Finalist Essays from the Center for Homeland Defense and Security's Second Annual Essay Competition, 2009

Essay Question

What advice concerning Homeland Security would you give the next presidential administration and why?

Winning Essay

Emergency Response, Public Health and Poison Control: Logical Linkages for Successful Risk Communication and Improved Disaster and Mass Incident Response
Valerie Yeager, Research Assistant, University of Alabama at Birmingham South Central Center for Public Health Preparedness

Finalists

(listed in alphabetical order by last name)

The Department of Homeland Security Initiative for Community Empowerment and Security: A Community Based Approach to Homeland Security
George Ewing, Client Development Officer, CitiFinancial Auto

A National Information Policy
Andrew Faltum, Military Lead Analyst, Alion Science and Technology

Saving the Internet or "Who Are You Going to Trust"
Harry Haury, Chief Executive Officer and Founder, NuParadigm Government Systems, Inc.

Building a Central Intelligence Registry
George Pugh, President, George Pugh & Co.

About the Competition

The Center for Homeland Defense and Security (CHDS) essay contest, now in its second year, is aimed at stimulating original thought on issues in Homeland Security and Homeland Defense. CHDS launched the contest in 2008 to provide people from around the country the opportunity to express their opinions on homeland security issues and to suggest new ideas. This year's winner and four finalists were selected from 147 contest submissions by a committee comprised of CHDS staff, faculty, and alumni. The variety of the essay topics submitted, as well as the backgrounds of the authors, highlights the vast scope of the impact that homeland security policies, programs, and challenges have on our communities and professions. This year's contestants were asked to answer the question, "What advice concerning Homeland Security would you give the next presidential administration and why?"

Congratulations to this year's winners. We hope reading their essays will accomplish the contest objective of stimulating thoughts and ideas and promoting discussion and debate on homeland security and defense issues.

More information about the competition, including the question and guidelines for the current competition and an archive of questions and finalist essays from previous competitions can be found at the following web address:
http://www.chds.us/?essay/overview

EMERGENCY RESPONSE, PUBLIC HEALTH AND POISON CONTROL: LOGICAL LINKAGES FOR SUCCESSFUL RISK COMMUNICATION AND IMPROVED DISASTER AND MASS INCIDENT RESPONSE

Valerie Yeager

Valerie Yeager is a 2007 graduate of the University of Alabama at Birmingham's School of Public Health. Upon completion of the MPH, she began working with the South Central Center for Public Health Preparedness as a research assistant. She is also currently a doctoral student in the University of Alabama at Birmingham's School of Public Health. Ms. Yeager was awarded the 2007 Lister Hill Policy Fellowship and served as a fellow in the Center for Disease Control and Prevention's Division of Global Migration and Quarantine. She served as an applied anthropological researcher in a HIV clinic in South Africa, writing about the challenges of HIV treatment in impoverished areas. While documenting the experiences of patients and the clinic team, Ms. Yeager also worked to complete a master degree in journalism with the University of Stellenbosch in South Africa. Ms. Yeager may be contacted at v.yeager@gmail.com.

The author would like to acknowledge and thank the poison center representatives who have taken the time to speak about their centers and thank the anonymous reviewers for their comments. She would also like to thank Lisa McCormick, Dr. Peter Ginter and Dr. Nir Menachemi for their encouragement and guidance in the development of this paper.

INTRODUCTION

The 2002 *National Strategy for Homeland Security* established a broad mission to find ways to improve homeland security. [1] In addition to preventing and mitigating disasters, the 2002 *National Strategy for Homeland Security* highlighted the need to develop complimentary systems to avoid duplication and increase collaboration and coordination. [2] Progress toward these objectives will ensure more effective responses to all hazards faced by Americans and contribute to the overall

mission of improved security. This essay explores the possibilities of linking emergency response and public health with the poison control system for increased collaboration and coordination during disasters and emergencies. If successful, these linkages will ensure that we are more capable of effectively preventing, responding to, and recovering from disasters and emergencies. The provision of accurate public information and active surveillance, prevention of avoidable of surges in medical need, continuity of response operations, mitigation of public anxiety, and cost-savings for the health care system make Poison Control Centers a natural ally for disaster response agencies and public health. [3]

DISASTERS AND EMERGENCIES REQUIRE CONSISTENT AND ACCURATE PUBLIC INFORMATION

Recent natural disasters like Hurricanes Katrina and Rita, terrorist events such as the Oklahoma City Bombing and the events of 9/11, and public health incidents such as Salmonella and Escherichia coli (E. coli) outbreaks all required effective risk communication and safety guidance during and after the events. [4] Currently, however, Americans do not have a consistent mechanism for the timely and repeated delivery of trustworthy public safety and health information. [5] Most Americans rely on information translated through mass media before, during, and after a disaster or emergency incident; but the inherent flaw in this system is that we cannot ensure the consistent and accurate translation of crucial public safety and health information.

As in most countries, Americans endeavor to discern between the factual and sensationalized information delivered through mass media. Additionally, people experiencing extreme anxiety or fear during a disaster or emergency incident will want assistance making health-related decisions, but the mass media cannot answer individual questions. [6] When we experience extreme anxiety and fear, we seek reliable, trustworthy, and knowledgeable advice from respected individuals such as the police, the government, and medical professionals. [7] This is inherently problematic during and immediately after disasters as there may be no direct connections to these agencies or officials. In most mass casualty and disaster events, these officials will be heavily taxed by the response to the event and will likely be unable to handle the mass inquires and calls for personalized information and guidance. [8]

In light of this dilemma and in response to the 2002 *National Strategy for Homeland Security*, there exists great potential to increase collaboration and coordination and utilize the well-developed infrastructure present in the poison control system. [9] This system currently has the potential to provide for immediate, and consistent personalized public information during and after a disaster

or emergency incident. The poison control network is well established. In its fifty-five years of service it has become well known and trusted among the American public as a source of reliable information.

Mitigating Unnecessary Medical Surges

Public information is crucial during disasters and mass incidents. Efficient person-to-person information mitigates worry and potentially keeps people from rushing to an emergency room for answers. [10] Fear and anxiety are mediated by information; therefore it is essential that we strive to find a mechanism to provide the public with a reliable system for receiving accurate and consistent information during a disaster or emergency incident. [11]

A recent study highlighted the crucial role of adequate public health information during disasters and mass incidents. [12] It found that the American public will indeed seek out protective information and guidance during a disaster or mass incident. [13] If social distancing measures are implemented (requesting that individuals remain at home unless absolutely necessary) people will want a means to reach trusted health professionals from their homes. Without adequate and sometimes personalized information, people who are concerned that they may be ill or exposed to the infectious agent may go to an emergency department or physician's office for reliable answers. Situations such as an infectious disease outbreak, especially with high-profile diseases like Avian or Pandemic Influenza, have great potential to overwhelm our medical system and create major obstacles to efficiently treating those in need of care. [14] Additionally, those who have not been exposed, but are worried about being ill may actually be exposed to the infectious agent if unnecessarily visiting physicians and emergency departments.

Active Surveillance Capabilities

Poison control centers have the potential, if linked with public health and trained to handle public health related issues, to efficiently receive and respond to requests for public health information and guidance. They also have the systems and capabilities to perform active surveillance and reporting and can be utilized to screen and refer callers to appropriate facilities for medical screening and/or treatment. [15]

In response to the 2006 radiological dispersal incident, an event of public health significance, Britain utilized their nurse-led, telephone system, the National Health System Direct (NHS Direct),

to quell the fears of thousands of citizens who were unaware of the health risks of radiological exposure, unfamiliar with Polonium-210, or unsure of how or if they could have been exposed to Polonium-210. [16] They also used this same telephone nurse system to screen potentially exposed individuals and refer those persons to appropriate centers for urine collection and analysis. NHS Direct was able to perform active surveillance during the incident.

During the response to the intentional radiological dispersal incident, the Health Protection Agency, Britain's equivalent of the United States' Centers for Disease Control and Prevention, provided essential information both through the NHS Direct Internet site and the twenty-four-hour, nurse-staffed telephone help line. Within days of informing the public that Litvinenko died of an intentional radiological poisoning, NHS Direct received over 2,000 phone requests for information about exposure, side effects, and other concerns. In the next month, the number rose to a total of almost 4,000 calls about the incident. [17] Imagine if these 4,000 callers had rushed to the nearest emergency department with their worries. The health system would not have been able to triage all of these thousands of people along with other unrelated emergency cases. The surge would have severely taxed the health care system and the laboratory network. The provision of personalized, adequate health information provided immeasurable benefits to the response efforts.

NHS Direct also utilized a systematic approach to screen individuals for potential exposure based on the known information about the event and were subsequently able to refer this smaller group of nearly 800 people on for medical monitoring. [18] The U.S. can utilize the poison control system in a manner similar to what was done in the Britain Litvinenko intentional dispersal event. Currently they are assisting in the response to the H1N1 outbreak. According to the National Poison Data System, between May 20th and August 13th, 2009, the U.S. poison control system fielded 392 calls from the public about H1N1. [19] This is evidence that the U.S. public utilizes poison control centers as a resource for information about diverse health topics, not only poisonings.

