Senior Service College FELLOWSHIP PROJECT

SECURE INFORMATION SHARING IN A DEFENSE SUPPORT TO CIVIL AUTHORITIES ENVIRONMENT

BY

LIEUTENANT COLONEL EUGENE T. (GUY) GORMLEY
United States Army National Guard

USAWC CLASS OF 2009

U.S. Army War College, Carlisle Barracks, PA 17013-5050

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
20-03-2009	Civilian Research Paper	01-08-2008 – 01-04-2009

4. TITLE AND SUBTITLE

Secure Information Sharing in a Defense Support to Civil Authorities Environment

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

LTC Eugene T. (Guy) Gormley, ARNG

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION A: UNLIMITED

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In the past few years, Defense Support to Civil Authorities (DSCA) has become a more important mission for the military services, especially the National Guard. In the aftermath of events such as 9/11, Hurricane Katrina and others, the federal and state governments have recognized the importance of timely and accurate information sharing to support pre-event planning and effective response during an event. Another key issue facing Chief Information Officers (CIOs) is the aspect of information security/ information assurance. In this age of continuous cyber attack, protection of networks and the data they contain is also of the highest importance. The assets of the National Guard are a powerful and underutilized tool to protect state level networks and facilitate better information sharing between the state and federal networks. Using the State of Virginia as an example, this paper will examine the implementation of information sharing between the Army National Guard and the state emergency management agency and make recommendations to improve the information sharing environment in those organizations.

15. SUBJECT TERMS

Information Sharing, Cyber Attack, Information Security, Information Assurance

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			LTC Eugene T. Gormley
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	32	**19b. TELEPHONE NUMBER** *(include area code)* 540-273-1913

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

USAWC CIVILIAN RESEARCH PROJECT

SECURE INFORMATION SHARING IN A DEFENSE SUPPORT TO CIVIL AUTHORITIES ENVIRONMENT

by

Lieutenant Colonel Eugene T. (Guy) Gormley
United States Army National Guard

Dr. Virgil Gligor
Carnegie Mellon University Adviser

Colonel Frank Blakely
U.S. Army War College Faculty Mentor

This CRP is submitted in partial fulfillment of the requirements of the Military Education Level 1 (MEL 1) of the Senior Service College Fellowship Program – Academic Year 2009.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel Eugene T. Gormley

TITLE: Secure information sharing in a defense support to civil authorities environment

FORMAT: Civilian Research Project

DATE: 12 March 2009 WORD COUNT: 5,606 PAGES: 32

KEY TERMS: Information Sharing, Cyber Attack, Information Security, Information Assurance

CLASSIFICATION: Unclassified

In the past few years, Defense Support to Civil Authorities (DSCA) has become a more important mission for the military services, especially the National Guard. In the aftermath of events such as 9/11, Hurricane Katrina and others, the federal and state governments have recognized the importance of timely and accurate information sharing to support pre-event planning and effective response during an event. Another key issue facing Chief Information Officers (CIOs) is the aspect of information security/ information assurance. In this age of continuous cyber attack, protection of networks and the data they contain is also of the highest importance. The assets of the National Guard are a powerful and underutilized tool to protect state level networks and facilitate better information sharing between the state and federal networks. Using the State of Virginia as an example, this paper will examine the implementation of information sharing between the Army National Guard and the state emergency management agency and make recommendations to improve the information sharing environment in those organizations.

SECURE INFORMATION SHARING IN A DEFENSE SUPPORT TO CIVIL AUTHORITIES ENVIRONMENT

In the past few years, Defense Support to Civil Authorities (DSCA) has become a more important mission for the military services, especially the National Guard. In the aftermath of events such as 9/11, Hurricane Katrina and others, the Federal and State governments have recognized the importance of timely and accurate information sharing to support pre-event planning and effective response during an event. Several federal level plans and a federal program office have been put in place to ensure the smooth flow of information between all levels of government.

Another key issue facing Chief Information Officers (CIOs)[1] is the aspect of information security/ information assurance. In this age of continuous cyber attack, protection of networks and the data they contain is also of the highest importance. Therefore,

> Two competing considerations exist when managing the flow of information intended to mitigate the risk of malicious activities or to respond to incidents generated by malicious activities. The primary goal is to get information distributed to the broadest range of people or systems that need the information, but this goal must also be balanced by the need to keep the information out of the hands of malicious individuals.[2]

The assets of the National Guard are a powerful and underutilized tool to protect state level networks and facilitate better information sharing between the state and federal networks. Using the State of Virginia as an example, this paper

---

[1] In the military CIOs are also know as G-6, A-6 or J-6. I will use CIO throughout this paper to reduce confusion unless specifically spelled out in the text.

[2] ISAC Council White Paper "Vetting and Trust for Communications among ISACs and Government Entities", page 1. January 31, 2004. Available at http://www.isaccouncil.org/pub/Vetting_and_Trust_013104.pdf Accessed on 7 February 2009.

will examine the implementation of information sharing between the Army National Guard and the state emergency management agency. Based on this examination, I shall make recommendations for improving the information sharing environment and information security/ information assurance posture of both organizations. This paper will only examine information sharing at the sensitive but unclassified (SBU)[3] and unclassified network level.

The Case for Information Sharing

We live in the information age and secure information management is being looked at more and more as a key component of business operations. Information is vital for governments to conduct normal functions and becomes even more important during a local, state or national emergency. In the words of one historian, in an example that can apply to any level of leadership in any crisis, "A commander….needs information as badly as he needs rations, water, and ammunition. In fact, on many occasions he needs information…more than anything else. You can keep going on an empty belly, but lack of information can kill you very suddenly."[4]

One of the key recommendations of the 9/11 Commission report was that "Information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge."[5]This shortfall was widely recognized, even before 9/11, as evidenced by the myriad of knowledge

[3] Sensitive But Unclassified (SBU) has been replaced at the Federal level by Controlled Information (CUI), however CUI is not in general usage yet.
[4] John Elting, Swords Around a Throne (London, Collier MacMillan Publishers 1988, Page 103.
[5] The National Commission on Terrorist Attacks Upon the United States The 9/11 Commission report", page 417. Available at http://govinfo.library.unt.edu/911/report/index.htm accessed on 7 February 2009.

management initiatives across DOD and elsewhere (i.e. Army Knowledge Online (AKO), Navy and Marine Corps Internet (NMCI), Defense Knowledge Online (DKO), and many others).

In a more recent and pertinent example during Hurricane Katrina:

> Mississippi Governor Haley Barber summed up the lack of communications: "My head of the National Guard might as well have been a Civil War General for the first two or three days because he could only find out what was going on by sending somebody. He did have helicopters instead of horses, so it was a little faster, but the same sort of thing.[6]

Governor Barber was referring to the collapse of the communications networks, but could also just as well have been referring to the lack of information from other sources. Lack of good information sharing policies and procedures has been cited as a significant lesson learned in the aftermath of Hurricane Katrina.[7]

The need for information sharing exists not only at the federal and state to federal levels. A significant amount of the need and data traffic exists at the state and state to local levels. In an emergency, the incident always[8] starts out as a local problem. The incident managers have an important need for information to support their decision-making process.

