

THE CIP REPORT

CIP Legal Issues

Posse Comitatus I 2

Posse Comitatus II 4

Public to Private Transition .. 6

Identity Theft 7

Jose Padilla 9

CFIUS and CIP 12

Newsletter Editorial Staff

Editors

Jessica Milloy

Jeanne Geers

Staff Writers

Amy Cobb

Randy Jackson

Colleen Hardy

Maeve Dion

JMU Coordinators

John Noftsinger

Ken Newbold

Publishing

Zeichner Risk Analytics

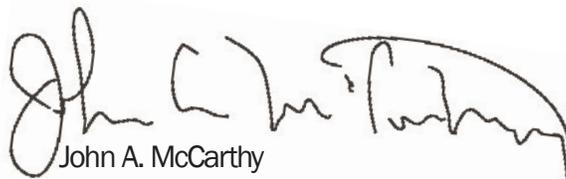
Contact: cipp01@gmu.edu
703.993.4840

If you would like to subscribe to *The CIP Report* please click [here](#). Visit us online for this and other issues at <http://cipp.gmu.edu>

This issue of *The CIP Report* draws together a series of articles on topics germane to critical infrastructure. These topics, such as posse comitatus, identity theft, CFIUS, and the issues surrounding the Padilla case, represent areas of research currently underway at the CIP Program by our legal team. While each of these articles provide only an overview of the entire issue at hand, more information is and will be available online as the research further matures.

In addition to articles by our own internal legal scholars, we have included an article by a current George Mason Law student and a piece on Ed Gibson, Microsoft's UK Chief Security Advisor.

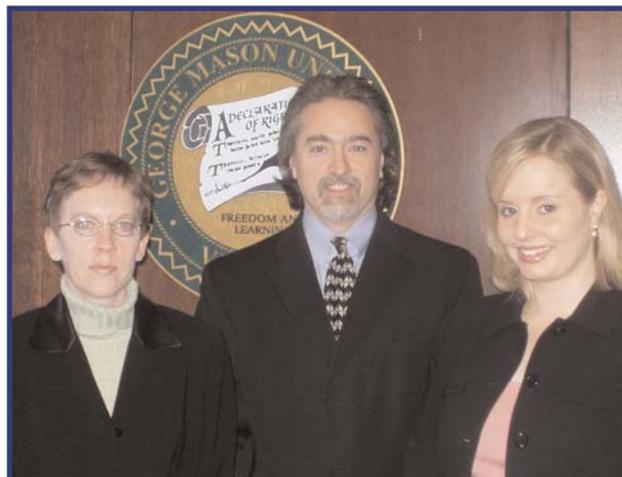
Our legal team is also currently working to produce a monograph on CFIUS, Committee on Foreign Investment in the United States, which will include contributions by Rep. Donald Manzullo (R-IL); Mr. Todd Malan, Executive Director of the Organization for International Investment; David Marchick, Esq., Mark Plotkin, Esq. and David Fagan, Esq. of Covington and Burling; Kristen Neller Verderame, Esq., Chief Counsel BT Americas Inc. and Chair of the British - American Business Council; and Commissioner Patrick Mulloy of the U.S. - China Economic and Security Review Commission, which is available on our website (<http://cipp.gmu.edu/research/>).



John A. McCarthy
Director, Critical Infrastructure Protection Program
George Mason University, School of Law



School of Law
CRITICAL INFRASTRUCTURE
PROTECTION PROGRAM



The CIP Program legal team:
Maeve Dion, Randall
Jackson, and Colleen Hardy.

Posse Comitatus and the Military's Role in Disaster Relief

Randall Jackson, J.D., CIP Program



Introduction

There are currently adequate laws and structures in place to facilitate the use of the military in relief efforts in the event of a major catastrophe of whatever kind. *Posse comitatus* plays a key role in delineating exactly under what circumstances the military *may* and *may not* be used for the explicit purpose of enforcing domestic law. It is of crucial importance for key decision makers within the federal government, state governments and the military (including the National Guard) to understand exactly what is allowed and what is not allowed under various conditions. Steps should be taken to ensure that rules for using the military are clearly understood by all levels of leadership.