EXISTENT CONTINUITY OF OPERATIONS PLANS

In addition to potentially reducing healthcare surge-capacity dilemmas and to providing active surveillance, poison control centers often have continuity of operations plans to ensure continuation of services in emergency or disaster situations. In order to receive federal funding, poison centers must meet the American Association of Poison Control Centers' certification standards that include having mutual aid agreements for both local and national poison center partnerships for when call assistance is needed.

For the most part, poison control centers have the autonomy to plan and train for emergencies and disasters as they deem appropriate. While exact statistics are unknown, many of the sixty poison centers are able to generate their own electricity to run computer systems and receive telephone calls should their region experience damaged infrastructure during a natural disaster or terrorist event. Additionally, some centers have plans for their nurses to telecommute if the disaster or event requires (and allows) it and, through a universal online information platform, they have the ability to receive immediate information updates simultaneously across the sixty centers. [20] While not all poison centers are currently able to access this platform online in real time, this resource is in development. In the meantime, email can be used to get consistent urgent response messages across all centers simultaneously.

Handling Anxious and Fearful Callers

Not only do poison control centers have the infrastructure and systems to receive calls and provide consistent, accurate information, they are also trained and experienced in communicating with anxious, worried callers. With appropriate situational information, poison control specialists can also field calls from worried and emotional callers during disasters and mass incidents. Certainly, these specialists can benefit from improved psychological first aid skills, but the foundation for this response exists.

In the 2003 SARS outbreak in Toronto, Canada's Telehealth system (another national, nurse-led telephone system) provided crucial support during an event that required strict social distancing measures and caused extreme and hyper-vigilant fear among citizens. Prior to the outbreak, Telehealth fielded approximately 2,000 calls per day. During the event, nurses handled over 20,000 calls per day. [21]America's existing poison control system has the infrastructure and the trained personnel to provide a similar response to calls for personalized, accurate and consistent risk communication during a disaster or emergency incident. While one regional center alone may not be able to handle all of the calls of a regional disaster such as the Toronto SARS outbreak, unanswered calls will roll to partner centers for additional support. It is also possible to forward calls to other centers as needed. In 2007, US poison control centers fielded over 4 million calls, averaging almost 12,000 calls per day as routine service. [22] Some poison control centers are working to identify additional nurses to commit to training and assist as needed in an outbreak or other emergency or disaster-related event. In some cases, contingency plans include the assistance of retired nurses located through partnerships with state public health agencies. This is an example

of one way poison centers and public health can plan and work together to increase preparedness and resiliency during a prolonged emergency or disaster.

As a federalist nation founded on individual state autonomy, it is difficult to provide consistent messaging to the public in multiple states and regions when disasters and emergency incidents happen. The poison control system, as previously discussed, has the existing infrastructure to provide consistent messages to the poison control centers in all fifty states. With a universal access number, callers can easily reach their regional poison control center from anywhere in the U.S. If, for any reason, the regional phone lines are unavailable, the call will automatically roll to partner poison control centers. If there is a disaster affecting phone service in the region, poison centers will forward their calls to their national partners until the region regains service. They also have a language line for speaking with non-English speakers and telecommunication devices for the hearing or speech impaired.

An Example of a Successful Linkage

The Georgia Poison Center has been collaborating with the state Department of Public Health for over a decade. They receive public health's after-hours calls, provide guidance, and triage calls requiring direct connections to on-call public health officials. Georgia's Department of Public Health contributes funding to the Georgia Poison Center to cover the cost of providing this service and for triaging all rabies calls. [23] In addition to calls rolled from the Department of Public Health phone lines, the Georgia Poison Center has assisted callers during the 2004 fire that resulted in chemical releases around the city of Atlanta, and the closing of an area hospital and freeway. They field calls about unknown substances, such as during the white powder Anthrax incidents of 2001, and they handle food outbreak concerns and reports. Already, other poison control centers, as in Georgia, are working with public health to improve their response and recovery from incidents and outbreaks. It is essential to foster these and other relationships between poison centers, public health, and emergency response. In states where partnerships exist, the linkages necessary for improved all-hazards risk communication, response, and recovery will be developed with greater ease.

Utilizing Existing Systems as Cost-Savings

According to 1992 national data, the poison control system reduced annual medical spending by $355 million through cost avoidance by managing caller concerns and reducing the need for callers to attend emergency departments. [24] Similar cost savings may be possible for disaster and mass

incident response and general assistance to public health departments. One possible challenge to developing these partnerships is that the increase in cost to the poison control centers must be supplemented with appropriate funding from federal or state governments or new partner organizations.

Poison control centers continue to struggle to remain financially viable. They currently receive federal funding through the Poison Control Center Enhancement and Awareness Act but the appropriated amount can change depending on the federal budget. For most centers this federal funding does not provide enough support to cover their entire annual budget. Poison centers receive state funding as well, which means that year-to-year state budget cuts have the potential to have a negative impact on the future of some poison control centers. As a result of these funding inconsistencies, some poison control centers have utilized innovative mechanisms to ensure financial support. For example, in one state, all medical centers receiving assistance from poison centers provide supplemental funding to the state poison control system. Another state receives supplemental funding from tax structures such as long distance phone taxes. Useful partnerships between public health, emergency management, and homeland security have the potential to supplement the budgets of poison control systems while simultaneously providing benefits to the partner agencies and, perhaps most importantly, to the U.S. public in the form of improved homeland preparedness, response, and security.

CONCLUSION

As we "strive to create a fully integrated national emergency response system that is adaptable to any terrorist attack, no matter how unlikely or catastrophic, as well as all manner of natural disasters," [25] it is natural that public health and emergency management partner with poison control centers and utilize the strong foundation present in the poison control infrastructure. Americans will expect forthcoming risk communication and it is necessary that we think through how we will field the many thousands of telephone calls, public inquires, and requests for guidance that may result for any number of hazards. Personalized information may be necessary to keep our other response and medical systems functioning efficiently; however, we need to ensure adequate and consistent messages. The poison control system can already do this, but we will need to overcome the potential barriers of obtaining buy-in for establishing partnerships among these agencies and increase funding for the already over-taxed poison control system so they expand

their current training to include all-hazards preparedness and develop successful linkages with appropriate agencies.

In response to the call for improved all hazards response, coordination and collaboration, it is vital that the department of homeland security, emergency management, public health, and the poison control system come to the table to begin these important discussions. Only then can we begin to address questions such as what is needed to promote consistent messaging, how many more people do we need to provide sufficient support for the call system in a national disaster or outbreak, and what are the weaknesses in our current telephone answering system and infrastructure? Until we have an evidence base that explains the opportunities that exist and the gaps we must fill to improve disaster and emergency response we are no further along toward improved security.

---

[1] U.S. Department of Homeland Security (DHS), *National Strategy for Homeland Security* (2002), http://www.dhs.gov/xabout/history/publication_0005.shtm.
[2] Ibid., 11.
[3] Agency for Healthcare Research and Quality, "Addressing Surge Capacity in a Mass Casualty Event: Bioterrorism and Health System Preparedness," *Issue Brief 9* (October 26, 2004), http://archive.ahrq.gov/news/ulp/btbriefs/btbrief9.htm.
[4] L. Artalejo and others, *Report for Health Resources and Services Administration: The Value of the Poison Control Center* (Washington, DC: 2008); A. Robinson and W. Newsletter, "Uncertain Science and Certain Deadlines: CDC Responds to the Media During the Anthrax Attacks of 2001," *Journal of Health Communication* 8, no. 4, sl (2003): 17-34; World Health Organization (WHO), *Outbreak Communication Guidelines* (2005), http://reports.typepad.com/pandemic_plan/2005/12/risk_communicat.html.
[5] Agency for Healthcare Research and Quality, "Addressing Surge Capacity in a Mass Casualty Event."
[6] D.A. Shore, "communicating in Times of Uncertainty: The Need for Trust," *Journal of Health Communication* 8 (2003): 13-14.
[7] R.J. Wray and others, "Communicating With the Public About Emerging Health Threats: Lessons from the Pre-Event Message Development Project," *American Journal of Public Health* 98, no. 12 (2008): 2214-22; Shore, "Communicating in Times of Uncertainty;" WHO, *Outbreak Communication Guidelines.*
[8] J.P. Koplan, "Communication During Public Health Emergencies," *Journal of Health Communications* 8 (2003): 144-45; Robinson and Newsletter, "Uncertain Science and Certain Deadlines."
[9] Artalejo and others, *Value of the Poison Control Center*; R.J. Geller, Z.N. Kazzi, and V.A. Yeager, "Improving Disaster Communication: The Role of Poison Centers in Public Health," Satellite Broadcast, Alabama Department of Public Health, July 22, 2008; V.A. Yeager, Z.N. Kazzi, and L.C. McCormick, "Poison control Centers – The Missing Link in Disaster Preparedness," paper presented at the Public Health Preparedness Summit, Atlanta, GA, February 2008.
[10] F. Bunn, G. Byrne, and S. Kendall, "The Effects of Telephone Consultation and Triage on Healthcare Use and Patient Satisfaction: A Systematic Review," *British Journal of General Practice* 55, no. 521 (2005): 956-61; L.E. Felland and others, *Developing Health System Surge Capacity: Community Effort in Jeopard*y, Research Brief No. 5 (Center for Studying Health System Change, June 2008), http://www.hschange.com/CONTENT/991/991.pdf; Agency for Healthcare Research and Quality, "Addressing Surge Capacity in a Mass Casualty Event."
[11] WHO, *Outbreak Communication Guidelines.*
[12] Wray and others, "Communicating with the Public;" G.M. Bogdan and others, *Health Emergency Assistance Line and Triage Hub (HEALTH) Model.*
[13] Ibid.