> Information is the life blood of any organization, and to an ever-increasing extent that information exists and is most valuable in electronic form. In the case of public agencies, and state governments particularly, the economy and speed with which data can be captured and employed to transact public business is remarkable. Data are aggregated and analyzed to support implementation and management of public programs….shared among agencies to reduce costs and enhance services, and published or

[6] Special Report of the Committee on Homeland Security and Government Affairs, S. Rept 109-322 "Hurricane Katrina: A Nation Still Unprepared", 109th Congress, 2nd Session. Available at http://www.gpoaccess.gov/serialset/creports/katrinanation.html Accessed on 7 February 2009.
[7] See "The Federal Response to Hurricane Katrina: Lessons Learned" available at http://library.stmarytx.edu/acadlib/edocs/katrinawh.pdf Accessed on 7 February 2009.
[8] See the National Response Framework, Pages 10 and 15 at http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf and The National Incedent Management System (NIMS) at http://www.fema.gov/emergency/nims Accessed on 7 March 2009.

> disseminated to allow transparency or as a resource to citizens and business. All contribute to the sense that the enterprise is almost literally, all about the data.[9]

The need for this data exists at the strategic, operational and tactical levels of government response to a national emergency. In terms of information sharing and management, the strategic level correlates to the federal pre-event planning/ event response and federal to state coordination in an emergency. The operational being the state and state to local relationship and the tactical environment exists at the local level of response. This rational follows the accepted relationships set forth in the National Incident Management System (NIMS).[10]Understanding the different command and control relationships is very important for the Guard members to understand so they know the importance of maintaining the state and or local networks should they be called on to do so.

Information in modern tactical networks is generated from multiple sources: global positioning system receivers, unmanned and manned sensors, observations and the internet, to name just a few. In today's environment, information must flow quickly from these sensors to analysts and decision makers and, finally, to those who must execute action. Any delay of more than a few minutes from detection to action often significantly reduces the effectiveness of the response.[11]Should the information not be shared in a timely manner, there

---

[9] Charles Robb and others, "Protecting the Realm: Confronting the realities of State Data at Risk" NASCIO 2008 Available at http://www.nascio.org/publications/documents/NASCIO-ProtectingRealm.pdf Accessed on 7 February 2009.

[10] See National Incident Management System (NIMS) at http://www.fema.gov/emergency/nims/AboutNIMS.shtm Accessed on 7 February 2009.

[11] Mel Crocker "Cross Domain Information Sharing in a Tactical Environment" Software Technology Support Center, Mar 2007 Issue. Available at http://www.stsc.hill.af.mil/crosstalk/2007/03/0703Crocker.html Accessed on 7 February 2009.

can be severe consequences to life and property of the citizens of our nation as shown by the delayed response to Hurricane Katrina.

The past 10 years or so have given many examples of information shortfalls and their consequence (9/11 and Katrina). Based on the lessons learned from these incidents, major and minor, governments at all levels have begun to codify information sharing in public policy and create information sharing initiatives to correct the problems in government communications.

Information Sharing Initiatives

What is the state of information sharing initiatives at the Federal level and how are these being applied at the Virginia state level? It is important to understand what the current state of information sharing is and how these initiatives impact Virginia. The logical next step, then, is to examine the status of current federal and state information sharing initiatives. The subsequent step is to see how these initiatives are applied in the information exchange between the Virginia National Guard (VaNG)[12] and the Virginia Department of Emergency Management (VDEM). Understanding this will not only help these organizations, but also assist with the development of a strategy that will be applicable across the country.

For the DSCA environment, the most important initiative is the information security strategy from the Department of Homeland Security (DHS), released on April 18th, 2008. This strategy was built on the 2007 updated National Strategy for Information Sharing. The DHS strategy aims

[12] In Virginia and all other states, the National Guard includes the Army National Guard (ARNG) and Air National Guard (ANG).

> To ensure that information and intelligence flow where and when they should, DHS must foster information sharing, consistent with law, regulation and policy, in each of the following ways: i) internally within DHS. ii) horizontally within the U.S. Government between both law enforcement agencies and the intelligence community, iii) vertically with state, local, territorial, tribal and private sector partners, and iv) horizontally with the law enforcement and intelligence agencies of foreign allies and appropriate international institutions.[13]

The DHS strategy follows the recommendations of the 9/11 Commission and President's strategy for information sharing. The major method DHS is using to implement this strategy is the Homeland Security Information Network (HSIN), HSIN "…allows all states and major urban areas to collect and disseminate information between federal, state, and local agencies involved in combating terrorism."[14]HSIN has faced some criticism from the Government Accountability Office (GAO) and others, but will eventually provide an effective network to the support the DHS mission.[15]DHS is also heavily involved in the Fusion Centers[16]created by the several states.

Within the Federal Intelligence Community, there is the Information Sharing Environment (ISE) (this was, until recently, the program manager for Information Sharing).[17]The ISE provides standards and foundations for

---

[13] Department of Homeland Security, "Department of Homeland Security Information Sharing Strategy", April 18, 2008. Available at http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf Accessed on 7 February 2009.

[14] Homeland Security Information Network page: http://www.dhs.gov/xinfoshare/programs/gc_1156888108137.shtm Accessed on 7 March 2009

[15] See David A. Power "Homeland Security Information Network Needs to be better Coordinated with Key State and Local Initiatives" GAO-07-822T May 10, 2007. Available at http://www.gao.gov/new.items/d07822t.pdf Accessed on 7 February 2009.

[16] Many states and larger cities have created state and local fusion centers to share information and intelligence within their jurisdictions as well as with the federal government. The Department, through the Office of Intelligence and Analysis, provides personnel with operational and intelligence skills to the fusion centers. http://www.dhs.gov/xinfoshare/programs/gc_1156877184684.shtm Accessed on 11 March.

[17] See: http://www.ise.gov/index.html Accessed on 7 February 2009.

information sharing across the intelligence and law enforcement spectrum. The standards shown on their website are largely the National Institute of Standards and Technology (NIST) standards that will be discussed in recommendations below. ISE has also come under GAO scrutiny, saying "…this plan lacks important elements essential to effectively implement the ISE."[18]The GAO report identified gaps in the ISE's scope and implementation. The report also highlighted that while the ISE has done much work on setting goals and objectives, the ISE has not shown how it has improved information sharing. This lack of information on the efficacy of information sharing programs is a common problem. There is very little data on how well these programs are performing.

The Department of Defense published its Information Sharing Strategy in May of 2007. This strategy lays out that "Sharing of Information is an increasingly important element of Departmental mission success."[19]The DOD strategy also has the one of the clearest definitions of information sharing: "Making information available to participants (people, processes or systems). Information sharing includes the cultural, managerial and technical behaviors by which one participant leverages information held or created by another participant."[20]Within the DOD strategy information sharing between the National Guard and the several states is an implied task rather than explicitly specified, but the DOD has

[18] Eileen R. Larence "Information Sharing: Definition of the Results to be Achieved in Terrorism-Related Information Sharing is needed to Guide Implementation and Assess Progress", GAO-08-637T, July 23, 2008. Available at http://www.gao.gov/new.items/d08637t.pdf Accessed on 7 February 2009.
[19] Office of the Chief Information Officer, "Department of Defense Information Sharing Strategy", Page ii, May 4, 2007. Available at http://www.defenselink.mil/cio-nii/docs/InfoSharingStrategy.pdf Accessed on 7 February 2009.
[20] Ibid, page ii.

taken some concrete steps that show that the NGB portion of the DOD Information Sharing mission is important.