Background

Under *posse comitatus*, the Army and Air Force may not be used to enforce domestic law.¹ This status has been extended to include the Marines and the Navy.² It has also been interpreted to apply to the National Guard when federalized (chapter 10 status). However, far from being simply an absolute prohibition, *posse comitatus* additionally delineates under what circumstances the

armed forces may be used for domestic law enforcement. Therefore as a statute, it is just as much empowering as prohibitory. The rather broad conditions under which it empowers the armed forces to enforce domestic law are "*under circumstances expressly authorized by the Constitution or Act of Congress.*"³ A good example of such authorization is the Coast Guard. Although a member of the US Armed Forces, the Coast Guard does not fall under *posse comitatus* because Congress has, through statute, empowered it to enforce domestic law.⁴

Through the years Congress has enacted other legislation aimed at allowing the military into domestic law enforcement under certain circumstances. Broadly speaking, these statutes have tended to involve insurrection or threat to the US from external enemies. The prime example is the "Insurrection Act."⁵ Under the Insurrection Act, in times of civil disturbance or uprising in which "the President considers that unlawful obstructions, combinations, or assemblages, or rebellion against the authority of the United States, make it impracticable to enforce the laws of the United States in any State or Territory by the ordinary course of judicial proceedings"⁶ the military is authorized to enforce domestic law as long as the President has first issued an order to disperse

peaceably and return home. Because law enforcement is authorized, this is a true exception to *posse comitatus*.

Similarly Congress has enacted statutes empowering the military to play a role in interdicting drug flows,⁷ illegal immigration information sharing⁸ and the handling of chemical, biological and nuclear weapons/material.⁹ It must be clearly understood, however, that these latter "exceptions" are not really exceptions to *posse comitatus*. While they create a role for the military in domestic law enforcement operations, that role is still circumscribed and limited to "passive," as opposed to "active" duties. For example, law enforcement authorities may cooperate with military personnel in surveillance operations (thereby making use of the sophisticated training and equipment held by the military), but any actual arrest must be made exclusively by non-military law enforcement personnel.¹⁰ So while the military is brought in to assist domestic law enforcement, it is still remaining passive and therefore technically not enforcing domestic law. *Posse comitatus* remains intact.

The Stafford Act¹¹ is often cited as an exception to *posse comitatus*, however again it is not an exception because it does not empower the military to enforce domestic law. (Continued, Page 3)

Posse Comitatus (Cont. from Page 2) Rather, it outlines how the military may be used for short-term disaster relief.¹² Additionally, there are provisions in the Stafford Act allowing the military to take steps to protect life and property,¹³ but such steps are not to be undertaken as active law enforcement actions.

In regards to quarantine, generally state health officials have primary quarantine authority, while the federal government has authority over inter-state and international quarantine. Although quarantine can affect inter-state commerce, the court has ruled that its health component overrules and allocates quarantine to the police power of the state.¹⁴

Under 42 USC §264 (§361 of the Public Health Service Act), the Secretary of Health and Human Services (HHS) has primary responsibility for preventing the introduction, transmission, and spread of communicable diseases from foreign countries into the United States and within the United States and its territories/possessions. HHS then delegates to the Centers for Disease Control and Prevention (CDC) the authority to detain, medically examine, or conditionally release individuals reasonably believed to be carrying a communicable disease which have been delineated by the President through an Executive Order. If the Director of the CDC determines that steps taken towards quarantine by state and/or local official are inade-

quate, "he/she may take such measures to prevent such spread of the diseases as he/she deems reasonably necessary, including inspection, fumigation, disinfection, sanitation, pest extermination, and destruction of animals or articles believed to be sources of infection."¹⁵ No mention is made of the use of military resources for enforcement purposes (CDC is outside of DoD). However, should the pandemic create a situation in which domestic law cannot be enforced, it is possible the Insurrection Act could be used to authorize quarantine enforcement by the military.¹⁶

The National Guard is sometimes subject to *posse comitatus*, sometimes not. While operating under state jurisdiction (chapter 32 status), it is not subject to *posse comitatus*. However once federalized (chapter 10 status), *posse comitatus* applies. As long as a state's National Guard remains under state control it can act to enforce domestic law, and often does so in times of catastrophe. Retaining this power can be part of the motivation behind a governor's refusal to request federalization.