[14] Felland and others, *Developing Health System Surge Capacity*; Bogdan and others, *Health Emergency Assistance Line;* Agency for Healthcare Research and Quality, "Addressing Surge Capacity in a Mass Casualty Event."
[15] Artalejo and others, *Value of the Poison Control Center;* Geller, Kazzi, and Yeager, "Improving Disaster Communication"; S.E. Harcourt and others, "Can Calls to NHS Direct Be Used for Syndromic Surveillance?" *Communicable Disease and Public Health* 4, no. 3 (2001): 178-88.
[16] In November 2006, Alexander Litvinenko, a former Russian federal security service agent living in England and publicly accusing the then Russian President, Vladimir Putin, of fraudulent conduct, fell ill with stomach troubles. Over the course of the following twenty-two days, Litvinenko exhibited signs of acute radiation sickness and eventually died. The day he died, Britain's Atomic Weapons Establishment determined that he was poisoned with Polonium-210. (Spector, 2007) There were a number of locations where the poisoning could have taken place, which were then investigated by the British Health Protection Agency. M. Specter, "Kremlin, Inc.," *The New Yorker,* January 27, 2007, 50-63; J.W. Stather, "Invited Editorial: The Polonium-210 Poisoning in London," *Journal of Radiological Protection* 27 (2007): 1-3.
[17] HPA, "Update on Public Heatlh Issues Related to Polonium-210 Investigation" (December 28, 2006), *http://www.hpa.org.uk/web/HPAweb&HPAwebStandard/HPAweb_C1195733734356*.
[18] HPA, "Public Health Response to the Poloniu,-210 Incident" (September 19, 2007), *http://www.hpa.org.uk/webw/HPAweb&HPAwebStandard/HPAweb_C/1195733725705?p=1171991026241*.
[19] J. Fisher, Alabama Poison Center, personal communication with author, August 13, 2009.
[20] Geller, Kazzi, and Yeager, "Improving Disaster Communication."
[21] F.M. Burkle, "Measuring Pandemic Preparedness, Containment, and Effectiveness in Communities, States and Across Nations, *Proceedings from national Association of County and City Health Official's Preparedness Summit,* Atlanta, GA, February 2008.
[22] A.C. Bronstein and others, "2007 Annual Report of the American Association of Poison Control Centers' National Poison Data System (NPDS): 25th Annual Report," *Clinical Toxicology* 46, no. 10 (2007): 927-1057.
[23] Geller, Kazzi, and Yeager, "Improving Disaster Communication."
[24] T.R. Miller and D.C. Lestina, "Costs of Poisoning in the United States and Savings From Poison Control Centers: A Benefit-Cost Analysis," *Annals of Emergency Medicine* 29, no. 2 (1997): 239-245; Artalejo and others, *Value of the Poison Control Center.*
[25] DHS, *National Strategy* (2002). 42.

THE DEPARTMENT OF HOMELAND SECURITY INITIATIVE FOR COMMUNITY EMPOWERMENT AND SECURITY: A COMMUNITY-BASED APPROACH TO HOMELAND SECURITY: INITIATIVE, RESPONSIBILITY, AND ACTION

George Ewing
Client Development Officer, CitiFinancial Auto

The answer to preventing terrorist attacks within the United States, reducing America's vulnerability to terrorism, minimizing the damage, and recovering from attacks that occur in our Homeland, exists within America's vital and vibrant communities. I suggest that President Obama's administration consider the establishment of a Department of Homeland Security Initiative for Community Empowerment and Security (ICES) that focuses upon utilizing (and improving upon) the existing relationship between the Department of Homeland Security and local populations, schools, and businesses through city government. This three part initiative will foster a critical bond between the Department of Homeland Security and communities all over the United States. The Initiative for Community Empowerment and Security will provide for the establishment of local DHS prevention, intervention, education, and recovery programs through a series of partnership-based initiatives implemented by DHS through municipal governments.

THE DEPARTMENT OF HOMELAND SECURITY (ICES) SAFE COMMUNITY PROGRAM

The Department of Homeland Security (ICES) Safe Community Program aims to strengthen the relationship between local populations, city governance, and Homeland security. This program will include the facilitation of community educational activities to inform local populations about potential vulnerabilities, prevention, and sustenance in the event of an attack or natural disaster and recovery measures. Activities include the establishment of a homeowner and tenant reporting system and criminal background check program for landlords. The local population program will emphasize inclusion of members of the community and education programs focused on how to make communities safe, enabling individuals to learn about the empowerment initiative and other DHS programs already in place.

In the days following the 9/11 attacks, communities across the United States shook as it became evident that the terrorists responsible for the most destructive act of terrorism on U.S. soil had lived and thrived unchecked in communities throughout the United States. Members of these "sleeper" cells purchased and used mobile phones, completed email transactions at local libraries and businesses, shopped in grocery stores, and rented homes in both urban and suburban settings. Due to the social mobility, economic conditions, and immigration challenges being experienced in communities throughout the nation, there has been an unprecedented disconnect in the fabric of community interaction and transparency. Few tenants in apartment complexes know their neighbors; in suburbs across the Homeland, individuals share communities with virtually no interaction or knowledge of what is happening in the dwelling just next door. Quite often, they live in fear and apprehension. If community awareness and security are to improve, municipalities must be privy to what is taking place within their jurisdictions or areas of responsibility. The ICES local population program will facilitate local government responsibility and community involvement in their own safety and ability to handle an attack or disastrous event should one occur. The Local Population Program will host events including community-wide "Know Your Neighbor" education campaigns, community safety and security competitions, firefighter and police education programs, community forums on maintaining safe and secure communities, and a unique Homeowner/Tenant reporting system which will buttress community-building and responsibility.

Attempting to create a more secure or transparent community will require much more than simply obtaining corporate buy-ins, lists of tenant names to be compared to databases, or broad community directives. To accomplish community ownership of these and other security and safety initiatives will depend solely on the engagement and the education of the populace. Once the local government, law enforcement, and corporations have agreed upon their roles and responsibilities, there will be a need to debut these initiatives to the community. Funds garnered from Homeland Security grants could aid in underwriting interactive community-wide events that would highlight the community-based initiative programs available to the community, provide a venue for discussions about the state of security within the community, and be a place to share ideas and opinions about the programs and their efficacy.

In addition to these events being laced with information and educational activities, they will also be the catalyst for dialogues between groups and individuals about their own security and community concerns. The question of transparency in communities and teaching communities to be alert to potential security and safety situations will be accomplished through the "Know Your Neighbor"

aspect of the initiative. Communities that have a connected and aware population are more secure and will better ensure the safety of the nation. Providing funds to facilitate informal community meetings, gatherings, and neighborhood celebrations will strengthen the security for the community as individuals begin to understand the dynamics of their neighborhoods and become more involved with their community group. These events will also afford the community a greater awareness and enhanced perspective of suspicious or abnormal activity taking place in their neighborhoods. By being inclusive of all groups and choosing diverse venues (churches, synagogues, mosques, community centers, etc.), the activity-based community forums will foster communication and understanding amongst ethnicities, religions, and cultures as well.

"KNOW YOUR NEIGHBOR" PROGRAM

Currently, homeowners are required to report their accumulation of property, home improvements, and structural changes to their dwellings annually, a crucial aspect of data collection that affords a city or town a snapshot of the fabric of its community. In many municipalities, landlords must obtain a license to rent property they own. However, there are no requirements for the landlord to provide the names of prospective or actual tenants to city or to law enforcement officials. Today, the law requires that an individual's name and credentials be compared to the Office of Foreign Assets Control (OFAC) list to make certain that the individual is not involved in money laundering, in support of a sanctioned government, or a suspected terrorist when making financial transaction at a bank, financial institution, or even during an automobile purchase. When renting a home and establishing new residency in a community, there are no steps taken to ensure that a tenant's identity is verified or that they are who they say they are. A comprehensive community rental reporting initiative would afford more transparency in communities, allow municipalities to understand their community demographics, and ensure a greater level of security and response in the event of an attack or natural disaster.

THE DEPARTMENT OF HOMELAND SECURITY ICES SAFE BUSINESS PROGRAM

The Department of Homeland Security ICES Safe Business Program aims to strengthen the relationship between local governance (Mayor and/or City Council), community businesses, and Homeland security to coordinate, cooperate, and maintain community security and educate corporations on how the community-corporate relationship can make communities prosper and businesses grow while creating safer cities. This program will include educational programs on prevention, sustenance and recovery and emergency and suspect reporting procedures for business employees in the event of a terrorist attack or natural disaster.