One of the immediate responses to the communication shortfalls identified during Hurricane Katrina was for DOD to fast track the creation of National Guard Bureau's Joint Continental United States (CONUS) Communications Support Environment (JCCSE). One of the objectives of JCCSE is to support information sharing between DOD and the state governments and thus helps to support the DOD information sharing strategy.[21]JCCSE's immediate success was to provide a deployable communications capability to each state. This gives each state the means to send information to decision makers in the absence of commercial communications.

Another major component of JCCSE is the Joint Information Exchange Environment (JIEE). This is a web based Common Operating Picture (COP) tool that

> ...is an information collection, collation, organization, dissemination and archival tool providing real-time situational awareness and an automated, shared Operational Picture. It is the 'desktop' that operations center staffs use for effective event/crisis management and information sharing. It provides a clear operational picture to senior leadership, enabling them to consistently make rapid, accurate, and fully informed decisions. JIEE also supports content and document management tasks while providing data mining, data visualization, and operations tracking tools. Additionally, JIEE supports the daily operations of the National Guard Bureau's Joint Operations Center (JOC) and is compliant with Joint CONUS Communications Support Environment (JCCSE) standards for communications interoperability. The NGB JOC uses JIEE to track requests for information, organize responses, coordinate support to assist first-responders, ensure leadership is kept fully aware of events and decision requirements, share information among the state Guard units. [*sic*] Information 'pull' and selective information 'push' features are activated at the operations center level, enabling those closest to the

[21] JROCM 173-06 provided to the Author by the National Guard Bureau J-6 Staff.

situation to gather and disseminate cogent information to those requiring it, without overloading others. [22]

In short, JIEE has become the COP[23] system for the National Guard. JIEE is also becoming the COP standard for U.S. Northern Command (NORTHCOM).[24]The NGB CIO's intent is to provide JIEE to each of the state National Guard Headquarters and to each state EOC. Providing JIEE in each location establishes an information sharing connection to the NGB operations center and eventually to the NORTHCOM operations center providing situational awareness to NGB and US NORTHCOM.

Information sharing plans and policies (and implementation) is far less detailed in both the VaNG and VDEM. Based on interviews with the current VaNG and the VDEM CIOs, information sharing between the two is working very well. However, formal plans and policy are lacking and the information sharing actually happening has more to do with personal relationships in the two organizations than from good establish procedure.

JIEE is used by the VaNG, but only when forced by NGB and normally during a pre-planned exercise. The training and procedures for using JIEE are limited and usually consist of computer based training. The VDEM CIO is aware of JIEE, and has seen it demonstrated, but does not use JIEE. Both the VaNG and VDEM use a separate COP tool called WEBEOC to share information during an incident. Emailed attachments are the most basic (and frequently used)

[22] Taken from http://www.ksikoniag.com/Achievements/JIEE/tabid/63/Default.aspx Accessed on 7 February 2009.
[23] See http://www.jfcom.mil/about/fact_safcop.html for a clear definition of Common Operating Picture Accessed on 7 March 2009.
[24] Email exchange with LTC Tamara Higgins, US NORTHCOM J-63.

form of information exchange by VDEM and the VaNG along with Universal Serial Bus (USB, also known as thumb drives) drive exchanges.[25] The VaNG has a draft communications plan to support the VaNG All-Hazard Plan that includes information sharing. The VDEM CIO has drafted an Information sharing plan that will be included in the VDEM strategic plan and developed a very promising COP tool that is hardware platform independent and web-based. This tool, called "Virginia Interoperability Picture for Emergency Response" (VIPER) is being reviewed by DHS as a possibility for their COP tool.[26] VDEM developed VIPER to address the weakness and shortfalls that exist in WEBEOC.[27]

So, it can be seen that there are a plethora of strategies, plans and policies to address the information sharing shortfalls. This has led to greater cooperation and coordination between organizations at all levels of government, but much more work can be done. This benefit is very marked in the State of Virginia. Prior to 9/11, the VaNG was not a real partner with VDEM and was VDEM's last choice for support. Today, the two organizations are cooperating and seem to be well coordinated, if only on an ad hoc basis. However, these information-sharing initiatives have come with an increasing risk, the cyber attack threat to networks and the data they contain.

[25] Information in this section come from a series of interviews and email exchanges between the author and the VaARNG G-6 and the VDEM CIO.
[26] PowerPoint Briefing provided by the VDEM CIO.
[27] COP Tools are a major topic in government organizations. There is no clear standard and many competing solutions. The standardization of COP tools is outside the scope of this paper, but much more research in this area is needed.

Information Sharing Risks and Vulnerabilities

Cyber attacks are the greatest threat to information sharing initiatives. These attacks are on the rise and cause significant financial and operational losses to organizations. The risks associated with transferring data from one source to another increase the likelihood of a network being compromised. For instance, an employee that uses a USB drive to transfer a file infected with a computer virus spreads it from VDEM to the VaNG. This action causes the virus to spread to the Army National Guard network, and then potentially spreads the virus across DOD. Introducing a virus, or other malicious code, opens the system to hackers and puts personally identifiable information (PII) contained on the system at risk for data loss. Since 2005, over 250,000,000 records containing PII have been lost.[28]These data breaches can cost an agency millions of dollars to correct and mitigate.

Cyber attacks can take on many forms and come from many directions. Some are state sponsored and others come from lone hackers. For example, in 2008, a group of 11 people managed to steal 45 million users' bank and credit card details, resulting in the loss of more than $256 million. The group members were multinational and very sophisticated. They were able to commit their crime by sitting outside large, well known, retail stores and hacking into the store's network. "This illustrated asymmetry…and the enhanced vulnerability of commercial targets as opposed to direct military targets."[29]

[28] http://www.privacyrights.org/ar/ChronDataBreaches.htm Accessed on 7 February 2009.

[29] Jason Fritz, "How China will use Cyber Warfare to Leapfrog in Military Competitiveness", Page 45, Culture Mandela, Vol. 8, No. 1 October 2008 Provided to the Author by LTC Stephan Picard.

Hackers and producers of other malicious computer software (i.e. viruses and spyware) also target military installations and networks. “In 2005 alone, ‘the Pentagon logged more than 79,000 attempted intrusions’”[30] and the number grows every day. The attacks themselves take on many different and frequently changing forms. The types of cyber attacks include: security exploit, spoofing attacks, phishing, trojans, viruses, worms and denial of service attacks.[31] “The [United States of America’s] paramount position and its heavy reliance on computers have made it a prime target. For this reason it has some of the most extensive information on cyber attacks. The United States has had millions of computers infected at a cost in the billions of dollars.”[32] These attacks in many cases are also directed at state and local governments and constitute a real threat to state operations. Two recent examples show the possible effect on the national, state and commercial infrastructure. In May of 2007, much of the cyber infrastructure in the nation of Estonia was disabled by a large, coordinated and sustained attack.[33]Much the same happened at the start of the recent war between Russia and Georgia.