Analysis

The general thrust of *posse comitatus* and its surrounding statutes is that the military should only be used as domestic law enforcers in the event of some sort of insurrection, uprising or invasion (Insurrection Act). One can argue that this is parallel to the (Continued, Page 15)

Issues for Further Study

I. Perhaps it is time to revisit the Insurrection Act. Because it is the most prominent true exception to *posse comitatus*, perhaps it needs to be broadened to reflect a richer menu of instances in which it could be elicited. Three possibilities regarding such a proposal include:

a. Rename the Insurrection Act, but leave it unchanged. This possibility assumes that the current language of the Insurrection Act sufficiently empowers the military to enforce domestic law in a fairly broad set of circumstances: whenever "the President considers that unlawful obstructions, combinations, or assemblages, or rebellion against the authority of the United States, make it impracticable to enforce the laws of the United States in any State or Territory by the ordinary course of judicial proceedings."¹¹ The potential problem here is any baggage associated with the term "insurrection." Because this word conjures up specific images of attempts to overthrow the government, it may drive leaders to be overly cautious in invoking it, for fear of being accused of overreaching. This seems to have been the case with the Administration and Katrina. Perhaps the Insurrection Act could be renamed as the Domestic Disaster Relief Act or Major Disaster Assistance Act, for example. Alternatively, perhaps the proposals and the original should be combined, rather than eliminating the original (*i.e.* perhaps "insurrection" should remain within the title): *e.g.* the Domestic Disaster Relief and Insurrection Act. The idea is to remove any political stigma from the name and thus empower leadership to look solely to the circumstances of the disaster (Continued, Page 15)

A Call to Arms: Civil Disorder Following Hurricane Katrina Warrants Attack on the Posse Comitatus Act

by Ashley J. Craw, Student, GMU School of Law

Overview

Hurricane Katrina provided policymakers a concrete example of why current laws governing natural disaster response are simply inadequate. The Posse Comitatus Act (PCA) restricts the ability of the armed forces to perform domestic law enforcement functions. While this limitation may be appropriate as a general rule, there are instances where the military might be the best actor to maintain law and order. Over the years, Congress has realized this fact and has enacted a number of statutory exceptions to the PCA, allowing military personnel to perform law enforcement functions in specific situations. Congress ought to pass further legislation to provide another exception to the PCA during and immediately after a large-scale natural disaster. The essay will explore (1) why effective law enforcement is vital to the response effort, (2) why status quo mechanisms are not effective, (3) why current laws do not go far enough to allow military intervention into a natural disaster situation, and (4) why allowing the military to enforce laws would alleviate status quo problems.

A. Effective Law Enforcement is Vital to the Response Effort

While there is no formula to pre-

dict the collective human reaction to a natural disaster, one recurring reaction adds a disturbing and personal element to the destructive force of nature.¹ Crime, looting, and general civil disorder can often arise in the wake of a natural disaster,² creating unique strains on rescue³ and evacuation⁴ efforts. First, worries of crime and looting stalled evacuation efforts, as people were fearful to leave their property. Often able-bodied men and women refused to evacuate Katrina's disaster area due to fears of further property destruction through crime and looting.⁵ A poll taken by Susan Howell, a professor at the University of New Orleans Survey Research Center, revealed that perceptions of crime and safety were the most determinative factors influencing the decisions of New Orleans residents' willingness to evacuate.⁶

Second, civil unrest delayed aid and assistance, as first responders had to restore order before relief could be brought. This process of quelling civil unrest, crime, and mayhem in New Orleans took approximately a week,⁷ and was the primary concern of first responders.⁸ Susan Neely, former Assistant Secretary for Public Affairs at the U.S. Department of Homeland Security, stated, "The big concern is the huge diversion of first

responder resources to contain the civil unrest."⁹ Therefore, one of the first priorities in responding to a natural disaster must be to maintain law and civil order so that assistance, aid, and evacuation efforts can run more smoothly and effectively.