Over the past decades, community policing and law enforcement budgets have been exhausted by escalating crime and a lower tax base. Community businesses and corporations benefit from the human capital of the workers and consumers who reside in the municipalities in which they operate and earn substantial profits. Many terrorist attacks committed around the globe have been directed at businesses, hotels, and other for-profit entities. The ICES Business initiative is a program designed to aid businesses (who have a vested interest in community security) in coordinating and cooperating with the municipalities to help maintain community security and create formal plans of response to terrorist acts and natural disasters.

The first aspect of this initiative simply begins with the fostering of open lines of communication and a formal dialogue between city officials and business managers about community security issues and challenges. This reciprocal exchange of information will benefit the security of the community and afford an opportunity to develop coordinated plans between business and local government in the event of a natural disaster or terrorist attack. Private business has historically done a superb job at training and marketing ideas and creating solutions. Corporations will be vital in the education of their employees about emergency preparedness, reporting lines and procedures for potential Homeland security issues, and emergency measures in the event of a terrorist act or natural disaster.

Many of the largest employers in communities are big box retail stores and other minimum-wage income based service industries that have extended or nearly twenty-four hour a day operating schedules. Not surprisingly, late night hours (when many of these retail outlets are operating) happen to be the prime time for criminal and violent acts to occur within communities. With fewer police available and crime escalating due to a deteriorating economy, it is necessary to turn to corporate entities to ensure greater community policing and security. These businesses already have Closed Circuit Television systems that monitor their parking lots and interiors, but more involvement needs to be taken in policing the areas of the community surrounding the business districts. There is also a massive incongruence between municipal, neighborhood, and corporate perceptions and attitudes about community security that needs to be approached and acted upon.

Corporations want a safe and protected environment in which to conduct business and they should realize that if consumers feel threatened or exposed, they will choose not to participate in the economy. At the same time, while most law abiding citizens are at home in bed, it is the employees

of these same corporations providing minimum-wage jobs that are out and participating in the late night activities in communities. If the corporations chose to help provide funds to aid in the policing of their communities, and educated their employees about community security, they would be providing a service for both their associates and their patrons. In addition, there would be an entirely new level of policing and monitoring in place that would be available to observe and report strange, suspicious, or potentially malicious behavior.

THE DEPARTMENT OF HOMELAND SECURITY ICES SAFE SCHOOLS PROGRAM

The Department of Homeland Security ICES Safe Schools Program will strengthen the relationship between local governance, community schools, and Homeland security through emergency preparedness education, reporting methods and procedures activities, and community-based youth initiatives and programs. The schools-based program will also include educational activities to prepare for events such as natural disasters and other emergency situations.

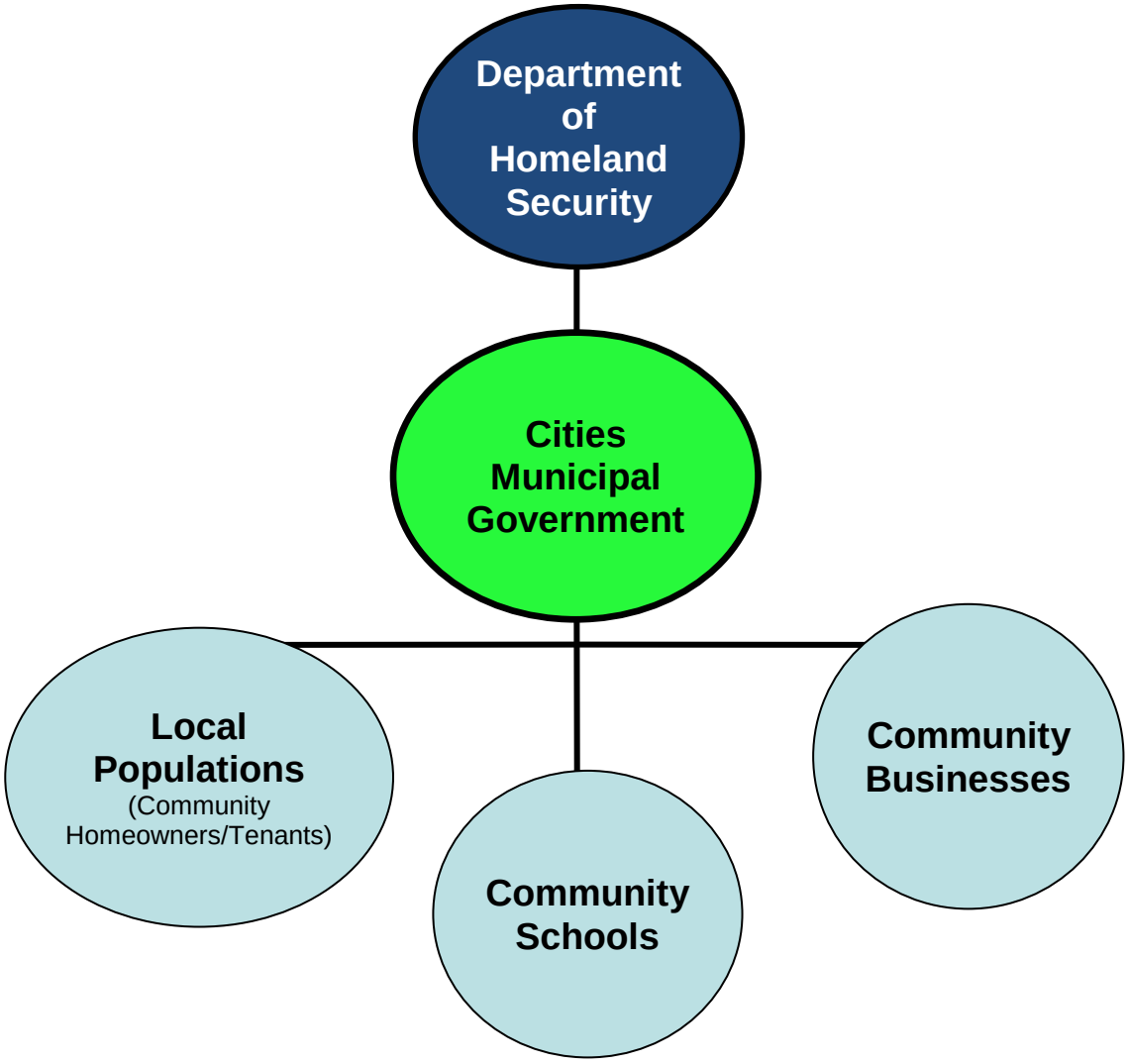
Schools are a major component in the fabric of every community. They are more than the epicenter of education, but are also a space where sporting events, after-school activities, and community events are held. School systems in many communities have historically done an excellent job incorporating ancillary programs into their curriculums which have included conflict resolution training, diversity programs, and other important initiatives that have reduced violence and educated students on a myriad of topics. Observing the success of these programs, the next logical step to disseminating the message of DHS and the ICES initiative with local government would be the facilitation and implementation of the third aspect of the program. This school-based program develops a solid relationship between the safety and security initiatives of DHS, the municipal government, and the local school system.

Local governments would charge local schools to deliver the message of emergency preparedness and procedures for emergency situations in the event of natural disasters in an interesting and informative battery of class projects. These projects could be delivered in tandem with science, natural science, and biological science curriculums. For older students, terrorism education (including reporting lines and community procedures during potential or actual terrorist events) could be taught inclusively with civics and government courses. The schools could also provide literature to be distributed to parents concerning these same themes (delivered to the home by students) to be discussed and shared in the family setting, further reinforcing the importance and validity of the program themes.

CONCLUSION

The key to improving Homeland security lies within the nation's greatest asset, its proud and incredible people and its pulsating communities. The Department of Homeland Security, through funding and consultative assistance, can improve security in neighborhoods by fostering corporate and municipal partnerships that make safety, security education, and policing the responsibility of all actors in the community, not just law enforcement agencies. The community focused segment of the ICES program will create a more aware, strong, and tightly-knit community. A comprehensive tenant reporting program will allow citizens to understand more about who is actively participating and residing in their communities, while also allowing local governments the ability to utilize that data to keep communities safe and secure. Community schools will become another conduit of training concerning DHS and municipal security initiatives providing another layer of education that involves parents, teachers, and the community. As with any new initiative, the success of these programs will be determined by the activity-based education schemes conducted throughout the community. These events, which should be supported by both business and government, will be the necessary catalyst to obtain "community ownership" of the program, greater community awareness, and increased security. The nation's communities are the very frontlines of Homeland security and with the institution of the ICES initiative there will be a reduction in terrorist threats and an increase in community preparedness and planning for the disasters, natural or man-made. The Department of Homeland Security Initiative enables President Barak Obama and his administration to bring lasting and positive change to our neighborhoods and provide greater protection for our most important resource, our communities.