> The Estonian attacks were the first to show how cyber attack against a state provides a debilitating effect at low cost, a lack of attribution, a lack of legal framework in defense and may point to a new arm of traditional attack. The Russo-Georgian war of August 2008 was even more sophisticated and intense than the Estonian case, showing a maturation of the process.[34]

---

[30] Ibid page 56.
[31] For a more complete definition of these attacks with examples, see ibid 49-54
[32] Jason Fritz, “How China will use Cyber Warfare to Leapfrog in Military Competitiveness”, Page 54.
[33] Patrick Jackson, “The Cyber Raiders hitting Estonia” BBC News, 17 May 2007. Available at http://news.bbc.co.uk/2/hi/europe/6665195.stm Accessed on 7 February 2009.
[34] Jason Fritz, “How China will use Cyber Warfare to Leapfrog in Military Competitiveness”, Page 57, Culture Mandela, Vol. 8, No. 1 October 2008 Provided to the Author by LTC Stephan Picard.

Should an attack of this kind happen in the United States, a significant portion of the threat would be directed at the state and local networks. Disabling these systems during a national emergency (e.g., a cyber attack directed at the surrounding states, DHS and DOD networks during a category 3 hurricane in Louisiana) would be potentially devastating. An attack of this kind could cause a major delay in the response to the natural disaster possibly resulting in an unnecessary loss of life and property. "U.S. national security relies in large part on the soundness of state government information systems and there has been growing pressure on state IT executives to make these systems secure."[35]The state and local governments own the majority of communications networks supporting public safety functions. An attack targeting the local 911 system could cause mass confusion and loss of life if it happened during some other large emergency. The ability to defend against these attacks is limited if the organization is not prepared in advance. The current state of cyber readiness in most organizations is not sufficient to respond quickly enough to an Estonia-like attack. One of the leading cyber-defense research think tanks, the SANS Institute, "…confirms that the time to download and apply critical security patches now exceeds a network's survival time."[36]This means that an unprepared location could not fix a problem quickly enough to prevent the network from shutting down.

[35] Ed Janairo, "States fight against cyber-terrorism", State Government News, March 2002. Available at http://www.csg.org/pubs/Documents/sgn0203StatesFightCyber-Terrorism.pdf Accessed on 7 February 2009.
[36] Dave Zwieback, "The Gathering Storm: The Future of Cyber Attacks" CounterStorm, Inc 2005 Available at http://inkcom.com/pdf/inkcom_gathering_storm.pdf Accesses on 7 February 2009.

In these uncertain economic times, the cost of these attacks could greatly deplete a state or local budget. The parallel analogy is a major snowstorm occurring late in the season when a transportation department salt budget has already been used. Information technology department budgets are based on relatively fixed costs and normally have no flexibility to react to emergencies. The cost to replace or upgrade attacked equipment could cause a reduction in manpower and/or training resources for information security personnel. Just on the commercial side "Software defects, and hacker attacks, cost the U.S. economy from US$20 billion to $100 billion annually…. This includes all of the additional security protection that consumers are forced to buy, and the parts of the economy that lose revenue because of money flowing into managing software defects."[37]Also, "Investigations into the stock price impact of cyber-attacks show that identified target firms suffer losses of 1% - 5% in the days after an attack…price drops of this magnitude translate into shareholders losses of between $50 million and $200 million."[38] Recent research also suggests that a massive cyber attack could cost the U.S. Economy more than 50 times the economic losses of Hurricane Katrina.[39]

As can be seen, the threat of cyber attack is great and costly. The risk of opening up vulnerabilities is one of the significant barriers to information sharing.

---

[37] Blake Glenn, "They're Not Trying to Make Bad Software", TechNews World, February 3, 2009. Available at http://www.linuxinsider.com/story/64810.html Accessed on 7 February 2009.
[38] Brian Cashell, William D. Jackson, Mark Jickling and Baird Webel "The Economic Impact of Cyber Attacks" Congressional Research Service order code RL 32331, April 1, 2004. Available at http://www.au.af.mil/au/awc/awcgate/crs/rl32331.pdf Accessed on 7 February 2009.
[39] Eric Green, "New Research shows Cyber Attack Could cost US 50 times more than Katrina", Market Wire, July 2007 Available at http://findarticles.com/p/articles/mi_pwwi/is_200707/ai_n19429846 Accessed on 7 February 2009.

CIOs want to limit access to outsiders and protect vital data (the recent loss of external media drive access on DOD networks for example[40]). Government organizations need to take all proper precautions to protect their networks and secure data. However, this should not interfere with vital information sharing between organizations. Information security is a drag on information sharing, but other barriers also exist that affect how well organizations share information.

Remaining Barrier to Information Sharing

The major remaining barrier to smooth information sharing, while not insignificant, can be quickly summarized. In addition to the policy and potential funding issues addressed above, the largest barrier to effective information sharing is trust. The trust issues evolve from an organizational culture that emphasizes parochial concerns over effective cooperation with other agencies.

The trust issues come from two major sources: 1) the risk of network/ data breaches (addressed above) and 2) inter-departmental/ agency politics and the "Not Invented Here" syndrome. Robert L. Flowers, commissioner of Public Safety for the State of Utah has studied this issue and concluded

> …when seemingly reasonable changes are made in the way that information is supposed to be gathered and distributed, the lack of trust between the people in that redesigned system will sabotage its actual effectiveness. Second, people in the information system are often subject to "groupthink;" that is they lose their ability for independent thought and judgment, and instead follow the herd in resisting efforts for change. Third, officials are prone to parochialism. They view problems from a narrow, local perspective, rather than from the bigger picture of State and national requirements for homeland security. …My findings are typified by the response offered by an elected Sherriff to efforts at involving his

[40] See http://www.securecomputing.net.au/News/128992,us-military-bans-usb-thumb-drives.aspx for more information.

department in an informational sharing database: “Stay out of my county and take the database with you.[41]

While not nearly as extreme as the example above, this statement typifies the relationship between VDEM and the VaNG. The two organizations are very cooperative, but there is still a lack of trust at the organizational level to allow a true information sharing environment.

There is also a lack of public policy to facilitate an information sharing environment and engender trust between organizations. The sovereignty of the states[42] complicates mandating an information sharing environment. However, there are no published standards for information sharing and no standard enterprise architecture[43] template along the lines of the Department of Defense Architecture Framework (DODAF)[44] for the states to develop their own. The various information sharing strategies mentioned above lack implementing guidance that includes the states. Currently, the DODAF does not include the NGB to state relationship. There are several things that can be done to improve this situation and solidify the information sharing relationship between the National Guard and the States.

[41] Robert L. Flowers, “Strategies to Build a Trusted and Collaborative Information Sharing System for State-Level Homeland Security” Naval Postgraduate School, June 2004. Available at https://www.hsdl.org/homesec/docs/theses/04Jun_Flowers.pdf&code=dc57497d2a2f0bfd2c1d06caafeb9f43?search Accessed on 7 February 2009

[42] For an in-depth discussion of state sovereignty and the impact to state and federal relations, see: http://www.fas.org/sgp/crs/misc/RL30315.pdf Accessed on 7 March 2009

[43] Enterprise Architecture is the organizing logic for business processes and IT infrastructure reflecting the integration and standardization requirements of the firm’s operating model. For more information on how it used in government areas see http://www.gao.gov/bestpractices/bpeaguide.pdf. DOD organizations are under a mandate to implement DODAF. Accessed on 7 March 2009.

