
Colorado Springs, Colorado
Denver, Colorado
District of Columbia
Orlando, Florida
Pensacola, Florida
Sarasota, Florida
Tampa, Florida
Atlanta, Georgia
Honolulu, Hawaii
O'Fallon, Illinois
Indianapolis, Indiana
Leavenworth, Kansas
Aberdeen, Maryland
Annapolis Junction, Maryland
Hanover, Maryland
Lexington Park, Maryland
Linthicum, Maryland
Rockville, Maryland
Troy, Michigan
Kansas City, Missouri
Omaha, Nebraska
Red Bank, New Jersey
New York, New York
Rome, New York
Dayton, Ohio
Philadelphia, Pennsylvania
Charleston, South Carolina
Houston, Texas
San Antonio, Texas
Abu Dhabi, United Arab Emirates
Alexandria, Virginia
Arlington, Virginia
Chantilly, Virginia
Charlottesville, Virginia
Falls Church, Virginia
Herndon, Virginia
McLean, Virginia
Norfolk, Virginia
Stafford, Virginia
Seattle, Washington

The most complete, recent list of offices and their addresses and telephone numbers can be found on www.boozallen.com

www.boozallen.com