The Department of Homeland Security
Initiative for Community Empowerment and Security Model



A National Information Policy

Andrew Faltum

Military Lead Analyst, Alion Science and Technology

In the wake of the 9-11 attacks, as America began searching for answers, it became clear that the means of sharing critical information between the various organizations engaged in protecting us were woefully inadequate. With the many initiatives put forth since then, there has been improvement in the timeliness and quality of information sharing, but there is still no comprehensive, methodical and disciplined approach to overcoming the institutional and cultural barriers to more effective information sharing. Without such a long term approach, we may be inadvertently increasing our risk – we may be moving away from a "risk avoidance" approach to information sharing to a "risk acceptance" approach in which we have not properly weighed the risks versus benefits involved. This paper will lay out a recommended approach to a comprehensive national information policy that would be based on principles of risk management. The key points are:

- The Federal Government must develop a comprehensive national information policy that provides an overarching framework for developing specific guidance in areas such as information security, classification and declassification decisions, and information sharing with international, state, local, tribal, non-government partners and the public.

- This information policy must be based on a rational risk management methodology that balances need to know against the need to protect. Risk management, for the purposes of national policy, must include risk analysis and risk response processes.

- Risk, as a commonly used but not commonly understood term, is composed of criticality (sometimes referred to as "impact"), vulnerability, and threat (includes all hazards).

- The proposed risk management methodology can be developed on the basis of existing analytical models. The key concept is that, under the national information policy, content should regarded as an asset and that risks can be determined in a similar fashion to the way we determine risk for other assets, such as infrastructure.

Currently, there are a multitude of legal, policy and procedural approaches within the federal government that deal with the protection or dissemination of information. The levels of protection

afforded to some categories of information are in fact based on assessment of risk, although in practice this is not often recognized. For example, under Executive Order 12958 "Classified National Security Information" (amended by EO 13292) the differences between Top Secret, Secret and Confidential information are based on the level of potential damage to national security, i.e. the *risk* incurred, if the information is compromised through unauthorized disclosure.

Even though there may be inherent risk decisions underlying many of our information policies, they are not based on a consistent approach between communities of interest. With no common terms of reference, criteria for comparison or analytical framework by which to make informed decisions, many of the current information sharing initiatives fixate on the processes and information technology solutions required and not on the information content itself. The information *content* is the whole point of the information sharing process. We cannot convince partners to share their information unless we can assure them that their information will be protected appropriately.

What is needed is an overarching information construct, that is, a comprehensive National Information Policy, by which different communities of interest can relate to each other on the basis of common understanding. Left to their own devices, communities of interest have often shown that they develop their own terminology, processes and procedures. The first necessary step to addressing this multiplicity of approaches is to establish national policy that serves as capstone guidance. The development of such policy, in turn must be based on an analytical approach to risk management. (This risk management process will be further explored in later sections.) The proposed approach would:

- Balance the need to share against the need to protect, enabling true risk management, not just risk avoidance or risk acceptance.
- Form a sound basis for establishing protection criteria, e.g. security classification guidance, handling unclassified but sensitive information, privacy and medical data safeguards, protecting proprietary commercial information, public affairs guidance during times of crisis, etc.
- Provide a means to examine policy and guidance to ensure a consistent approach to both information security and information sharing.
- Ensure that actual information sharing and protection requirements drive technology solutions instead of the current situation, where our technology has created the possibility of being inundated with too much irrelevant information instead of providing the right information to the right recipients, at the right time, i.e. true knowledge management.

- Establish a common analytical framework for interaction with information sharing partners, e.g. Department of Homeland Security, Department of Defense, state and local governments, foreign governments, non-governmental organizations, the private sector, etc.

It is important to stress that this framework will not provide all the specific guidance needed for particular circumstances, but that specific guidance for an individual community of interest must be consistent with, and derived from, the national capstone guidance. Once a national level construct has been established, the next step is the rationalization of other information policies to ensure that they are consistent with national guidance, do not conflict with other communities, and are not duplicative or inconsistent. This will be a long term process, but we must start now. We have avoided dealing with the larger issues in the interest of obtaining near term improvements. While this has had some benefits, it is time to take a more deliberative approach before our stop gap measures become unmanageable. The first step is to adopt a consistent risk management process.

Risk management is a widely used term that means different things to different communities of interest, usually within a particular context. Within the Department of Defense, the mission assurance concept developed by the Assistant Secretary of Defense for Homeland Defense and Americas Security Affairs (ASD(HD&ASA)) can serve as a starting point for a national risk management process. Under this mission assurance concept, risk management includes risk assessment and risk response. This approach can be extended to the national level.

- Risk assessment is a systematic, unconstrained, examination of risk that includes:

  - Determination of criticality based on operational impact. In some risk management processes, criticality is often identified as the *impact* of the loss or degradation of an asset. Within DOD, criticality is determined by examining the missions assigned, the tasks necessary to complete these missions, and the impact of loss or degradation of capabilities provided by various assets. Many other organizations, including the private sector, also have "mission statements" and "business processes" that can be related to criticality.

  - Assessment of vulnerability based on common standards. A widespread problem within government and the private sector is the lack of commonly agreed upon assessment criteria and methodologies.

  - Identification of potential threats and hazards. Within Dodd there is often a distinction made between threats, which are seen as deliberate actions that may be taken by an adversary, and hazards, which may include natural disasters or accidents. These related

ideas are often combined for the purposes of risk analysis under an "all hazards" terminology.

- Risk response is a tradeoff analysis between operational impacts, technical capabilities and available resources that can be used to develop recommended courses of action. Generally, the response is to remediate the vulnerability, mitigate the effects, or accept the risk. Within the context of the National Information Policy, this would equate to the changes in policy and procedures that are being called for now in many information sharing initiatives. The difference is that under the proposed approach, there would be sound analytical processes and methods to derive such changes.

There are many analytical processes and methods that could be adapted to weigh information content risk, such as network theory and the methods used by DOD for weapons effects. An example would be the methods used to develop the Joint Munitions Effectiveness Manuals, which can be used to determine weapons effects or survivability. Once the need for a common analytical framework has been accepted, candidate processes and methods could be examined in greater detail in subsequent implementation actions. There are also a number of recommended steps that can be taken immediately to establish both the National Information Policy and the supporting analytical framework. These include:

- Establishing an informal group from government, the commercial sector and academia with experience in information related professions, e.g., news media, intelligence, public affairs, to survey existing information sharing methods, risk management processes, network theory, vulnerability assessment processes, etc. to identify possible candidates suitable for an information risk management process. (Note: this group should *not* include *information technology professionals* at this point. The reason is that there is an unfortunate tendency of organizations to skip the very necessary first step of examining information content needs and jump to developing technical solutions to sharing information without considering the *what* and *why* of information sharing.)

- The initial survey output from the informal study group could form the basis for further, more focused effort that may take the form of government or academic research into information process modeling. (Note: there may already be relevant ongoing efforts, such as in the areas of intelligence fusion or suspicious activity reporting, that could be leveraged or expanded upon to a broader context.)

- A parallel effort should focus on risk management process modeling and development of common criteria and terminology. This effort should be complementary to the information process modeling.

- The recommendations from both the risk management and information process groups should be handed off to the Director of National Intelligence to incorporate their findings into a draft National Information Policy. Under the overall supervision of the DNI, there should be specific actions to draft a national information policy and timelines for completion.

- Once the National Information Policy is in place, those government organizations that are proponents for related policies, e.g. information security, public affairs, etc. would be tasked to review and revise their guidance as necessary to conform to the national information policy.

The need for change in the way we approach information sharing, once accepted, must be implemented by means of the proposed National Information Policy. This policy in turn, must be formed on the basis of consistent, logical analytical processes and methods that examine information content. We should be under no misapprehension that these recommendations can be implemented immediately or that there will not be contentious issues that may need to be resolved as we develop our courses of action. However, the National Information Policy will allow us to establish orderly, effective information sharing and will have significant benefits in many other areas in the future.

SAVING THE INTERNET OR "WHO ARE YOU GOING TO TRUST"

Harry Haury

Chief Executive Officer and Founder, NuParadigm Government Systems, Inc.

The threats to our country posed by the inappropriate trust of systems, networks and the Internet are real and the risks are growing in number, frequency, and consequence every day. The weaknesses of the current systems and "known" exploits have grown to the point of near absurdity, yet the only options currently available at this point are to deal with these mounting consequences while the losses continue to mount and the sophistication of the attacks continues to grow. In the course of any discussion it is impossible to cover every vulnerability with any meaningful solution given the almost infinite possible system permutations. But it is useful to discuss what is of concern and what the significance might be to an improperly protected system. Risks can be broadly categorized into the four attacker objectives with our current systems:

1. The adversary wants to "exfiltrate" or steal important information. This can range from personal information, such as passwords, medical records, and credit card numbers, to state and corporate secrets. Any sensitive information stored on a network or computer it is a potential target. The purpose of the adversary in this type of attack can range from general mischief, to identity theft, and even to state based warfare.
2. The perpetrator would like to forge information to allow them access to systems for the purposes of theft, sabotage, denial, or spying.
3. Capture or misappropriation of systems with objectives ranging from free use of computer systems capabilities to setting up massive botnets to facilitate future denial of service attacks.
4. Direct denial through the sabotage of critical network infrastructure or the flooding of networks with excessive amounts of traffic.