[44] See http://en.wikipedia.org/wiki/DoDAF for an explanation of DODAF.

Recommendations to improve the environment

This paper has shown the current state of information sharing initiatives from the perspective of the National Guard and state emergency management agencies. There are many benefits to information sharing, but also many risks and barriers. How can we make the situation better and at the same time reduce the risk to our local, state and federal networks? The technology to facilitate information sharing exists today. The real barriers are policy, organization and trust. Using the DOD Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) [45]method, the states can improve the information sharing environment at a relatively low cost.

Any solution to the information sharing problem in today's fiscal reality should be revenue neutral or provide a cost savings. There is much that can be done at the public policy level at little to no cost. DHS and DOD should coordinate their enterprise architecture efforts to include the information sharing relationship at the National Guard/ state emergency management level. This should include a generic template for information sharing enterprise architecture that the states can modify. Building the required views for enterprise architecture is time consuming and costly. Recently, the VaNG estimated it would cost $300,000 to contract for enterprise architecture development just for the VaNG

[45] "DOTMLPF is an acronym used by DOD. It also serves as a mnemonic, to remind Pentagon staff planners of the issues to be considered whenever establishing a new national security capability. Prior to undertaking a new effort, military planners are expected to complete a DOTMLPF Study". See http://en.wikipedia.org/wiki/DOTMLPF for a more in depth discussion. Accessed on 7 February 2009.

portion of the enterprise.[46]Providing the states with an 80% generic solution, modifiable to the specific state would reduce time, effort and cost, and should help to gain a wider acceptance of a national standard.

In addition, DHS and DOD should write implementing guidance for information sharing. The CIOs at those organizations could coordinate and issue a joint Pamphlet on the who, where, when and what, leaving the how to each state to determine. Doing this jointly would reduce the cost to DHS and DOD and keep the standards synchronized. Because of the state sovereignty issue and Posse Comitatus[47]this needs to be guidance, not regulation. “The solution is not centralization of interagency coordination at the highest levels of government, but clearer inter- and intra-agency guidance. The goal must be truly horizontal interagency planning performed virtually simultaneously at [all levels].”[48]

A second policy answer is for DHS to set the standards for data elements required for information sharing. Standardizing the data elements keeps the solution platform independent and allows the states to opt into federal information sharing systems, develop their own solutions, such as the Virginia VIPER system, or buy a commercial system as their own situation dictates. Using this solution prevents the states from having to immediately replace the systems they already operate, which eliminates another cost concern. “[Government] should

[46] Interview with the VaNG CIO.
[47] The Posse Comitatus Act (PCA) - Prohibits search, seizure, or arrest powers to US military personnel. Amended in 1981 under Public Law 97-86 to permit increased Department of Defense support of drug interdiction and other law enforcement activities. (Title 18, "Use of Army and Air Force as Posse Comitatus" - United States Code, Section 1385). The role of network monitoring by the federal government in a DSCA environment has not been vetted in the courts. PCA may apply.
[48] Matthew F. Bogdanos, “Joint Interagency Cooperation: The First Step”, page 16, JFQ Issue 37 available at http://www.dtic.mil/doctrine/jel/jfq_pubs/0437.pdf Accessed on 7 February 2009.

replace the current ad-hoc, personality-dependent form of information sharing among agencies by establishing and enforcing minimum standards of information sharing at the appropriate classification level."[49]

The various organizations can address the major issues of culture, trust and vulnerability to the network through a common set of risk management standards. If all of the organizations involved in information sharing use the same risk management methodology and provide the results to each other, a trust can be built from managing the identified risks together to ensure protection of the network. In the U.S. Army, the soldiers are used to conducting a risk assessment on every move, training event, exercise and operation; by extending this culture of risk management to their civilian partners, the National Guard can build a higher level of trust with the state emergency management agencies.[50]

To support this new culture of risk management, there is an existing solution that the National Guard can help apply with their civilian partners. The National Institute of Standards and Technology (NIST) have created

> …a generalized framework for managing enterprise risk for information standards that support organizational missions and business functions. The Risk Management Framework (RMF…provides a comprehensive vehicle for federal agencies and contractors to use in building IS [Information Security] into an organizations infrastructure….The RMF represents the security related activities that occur within an enterprise's system-development life cycle and that private-sector (and State) organizations that FISMA[51]doesn't cover can adopt. Such organizations can adopt the activities using the framework's "Plug and Play" features

[49] Ibid page 17.
[50] See https://safety.army.mil/.

[51] FISMA = Federal Information Security Management Act of 2002.

that allow use of any security categorization approach, risk assessment, set of security controls, or assessment process.[52]

The ISE has adopted the NIST Standards. The DoD Information Assurance Certification and Accreditation Process (DIACAP) should be modified to adopt the NIST Standards as well. Then, DHS can recommend to the states that they adopt them, putting all levels of government on the same risk assessment model. States would not be forced to accept the NIST Standards, but would need to be aware of them for information sharing with the Federal Government.[53] "At the present state of knowledge; we cannot identify any one best cyber-risk model that all firms and organizations could usefully adopt. There may never be such a one-size-fits-all procedure."[54] The NIST standards are probably as close as the various governments can get in the foreseeable future.

The Virginia National Guard can assist VDEM in managing the risk assessment process and improve the trust relationship at the same time. "One of the issues in the government is that we don't have enough trained Security folks…"[55] The National Guard is uniquely positioned to help states with the information security personnel issue. Each National Guard Joint Force Headquarters (JFHQ, i.e. the National Guard State Headquarters) has a computer emergency response team (CERT) included as part of its CIO

[52] Ron Ross, "Managing Enterprise Security Risk with NIST Standards" IEEE August 2007. Provided by Dr. Ross.
[53] The complete NIST Standards are available in NIST Special Publication 800-39.
[54] Brian Cashell, William D. Jackson, Mark Jickling and Baird Webel "The Economic Impact of Cyber Attacks" page 34, Congressional Research Service order code RL 32331, April 1, 2004. Available at http://www.au.af.mil/au/awc/awcgate/crs/rl32331.pdf Accessed on 7 February 2009.

[55] Wilson Dizzard, "IT Security calls for collaboration" Government Computer News Mar 23, 2002 available at http://gcn.com/articles/2002/03/03/IT-security-calls-for-collaboration.aspx Accessed on 7 February 2009.

organization. This team of 10 – 12 soldiers has the same mission as the U.S Army computer emergency response team (ACERT). The CERT's mission is to

> …is to conduct Command and Control Protect (C2- Protect) operations in support of Army commanders worldwide. The objective is to ensure the availability, integrity and confidentiality of the information and information systems used in planning, coordinating, directing and controlling forces. ACERT supports systems administrators reporting suspicious activity on their computer networks. ACERT also has the responsibility of keeping Army leadership informed of incidents, and promulgating alerts and warnings based on information collected from a variety of sources.[56]

In short, they are theoretically capable of providing vulnerability assessments and remediation. They exist to support the JFHQ and DOD networks at the JFHQ level, but they can be available to support other state agencies. This support would not be any different from the support the National Guard gives to the State during a state emergency and should not present a legal problem. The Adjutant General and the Secretary of Public Safety will probably require a detailed opinion from the legal departments on both sides to be sure. However, the authorized VaNG CERT is not currently manned, equipped or trained to perform this mission. The VaNG would have to correct this situation before the CERT could take on this mission. This is a resourcing question for the Adjutant General.