But what do these vulnerabilities mean to the country? Let's examine the implications through some simple scenarios:

1. **Christmas attack 2009.** Our retail operations in a continuing effort to cut costs migrate more and more to the Internet. Some major corporations are one hundred percent dependent upon Internet based sales and many companies now rely on the Internet for as much as 30 percent of their total annual sales. During the height of the Christmas buying season hackers employ a sophisticated distributed transaction attack automating the ordering of hundreds of millions of items across the Internet that are fraudulent transactions. This leads to a catastrophic chain of events:
    1. Credit card holders refuse to pay.
    2. Retailers become embroiled in recriminations about responsibility and liability for tens of billions of dollars worth of product.
    3. Credit card companies that have guaranteed Internet transactions for consumers go bankrupt.
    4. Companies facing a complete failure of trust in the transactions across the Internet 'temporarily' stop using the Internet or have to massively retool their online security processes losing important sales.
    5. Consumers stop exposing personal data across the Internet because of fear about information being stolen further curtailing sales.
    6. Declining Internet sales, massive fraud losses, hesitant consumers and lack of remaining 'brick and mortar' capacity combine to bankrupt hundreds of companies ranging from Internet florists to EBAY and Amazon.
    7. The already bad lingering recession from the previous year deteriorates into a full blown depression.
2. **Escalating tensions Winter 2010.** After years of quietly building silent Botnets another world power reaches the limit of what it declares is the unlawful arrogant hegemony of the United States of America and it unleashes attacks on the Internet itself. Because of the money invested and the stealthy work over years of patient attack all major networks are flooded with traffic. This is timed to coincide with the attacker's strategic attack on several critical transcontinental fiber hubs with simple crews disguised as utility workers cutting a number of very important fiber optic cables. The nation's telephony and network infrastructure has been allowed to converge to the point that many commercial and government networks share

critical bandwidth. Suddenly access to networks ends in many places. VOIP telephony is completely disrupted. Critical local network loops are knocked out. Point of Sale terminals cannot connect to credit card clearing systems or integrated supply logistics systems. The economy comes to a screeching stop for 10 days. Critical infrastructure from SCADA systems to first responder systems collapse resulting in dangerous shutdowns of large portions of the energy grid during the dead of winter. Hundreds of thousands of persons are displaced to emergency shelters. The new economic recovery sputters and fails. Thousands of citizens refusing to leave their homes die of exposure. The economic losses from denial of use and indirect infrastructure damage rapidly escalate into hundreds of billions of dollars. The Botnets have been built to heal themselves and to re-infect computers in layers so that it takes months of effort to clean the systems up and restore normal functioning to the Internet. Due to emergency segregation of the networks to restore some basic high priority capabilities, large segments of the Internet no longer have adequate capacity causing significant economic dislocation in the areas affected.

3. **Military espionage.** Net Centricity continues to build and inadequate systems boundary protections allow the networks to be instrumented with silent viruses, backdoors, sophisticated man in the middle proxies, and remote control software. The systems are being used to gather data about military operational capability, exfiltrate state secrets and position electronic warfare sentinels throughout our networks. Constant probing of our networks has heightened out alert status but many successful hacks are undiscovered. Without explanation new capabilities start showing up at an alarming rate in the opposing military services and during a controversial high profile military incursion red force and blue force tracking systems supporting command and control are suddenly compromised. Joint task list assignments target certain elements of coalition forces that are outside our direct command and control space so the compromise goes unnoticed for critical minutes while high altitude and standoff assets are brought to bear on friendly forces and a few of our own 'covert' assets. There are thousands of friendly casualties including the loss of several capital ships of friendly navies and numerous friendly aircraft. In

addition, there is a fundamental loss of confidence in the entire information/command chain resulting in the loss of our information enabled agility. Lengthened decision cycles and the as yet undetected active exfiltration of C4ISR data allows our own networks to become giant sensors for our adversary. Suddenly the advantage we had in our decision turning radius is lost to the opponent with all the resulting effects to our effectiveness on the battlefield.

The threats posed by these hypothetical scenarios are very real yet we tend to ignore the trends that make these things possible because they have not happened yet. The only things standing between us and these types of attacks are the imagination, patience, resources, sophistication and dedication of our opponents. The current state of our systems' security are clearly not the barrier they should be. Reflect for a moment on whether a determined well funded adversary would have the technical means to pull these attacks off. To date many attacks have been by criminal groups seeking personal profit or by individuals merely seeking bragging rights. State sponsored activity is out there, however, and they are not tipping their hands anymore than necessary as they probe our computers and where they successfully penetrate, we may not even have the capacity to detect the vulnerability. It is time to take these issues seriously and make meaningful and comprehensive efforts to protect our networks, systems and data with the highest priority. The focus must be on the development of effective information assurance capabilities that are cost effective, manageable, and massively scalable to provide for:

1. The trustworthiness of identity and authorization with sufficient granularity at the level of assurance necessary to insure that the applications affected manage access appropriately.
2. Elimination of forgery across the protected systems, ranging from packet spoofing to transaction forgery, through strongly protected physical guards, filtering devices and cryptography.
3. Building of systems that can be trusted to exclusively execute applications and instructions that are known to be authentic and approved.
4. Creation of intelligent and deterministic filtering and firewall capabilities that

terminate traffic that does not have the appropriate authorization or 'rights' to the privileges it is asserting. This has to be functional at any layer of the network stack including the application layer.

5. Protection of the core network routing infrastructure and common services such as DNS and BGP from external attack or compromise from any source.
6. Implementation of community separation to allow virtual application networks to control the sharing of common services and infrastructure information between the community participants in a trustworthy manner while in turn limiting the exposure to data exfiltration to those outside the community boundary.

Reflect for a moment……. are any of these scenarios technically infeasible? Are we comfortable with our primary protection being the lack of will, imagination or resources of those that wish us harm?

END TO END ASSURANCE REQUIRES AN END TO END TRUST FRAMEWORK

The vulnerabilities to modern computer systems for these types of attacks easily number in the tens of thousands. The reasons for these vulnerabilities are simple:

1. Existing systems simply were not designed for secure network based computing.
2. The non-deterministic nature and complexity of current environments make it impossible to protect against the determined attacker that comes at you with attacks that are exploiting the huge number of possible compound attack vectors exposed by these thousands of vulnerabilities.
3. There is no concept of enforceable trust and assurance across these systems that is able to transcend the original concepts built in isolated hierarchical legacy systems. These systems made broad assumptions in their original design that cannot be trusted in this new environment. In fact, given the vast growth in the range, scope and expectations of the user community defined under the auspices of "information sharing", they may not even be applicable.

THE NEED FOR A NEW ARCHITECTURAL APPROACH TO TRUST MANAGEMENT

What is desperately needed are trusted mechanisms for conveying and enforcing rules intersections in these information sharing driven systems. Trust rules, otherwise known as policy, must govern the intersection of by examining the "meta-characteristics" of data, which describe the actions being taken and the participants involved, so that actions can be limited to only those allowed under the conditions that exist at that time at that point of decision for that process. These "trust guards" require something new and outside current architectural wisdom.

Controlling trust in this manner requires a series of decisions to be made at each of a series of critical steps in a process in order to insure the necessary controls are in place to insure rogue requests are not executed. In current common parlance these would be called Policy Enforcement Points (PEPs), but this paper is calling for broadening the overall policy enforcement concept to include the entire policy infrastructure behind making these decisions. This architectural approach therefore generically refers to the decision intersection of policy based meta-characteristics as "Decision Points" in that they represent the many process points where a decision has to be made as to how to proceed (see Figure 1). This is a distinction from a Policy Decision Point (PDP) in current definitions which typically provide only a decision at the entry to the process. Decision Points of this type are characterized by potential discontinuity or asymmetry existing at numerous points along a system process whether acknowledged or not. These are simply the many cases where the character of the 'stuff' happening on one-side of a connection is different than the character of the 'stuff' on the other-side. These points of discontinuity are the core issues behind the vulnerabilities in the "system of systems" described above and these are a proliferation of these Decision Points make up the majority of the modern computing environment.

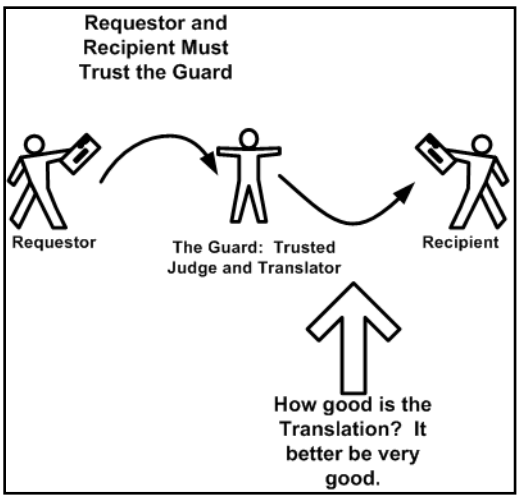


Figure 1 - Decision Points

The inability to control the resolution of these Decision Points is behind the proliferation of trust "holes" which plague the industry. This threat is also being significantly compounded daily with the ongoing growth in multi-step workflows between incompatible systems. These distributed Decision Points require context translations between systems which compounds the level of risk. These systems, which are often typically inadequately guarded individually already, are now required to establish some compatible means of exchanging information before they can even begin to determine if it is okay to do so. Exchanges of this type should be heavily guarded from a control and auditability standpoint and yet are often not even given special handling, much less scrutiny, with regard to trust enforcement under the current architectural "wisdom" (see Figure 2). This must change.

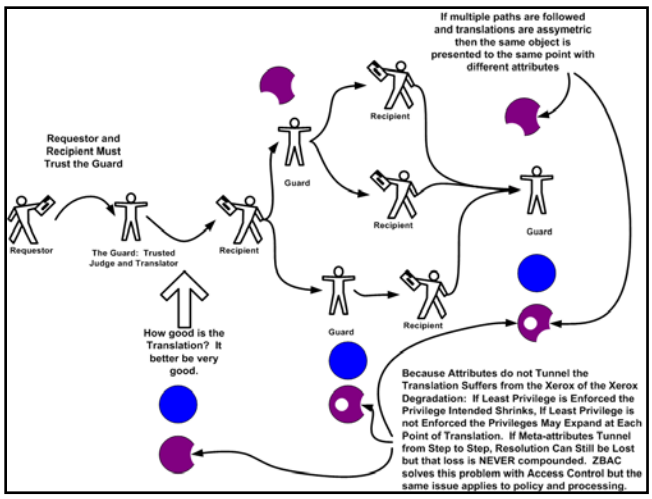


Figure 2 - Context Exchanges Complicate the Problem

In order for a system to be governed in this manner, these Decision Points, and especially those distributed between system boundaries, must be protected by "Trust Guards" that can enforce the validity of the actions being called for, the participants in the system, the infrastructure being used, and the meta-characteristics or state of the information flowing between all of the systems at any time (see Figure 3).

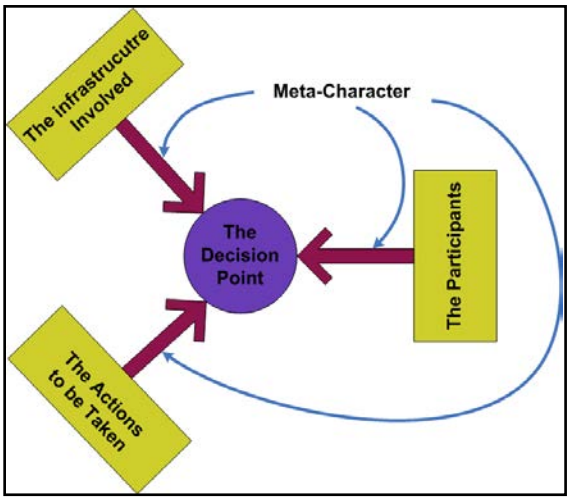


Figure 3 -Anatomy of a Trust Guard

There are thousands of known and theoretical vulnerabilities that need to be addressed and the costs involved will be significant. The failure to act in an effective manner, however, has already put our national security and economy at risk. Every day that goes by without a response only increases these risks and the costs needed to respond. These problems are solvable. It is only a question of resolve and good intent. A comprehensive multi-layered program to protect the country's systems should be undertaken immediately starting with the development of new technologies aligned with the realities of net centricity, information sharing and the Internet based on the trust structure described above. These systems must also:

- Meet stringent standards and objectives
- Be commercially available at a reasonable cost
- Have an extremely high level of assurance applied to protecting their critical data and functional assets.

The level of vigilance must also be increased significantly to specifically target new exploits and vulnerabilities which are being identified on a continuous basis. Only through a comprehensive and coordinated effort by government and industry can there be sufficient progress made to confront the profusion of current and emerging threats.

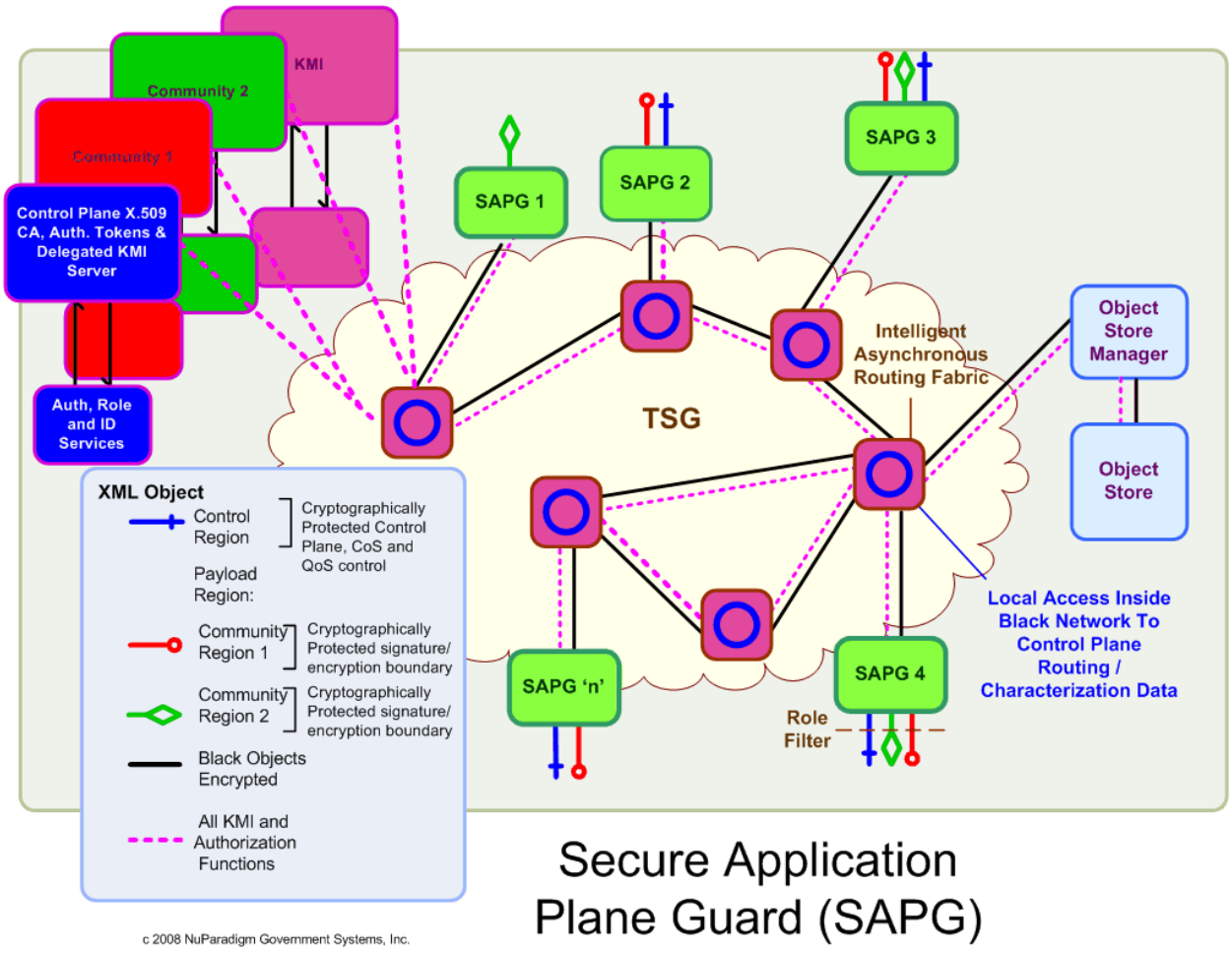


Figure 4 - A Vision of the Future: The Secure Application Plane

BUILDING A CENTRAL INTELLIGENCE REGISTRY

George Pugh

President, George Pugh & Co.

Mr. President, the core intelligence functions are collection, analysis and action. A Central Registry would improve the entire intelligence cycle and related decision support. The goal is to ensure that the raw data or analysis is available to those that need it to ultimately support your decisions. A Rand study notes:

> To summarize, two overarching concerns with domestic intelligence action are (1) continuing concern about information sharing across the intelligence–law enforcement seam; and (2) the effectiveness of information sharing across different levels of government. [1]

Information sharing is not restricted to purely domestic intelligence alone but must include the international sphere where enemy funding, planning and training take place. Many believe that reorganization of the intelligence function is the only way to correct these problems. Reorganization is a blunt instrument, which might well disrupt critical functions and relationships when most needed. At this time we simply don't know what good organization would be.

A better approach is to improve information sharing rather than disrupting time tested processes. A Central Registry could be implemented with minimum disruption while improving system wide functions. With so many interested organizations it is simpler to have a two step process, from producer, to registry and registry to user than in effective current practice. It is the same reason we use money rather than barter: in this case a two step system is more efficient than a one step one.

Creating a Central Registry is not a stop-gap, but will create an orderly system of data control and sharing doing no violence to existing organizational work, while reducing duplication of effort.