Until recently in the VaNG, as in many states, the CERT positions were used to provide operators for the deployable communications equipment provided by JCCSE. This situation is common across the rest of the National Guard. The task of operating the JCCSE communications suite can go to the network support (signal) company in the state, as it was in Virginia. This would provide the signal companies with equipment to train with until they are fielded

[56]See http://www.fas.org/irp/doddir/army/fm34-37_97/3-chap.htm.

new satellite equipment[57] and give them a state mission aligned with their communications training. If the state doesn't have a network support company, NGB (in its resourcing role) could allocate a network support platoon at the JFHQ to execute deployable communication missions[58] The implementation of Defense Integrated Human Resources Management System (DIHMRS)[59] in the next year may vacate enough positions in the JFHQ to support creating a network support platoon in the states that have no other signal organizations. These positions will come from the reduction of human resources and financial personnel required at the JFHQ due to the self-service functions in DIHMRS. The United States Property and Fiscal Officer, Data Processing Installation (USPFO-DPI) is another potential source of personnel. The implementation of DIHMRS will make the USPFO-DPI mission obsolete by transferring the local database managed by them to a nationally managed database.

The re-allocation of these positions is a resourcing decision for the Adjutant General. The CERT positions are also used to support full time staffing in the VaARNG CIO. However, these soldiers should be trained and equipped during weekend drill and annual training to support the CERT mission as called

[57] Most National Guard Network Support companies are currently waiting to field the Warfighter Information Network-Tactical (WIN-T). This is a satellite based communications suite. See http://www.globalsecurity.org/military/systems/ground/win-t.htm for more details. JCCSE provides a rough equivalent to a portion of WIN-T and would prove a good training system for the Guard Signal soldiers to maintain their skills. Accessed on 7 March 2009

[58] A very similar situation just happened in the state of Louisiana. Louisiana was given a one of kind signal company to support emergency communications in the state by NGB (Per conversation with the ARNG Signal Organizational Integrator.)

[59] Military Human Resources System (DIMHRS) is a Congressionally-mandated program with efforts spearheaded through the Department of Defense (DoD) that will provide the Services with an integrated, multi-component, personnel and pay system. DIMHRS will improve the delivery of military personnel and pay services. The system will provide each Service Member with a single, comprehensive record that will feature self-service capabilities to empower Service Members to update portions of their personal information. See http://www.dimhrs.mil/ for more information.

for in the mission statement of the JFHQ CIO paragraph of the JFHQ Table of Distribution and Allowances.[60]During an incident, the CERT should be used to protect the networks (federal and state as assigned by the Adjutant General). The CERT could support VDEM (and other state agencies) with risk assessments, vulnerability assessments, software and security upgrades and any other information security upgrades required as a training event on regular drill weekends.

Utilizing a standard risk management format and using the CERT to conduct assessments and remediation, the VaNG and VDEM will become more integrated. By doing this work a higher level of trust will develop, reducing many of the cultural barriers to information sharing. This also opens a new mission at the state level for the National Guard and using the CERT, the National Guard can provide better protection of state and federal networks than what currently exists at a very low cost.

Conclusion

> "Critical infrastructure is so vital to the United States that its incapacity would harm the nation's physical security, economic security, or public health. The Federal government has a key role in helping protect the nation's critical infrastructure from all types of hazards through programs of mitigation, preparedness, response and recovery."[61]

As has been shown, each of the conditions mentioned in this quote apply to the information systems and networks that support public safety at the state level. A vital requirement exists for information sharing at all levels of

[60] See the VaARNG JFHQ Table of Distribution and Allowances, managed by the VaARNG G-1.
[61] Paul Parfomak, "Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options", Page 1, Congressional Research Service, RL33206, September 12, 2008. Provided by LTC Jim Begley, NGB J-6 Staff

government, especially between the National Guard and emergency management agencies at the state level.

There are many risks and vulnerabilities that develop when two or more organizations share information. The organizations, during any electronic data exchange, create a condition where there is a greater probability for data loss and network compromises. However, by using available assets in a new way of thinking, the Guard and States can help protect their networks better and become a more integrated organization.

The CERTs available at the state level are a potential force multiplier that is currently unused. “Through the application of available and/or new technologies, states can make targets less vulnerable and thus less attractive. They can limit the damage that may result from an attack, increase the speed of recovery, and provide forensic tools to identify the perpetrators.”[62]This could almost be the doctrinal mission of a JFHQ CERT. True information sharing will not happen until the trust and culture issues are solved. Using the CERT to help mitigate these problems would go a long way to better securing our networks and better serving the nation.

[62] Lewis Brasncomb, “Protecting civil society from terrorism: the search for a sustainable strategy”, Page 273, Technology in Society 26 (2004) 271-285. Available at http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6V80-4BVP317-1&_user=10&_rdoc=1&_fmt=&_orig=search&_sort=d&view=c&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=46ebb5b8db69edb298a32c425299b49e Accessed on 7 February 2009

LIST OF SOURCES

1. Ager, Tryg, Johnson, Christopher and Kiernan, Jerry, "Policy-Based Management and Sharing of sensitive Information among government agencies." *IBM Almaden Research Center*, San Jose, CA 2006. Available at: http://www.almaden.ibm.com/cs/projects/iis/hdb/Publications/papers/milcom2006.pdf Accessed on 24 Feb 2009

2. Baldwin, Kirsten J., and Dahmann, Judith S., "Understanding the current state of US defense systems of systems and the implications for systems engineering." The MITRE Corporation, McLean, Va., 10 April 2008. Available at http://www.acq.osd.mil/sse/outreach/briefs.html Accessed on 7 February 2009

3. Bogdanos, Matthew, "Joint interagency cooperation: The first Step", *JFQ* Issue thirty seven. Available at: http://www.dtic.mil/doctrine/jel/jfq_pubs/issue37.htm Accessed on 24 Feb 2009

4. Branscomb, Lewis "Protecting civil society from terrorism: the search for a sustainable strategy", *Technology in Society*, No 26 5 March 2004. Available at: http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6V80-4BVP317-1&_user=525223&_rdoc=1&_fmt=&_orig=search&_sort=d&view=c&_acct=C000026389&_version=1&_urlVersion=0&_userid=525223&md5=330c8a285bd641f67b661a9f36293b6f Accessed on 24 Feb 2009

5. Brown, Bill, Cutts, Andrew, McGrath, Dennis, Nicol, David M., Smith, Paul, Toefel, Brett, "Simulation of cyber attacks with applications in homeland defense training" *SPIE*, Volume 5071 2003. Available at: http://adsabs.harvard.edu/abs/2003SPIE.5071...63B Accessed on 24 Feb 2009

6. Carafano, James Jay, "Improving the National Response to Catastrophic Disaster", Statement before the Committee on Government Reform, US House of Representatives, September 15, 2005. Available at: http://author.heritage.org/Research/HomelandSecurity/tst091505a.cfm Accessed on 24 Feb 2009