THE WHAT AND WHY OF A CENTRAL REGISTRY

History has shown, perhaps starting with the Domesday Book, that a complete inventory is necessary before any proper management of any entity is possible. A Central Registry provides that

environment. It is easier to audit one transaction cycle than many, and prevent management override for political or institutional purposes. A Central Registry will also permit the efficient implementation of the following controls:

1. Only vetted information will enter or leave the system, since inventory control rests with the registry, and ultimately with the Commander-in-Chief, rather than component organizations.

2. Information is consistently classified and presented within each data set: no one will have to learn a new system to use new data. For instance, consistent transliteration and treatment of foreign names is an absolute must. Establishing such common procedures is crucial for true information sharing. Doing the work upfront saves critical time later.

3. General access to programs is controlled at the registry level though the specific administrative duties may be delegated: such a system is very flexible. In cases of possible compromise, it is easier to take back bearings as all users or their organizations would be documented by the audit trail at the registry level.

4. A Central Registry would have broader standards of completeness than the sum of the demands by the organizations involved, and provide back up in cases of inadvertent destruction. In an emergency previously superfluous data would be immediately available.

The end result will be a database that is internally consistent and as comprehensive as possible. The system will win converts by making the analysts' job easier on one hand, and reducing administrative costs to the various organizations on the other.

How to create a Central Registry with minimal disruption

The best beginning would be with open source information. There is a critical need for it, and beginning with it would provide a very strong test of system strength and flexibility because the data set is much larger and more various than classified information is likely to be. Open source is very useful as confirmation for classified material or to add telling detail to a narrative. Never forget that even questionable sources have to suffer public scrutiny and often receive severe review: even dictators have to tell the truth on occasion.

Open source can be a great help, especially in unsettled circumstances, providing critical information with little lag time. During the Yom Kippur War, our ship received a great deal of classified information, but not much intelligence analysis relating. Fortunately, one of my Intelligence Center watchstanders subscribed to the Sunday Times of London. With only slight delay, generally two days, we knew where the fronts were, attrition levels, recce flights and had a solid relevant timeline. Combining classified unclassified material, the ship's intelligence personnel created effective briefings for both the ship's command and embarked staff. At times like these, the total system is stressed and assets are better used than provided backgrounders available elsewhere. As a note, the book that resulted from the newspaper's efforts, by Insight Team of the London Sunday Times is excellent, though dated.

The following from the Wall Street Journal shows some of the problems that have persisted even these many years:

> "How well these dots are being connected is less clear. Post-9/11 legal reforms now permit FBI agents to search Google and other commercial sites. Yet less than one-third of the FBI's national security branch agents and analysts have Internet access at their desks. A $500 million technology project to update the software to access the terrorist watch list of some one million names doesn't reliably track Arabic names when translated into English. It also doesn't allow basic search terms such as "and" and "or." [2]

A good open source database, for a start would help to get places like the FBI to use the computer, and more importantly to understand what it can and cannot accomplish and insist that the in-house systems meet their professional needs rather than beliefs of persons who control but do not have to rely on the product. In this case a very simple search engine and consistent transliteration would go a long way toward building trust in automated systems, and provide a standard or comparison.

Even if certain classified material did not make it into the system, it would provide a framework to better control any information and use it more effectively with the Central Registry material. If the material were not in the registry, it could be referenced so that cleared individuals would know it was there and obtain the data if needed.

Finally, all this preliminary work makes a transition to a true Central Registry for all intelligence organizations both easy and logical. Nothing suggested would preclude any function from diverging from more common practice, in service to the work at hand.

System Benefits

The first benefit is simply to know what the total universe of information is available and potentially available to the user. The initial open source effort would make later additions, no matter the source easier, and make classified information more useful, even if only referenced and not included in the Central Registry.

This system will have the ability to grow and change including classified material for internal use which can be easily shared in an emergency. The personal investment in learning the system will encourage the user to help improve it. Think of the commercial software packages: the more the user relies on the greater the motivation for others to use it too. Nothing succeeds like success and nothing guarantees that more than utility.

The more data available the easier it is to set valid acquisition goals and meet them quickly and efficiently. It is crises that call for resources beyond any possible contingency plan, where a comprehensive registry can literally save the situation. How many times have planners had to rely on incomplete or obsolete information in an emergency?

A related issue is getting the best people to work in a Central Registry. In a registry, data organization and control are the key missions. In most intelligence shops it is a low level housekeeping function. It also is a training ground for people who can anticipate needs and meet them before tasked, a sort of armorer if you will. It would be easier to attract and keep people at the top of their professions.

A common system, which is effective will encourage greater use, and improve the skills of the users, and it easier to integrate and test classified material during analysis.

Analytic Benefits

A working registry as described would quickly provide benefits to the user and a sense of participation which would increase their commitment to the system.

Serving my analyst customers, I discovered that they have no time to waste waiting for answers in the middle of a project. Even a short delay in obtaining key information can stall a project for a considerably longer period than the time of the delay would suggest, lowering the quality of the end product. Tasks have an internal logic, and delay can be deadly. Note that many scientist and other researchers work extremely long hours, and do so gladly to maintain their momentum.

A Central Registry will also serve as a copyright office. There are many instances when groups simply will not share their work with others for fear of nothing more than plagiarism. The system will establish both claims to content and priority of effort. By doing so, too, people, will get credit when due in their own research because it will be open to the scrutiny and comment of other analysts. In the academic world, standing is not only by amount published but also by how often an author is cited, that determines reputation.

Because the Central Registry will make it easier for the authors to have their work seen, they will also know who the better of their peers are and improve their thinking as well as that of others through informal liaison. Seeing more and better peer work helps thinking and saves duplicated effort. It also provides a very good place to develop new ideas.

Finally individual character and a drive for excellence combined with more information and research will improve quality of all work in the system.

BENEFITS TO THE INTELLIGENCE SYSTEM

The system is currently viewed by some as battling fiefdoms in a highly centralized organization. Creating a Central Registry with an integrated data retrieval system for both information and product will go along way to cure some of the more obvious instances of infighting and failure to communicate. Again, it is easier to coordinate using an intermediary that is two steps rather than one, than to develop a large number of bilateral 'barter' relationships.

With more data and more reviewers it will be increasingly difficult for anyone to ignore or hide facts to support of institutional or personal biases. There simply will be too much information from all sources to ignore inconvenient facts. Some analysts have tried to destroy the credibility of certain sources because the information could be used in ways which conflict with their political views. I have personal knowledge of one such instance where a source that had never been shown in error was said to be untrustworthy by analysts based on personal political bias. Such action would be much more difficult with a Central Registry.

Span of control will increase with a decline in layers of management in the analytic areas. The analytic quality will be the measure of the institution's standing, making management a support function, including expertise, rather than direction or manipulation of product.

Classified information will be more and more subject to confirmation from open source intelligence and in some instances trumped by it. Frederick Kagan worked on a surge related study when General Keane went to the American Enterprise Institute offices to check the progress. The general was stunned by the depth of the material the AEI had compiled. Based his years of Top Secret briefing he found it hard to believe that they had just used open source off the Internet. [3]

A good registry allows more finely turned collection efforts, guided by need rather than institutional inertia. Historically, only the highest levels of government could make a tasking for a specific piece or general class of information, and under this system that level of control will return. It also allows testing of classified information to see if it is in fact reliable. If a HUMINT source claims to be in a sensitive position but reports information after it appears in the media that is obviously should be suspect.

A Central Registry will help the administration deal effectively with issues relating to surveillance and civil liberties concerns, both foreign and domestic:

1. More and better information suggests ways to approach sensitive collection issues with minimal encroachment on civil liberties.

2. By having solid information on what it is and what is not available, the government is in a much better position to receive positive ruling on collection efforts where it can be shown that no alternative truly exists.

Finally a Central Registry provides enough information to make advanced statistical testing possible and open the way to uses yet undiscovered. Size, as Soviet planners used to say, has a quality all of its own. It is only when massive quantities of information are available can the truly awesome computing power currently available be used.

SUMMARY

Some like see the task as impossible:

> Government intelligence has been reorganized into the massive bureaucracy at the Office of the Director of National Intelligence. In contrast, countries such as Britain and Israel have structures that encourage information sharing while also ensuring competitive analysis of what the gathered intelligence really means. [4]

Actually the task is not impossible and in some sense the existence of the ODNI (Office of the Director of National Intelligence) makes it easier. Information sharing through a Central Registry will allow truly competitive analysis while protected essential working relationships and aid the creation new ones.

---

[1] Treverton, Gregory F. *Reorganizing U.S. domestic intelligence : assessing the options*. The Rand Corporation: 2008 ISBN 978-0-8330-4501-0 p.38

[2] Crovitz, L. Gordon. "Government Intelligence is Way Behind." Wall Street Journal: Sept. 15, 2008.

[3] Woodward, Bob. *The War Within: A Secret White House History 2006-2008*. Simon & Schuster, NY: 2008. p. 276-8

[4] Crovitz, L. G. *op cit.*