7. Carter, Ashton B., "The Architecture of Government in the Face of Terrorism", *International Security*, Vol 26, No. 3 (Winter 2001/2002). Available at: http://www.mitpressjournals.org/doi/abs/10.1162/016228801753399682 Accessed on 24 Feb 2009

8. Cashell, Brian, Jackson, William D., Jickling, Mark, Webel, Baird. "The Economic Impact of Cyber-Attacks", CRS report for congress, *Congressional Research Service*, The Library of Congress, April 1, 2004. Available at: http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf Accessed on 24 Feb 2009

9. CIO Cyberthreat Response & Reporting Project, "CIO Cyberthreat Response & Reporting Guidelines", CIO Magazine Available at http://www.cio.com/research/security/incident_response.pdf Accessed on 7 February 2009

10. Crocker, Mel "Cross-domain information sharing in a tactical environment", *Cross Talk- The journal of Defense Software Engineering*, Mar 2007 Issue. Available at: http://www.stsc.hill.af.mil/crosstalk/2007/03/0703Crocker.html Accessed on 24 Feb 2009

11. Committee on Homeland Security and Governmental Affairs, "Hurricane Katrina: A Nation Still Unprepared", 109th Congress, 2nd Session, Special Report, S. Rept 109-322. Available at http://www.gpoaccess.gov/serialset/creports/katrinanation.html Accessed on 7 February 2009

12. Dacey, Robert F., "Information sharing responsibilities, challenges, and key management issues", Testimony before the Subcommittee on Cybersecurity, Science, and Research and development and the Subcommittee on Infrastructure and Border Security, Select Committee on Homeland Security, House of Representatives, GAO, GAO-03-1165T, September 17, 2003. Available at http://www.gao.gov/new.items/d031165t.pdf Accessed on 7 February 2009

13. Department of Defense Architecture Framework- Overview available at: http://en.wikipedia.org/wiki/Department_of_Defense_Architecture_Framework Accessed on 24 Feb 2009

14. Department of Defense Directive 5105.77, May 21, 2008 Provided by MAJ Lee Furches, NGB J-6 staff.

15. Department of Defense Directive 8320.02, December 2, 2004 Available at http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf Accessed on 24 Feb 2009

16. Department of Homeland Security News Release "Fact Sheet: Protecting our federal networks against cyber attack" April 8th, 2008 Available at: http://www.dhs.gov/xnews/releases/pr_1207684277498.shtm Accessed on 24 Feb 2009

17. Dizzard, Wilson P. "IT Security calls for Collaboration", *Government Computer News* Mar 03, 2002. Available at: http://gcn.com/articles/2002/03/03/IT-security-calls-for-collaboration.aspx Accessed on 24 Feb 2009

18. Drake, David B., Streckler, Nicole A., and Koch, Marianne J., "Information Sharing in and across government agencies: The role and influence of scientist, politician, and bureaucrat subcultures", Social Science Computer Review 2004. Available at: http://ssc.sagepub.com/cgi/content/abstract/22/1/67 Accessed on 7 February 2009

19. Elting, John, Swords Around a Throne Collier MacMillan Publishers, London, 1988.

20. FEMA Staff, "National Response Framework", Department of Homeland Security, Washington, DC, January 2008, Available at http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf Accessed on 7 March 2009

21. Flowers, Robert L. "Strategies to build a trusted and collaborative information sharing system for state level homeland security" *Naval Postgraduate School*, June 2004. Available at: https://www.hsdl.org/homesec/docs/theses/04Jun_Flowers.pdf&code=74b989ea2fcdc56bf36420d027a367b5?search Accessed on 24 Feb 2009

22. Fritz, Jason, "How China will use cyber warfare to leapfrog in military competitiveness", Cultural Mandela, Vol 8, No 1 October 2008 Provided to the author by LTC Stephan Picard

23. Glenn, Blake, "Geekonomics Author David Rice: "They're not trying to make bad software." E-Commerce Times, 10/15/08 Available at: http://www.ecommercetimes.com/story/64810.html?wlc=1236201379 Accessed on 7 February 2009

24. Government Accountability Office, "Information Sharing: The Federal government needs to establish policies and processes for sharing terrorism-related and sensitive but unclassified information" Report to Congressional Requestors, March 2006. Available at: http://books.google.com/books?hl=en&lr=&id=ZgIgrUwfQS0C&oi=fnd&pg=PA4&dq=Information+Sharing:+The+Federal+government+needs+to+establish+policies+and+processes+for+sharing+terrorism-related+and+sensitive+but+unclassified+information&ots=0wRH2bKzse&sig=rkmsdN3hVVcoE21cUSwmy1FLOh4#PPP1,M1 Accessed on 24 Feb 2009

25. Grimes, John, "DOD Information Sharing Strategy", Internal DOD Policy Memorandum, May 4, 2007. Available at: http://www.defenselink.mil/cio-nii/docs/InfoSharingStrategy.pdf Accessed on 24 Feb 2009

26. http://www.dhs.gov/xinfoshare/programs/gc_1156888108137.shtm

27. http://www.dimhrs.mil/

28. http://en.wikipedia.org/wiki/DoDAF

29. http://en.wikipedia.org/wiki/DOTMLPF

30. http://en.wikipedia.org/wiki/Federal_Enterprise_Architecture

31. http://www.fas.org/sgp/crs/misc/RL30315.pdf

32. http://www.fas.org/irp/doddir/army/fm34-37_97/3-chap.htm

33. http://www.fema.gov/emergency/nims

34. http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf

35. http://www.gao.gov/bestpractices/bpeaguide.pdf

36. http://www.globalsecurity.org/military/systems/ground/win-t.htm

37. http://www.ise.gov/index.html

38. http://www.jfcom.mil/about/fact_safcop.html

39. http://www.ksikoniag.com/Achievements/JIEE/tabid/63/Default.aspx

40. http://www.privacyrights.org/ar/ChronDataBreaches.htm

41. https://safety.army.mil/

42. ISAC Council "Vetting and trust for communications among ISACs and government entities", White Paper January 31, 2004. Available at: http://www.isaccouncil.org/pub/Vetting_and_Trust_013104.pdf Accessed on 24 Feb 2009

43. Janairo, Ed, "States fight against cyber-terrorism", State Government News, March 2002. Available at http://www.csg.org/pubs/Documents/sgn0203StatesFightCyber-Terrorism.pdf Accessed on 7 February 2009

44. The Joint Staff, JROCM 173-06, Provided by MAJ Lee Furches, NGB J-6 Staff

45. Kim, Jin and Allard, William M. "Intelligence preparation of the battlespace: A methodology for homeland security intelligence analysis", *SAIS Review*, vol XXVII no. 1 (Winter-Spring 2008) Available at: http://muse.jhu.edu/journals/sais_review/v028/28.1kim.pdf Accessed on 24 Feb 2009

46. Laipson, Ellen, "New Information and Intelligence needs in the 21st century threat environment" *Henry L. Stimson Center*, Washington DC, 2008. Available at: http://www.stimson.org/domprep/pdf/SEMA-DHS_FINAL.pdf Accessed on 24 Feb 2009

47. Larence, Eileen R., "Definition of the results to be achieved in terrorism related information sharing is needed to guide implementation and Assess progress", GAO-08-637T, July 23, 2008. Available at http://www.gao.gov/new.items/d08637t.pdf Accessed on 7 February 2009.

48. Larence, Eileen R. "Federal Efforts are helping to address some challenges faced by state and local fusion centers", GAO-08-636T, April 17, 2008. Available at http://www.gao.gov/new.items/d08636t.pdf Accessed on 7 February 2009.

49. Lewis, James A. "Assessing the risks of cyber terrorism, cyber war and other cyber threats." Center for Stategic & International Studies, Washington DC, December 2002. Available at: http://www.csis.org/media/csis/pubs/021101_risks_of_cyberterror.pdf Accessed on 7 February 2009

50. Lipowicz, Alice, "GAO: Information sharing lacks definition" *Federal Computer Week*, FCW.com July 23, 2008. Available at: http://fcw.com/articles/2008/07/23/gao-information-sharing-lacks-definition.aspx Accessed on 24 Feb 2009

51. Markle Foundation Task Force, "Creating a Trusted Network for Homeland Security", Markle Foundation, 2003 Available at http://www.markletaskforce.org/Report2_Full_Report.pdf Accessed on 7 February 2009

52. McIntosh, Chris, "Draft VDEM CIO Strategic Plan" Undated, Provided by the Author

53. McIntosh, Chris, "Virginia Interoperability Picture for Emergency Response V.I.P.E.R.", PowerPoint Brief, Undated, provided by the Author.

54. Mosquera, Mary, "DHS, DOD focusing on information sharing", *Washington Technology*, 02/23/06. Available at: http://www.washingtontechnology.com/online/1_1/28049-1.html?topic=daily_news Accessed on 24 Feb 2009

55. Nakashima, Ellen, "Cyber attack data-sharing is lacking, Congress told." The Washington Post, September 19, 2008 page D 02, Available at http://www.industrialdefender.com/general_downloads/news_industry/2008.09.19_cyber_attack_data-sharing_is_lacking.pdf Accessed on 7 February 2009

56. NASCIO "2008 Best Practices in the use of information technology in state government" National *Association of State Chief Information Officers* Available at: http://www.nascio.org/publications Accessed on 24 Feb 2009

57. NASCIO "A blueprint for better government: The Information Sharing Imperative" NASCIO 2005. Available at: http://www.nascio.org/publications Accessed on 24 Feb 2009

58. National Institute of Standards and Technology (NIST), "Managing Risk from Information systems", NIST Special Publication 800-39, Second Public Draft April 2008. Provided to the Author by Dr. Ron Ross of NIST.

59. Parfomak, Paul W. "Vulnerability of concentrated critical infrastructure: Background and Policy Options" CRS Report for Congress, *Congressional Research Service*, Library of Congress, 12 September 2008. Provided to the Author by LTC Jim Begley, NGB J-6 Staff.

60. Powner, David A. “Homeland Security information network needs to be better coordinated with key state and local initiatives”, GAO-07-822T, May 10, 2007. Available at http://www.gao.gov/new.items/d07822t.pdf Accessed on 7 February 2009

61. Program Manager, Information Sharing Environment, “Annual Report to the Congress on the Information Sharing Environment”. *Program Manager, Information Sharing Environment* June 30th 2008. Available at: http://www.ise.gov/docs/reports/Annual-Report-to-Congress-20080702.pdf Accessed on 24 Feb 2009

62. Roberts, Alasdair, “ORCON Creep: Networked Governance, Information Sharing, and the threat to government accountability”, *Campbell Public Affairs Institute*, The Maxwell School of Syracuse University, October 2, 2003, Available at: http://teep.tamu.edu/Npmrc/Roberts2.pdf Accessed on 24 Feb 2009

63. Robinson, Brian “Unlocking the national cybersecurity initiative” *Federal Computer Week*, Sep 17, 2008. Available at: http://fcw.com/articles/2008/09/17/unlocking-the-national-cybersecurity-initiative.aspx Accessed on 24 Feb 2009

64. Ross, Ron “Federal Government Perspectives on Secure Information Sharing” PowerPoint Briefing delivered to the GTSI Technology Leadership Series on August 14th 2007. Available at:http://www.gtsi.com-eblast-vendors-tls-presentations-security.1030_Dr_Ross.ppt.url Accessed on 24 Feb 2009

65. Ron Ross, “Managing Enterprise Security Risk with NIST Standards” *IEEE* August 2007. Provided to the author by Dr. Ross.

66. Staff, “Department of Homeland Security Information Sharing Strategy”, Department of Homeland Security, Washington, DC, April 18, 2008 Available at http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf Accessed on 7 February 2009

67. Staff, “United States Intelligence Community, Information Sharing Strategy”, Director of National Intelligence, Washington, DC, February 22, 2008. Available at http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf Accessed on 7 February 2009

68. Staff Report, “The Cyber Raiders hitting Estonia”, BBC News, 17 May 2007. Available at http://news.bbc.co.uk/2/hi/europe/6665195.stm Accessed on 7 February 2009

69. Staff Report, “New Research shows cyber attack could cost US 50 times more than Katrina”, Market Wire, July 2007. Available at: http://findarticles.com/p/articles/mi_pwwi/is_200707/ai_n19429846 Accessed on 7 February 2009

70. Straw, Joseph, “GAO: Much work remains in information sharing effort” Security *Management*, 07/24/2008 Available at: http://www.securitymanagement.com/news/gao-much-work-remains-information-sharing-effort-004381 Accessed on 24 Feb 2009

71. Thomas, Kenneth R., “Federalism, State Sovereignty, and the Constitution: Basis and Limits of Congressional Power”, Congressional Research Service, RL30315, Library of Congress, Washington, DC, February 1, 2008, Available at http://www.fas.org/sgp/crs/misc/RL30315.pdf Accessed on 7 March 2009

72. The National Commission on Terrorist Attacks upon the United States “The 9/11 Commission report”. Available at http://govinfo.library.unt.edu/911/report/index.htm Accessed on 7 February 2009

73. Townsend, Frances F. “The Federal Response to Hurricane Katrina, Lessons Learned”, The White House February 23, 2006. Available at http://library.stmarytx.edu/acadlib/edocs/katrinawh.pdf Accessed on 7 February 2009

74. United States Code, Section 1385Title 18, "Use of Army and Air Force as Posse Comitatus"

75. US Securities and Exchange Commission, “2008 FISMA Executive Summery Report”, Office of the Inspector General, Office of Audits, Report No. 451 September 29th 2008. Available at http://www.sec-oig.gov/Reports/AuditsInspections/2008/451final.pdf Accessed on 7 February 2009

76. Walsh, David, “Greater Cooperation needed to defeat cyber enemies.” Defense Systems, Information Technology and Net-Centric Warfare, Jan 30, 2009. Available at http://cyberstrategies.wordpress.com/2009/02/04/greater-cooperation-needed-to-defeat-cyber-enemies Accessed on 7 February 2009

77. Zwieback, Dave, “The Gathering Storm: The future of cyber attacks”, CounterStorm, Inc 2005. Available at http://inkcom.com/pdf/inkcom_gathering_storm.pdf Accessed on 7 February 2009