B. Status Quo Mechanisms in the Wake of a Natural Disasters Are Inadequate

Status quo efforts are not adequate to maintain law and order, as evidenced by the fact that authorities were unable to subdue looting and crime in the immediate aftermath of Hurricanes Hugo¹⁰ and Katrina.¹¹ There are many logistical factors that hinder efforts to quell civil disorder after natural disasters. First, disaster areas are often so large that there simply is not enough manpower to control the region.¹² On September 3, 2005, President George W. Bush stated, "The magnitude of responding to a crisis over a disaster area that is larger than the size of Great Britain has created tremendous problems that have strained state and local capabilities."¹³ In fact, White House reports indicate that Hurricane Katrina was one of the largest natural disasters in the history of the United States, with damage to over 90,000 square miles in Louisiana, (*Continued, Page 5*)

Call to Arms (Cont. from Page 4) Mississippi, and Alabama.¹⁴

Second, there are simply not enough personnel to handle immediate law enforcement concerns, as state and local police lack manpower. For instance, New Orleans already had a strained and undermanned police force, consisting of only 1,500 officers.¹⁵ By September 5, 2005, only two-thirds of the New Orleans Police Force reported to work.¹⁶ This is not terribly surprising, as over seventy percent of the New Orleans Police Force had homes that were damaged or destroyed by Hurricane Katrina.¹⁷ Further, many local police officers had to evacuate and safeguard their own families, adding further stress to the chaos following a disaster.¹⁸

Third, National Guard response to a disaster can be slow, as troops must be called to duty, be noti-

fied that they must report to duty, actually report to duty, and then be organized and deployed to a disaster site. This multi-tiered process of calling and deploying National Guard troops is cumbersome, inefficient, and reliant on infrastructure (telephone networks, transportation, etc.) that may be damaged in the disaster. Although Hurricane Katrina made landfall on Monday, August 29, 2005,¹⁹ National Guard troops did not arrive to the area until Friday, September 2, 2005.²⁰ As mayhem and lawlessness ensued immediately following the hurricane, this delay of four days in responding to the crisis meant that National Guard troops played a minimal role in maintaining civil order.

C. Current Law Does Not Allow the Armed Forces to Enforce Civil Law

The Insurrection Act is often cited

as a mechanism by which President Bush could have directed military troops to enforce domestic law in Katrina's wake. However, a closer look at the Insurrection Act would reveal that this power is strained at best. The Insurrection Act allows the President to use a military force to control civil unrest in times of insurrection against state and local government.²¹ Black's Law Dictionary defines an insurrection as, "A violent revolt against an oppressive authority, usu[ally] a government."²² Further, Corpus Juris Secundum notes that:

*"Insurrection is distinguished from rout, riot, and offense connected with mob violence by the fact that in insurrection there is an organized and armed uprising against authority or operations of government, while crimes growing out of mob violence, however serious they may be and however numerous the participants, are simply unlawful acts in disturbance of the peace which do not threaten the stability of the government or the existence of political society."*²³

The Insurrection Act was used most recently in 1992, when California Governor Pete Wilson asked President George H.W. Bush for federal troops to help quell the Los Angeles riots.²⁴ In that instance, the riots that arose from an unpopular court decision were a challenge to the judiciary. Therefore, the Los Angeles riots were not senseless acts of violence, but instead were organized with the purpose of showing defiance to (Continued, Page 18)



New Orleans, LA., 10/17/2005 – National Guardsman, SGT Shawn on patrol in the 9th Ward neighborhood following Hurricane Katrina. FEMA photo/Andrea Booher

Public to Private Transitions: A Case Study

by John Elkington

Last year, a global software company chose a new chief security officer for its UK division. In an unusual move, the company did not cull its new security chief from the private sector IT ranks, but rather chose an individual with an extensive background in public sector law enforcement. This article is not meant as an endorsement of a specific product or company; the author provided this interview as an interesting case study of a security executive shifting from the public to the private sector.

The lights go down. The audience quiets. And the stage is taken by a man sporting dark glasses. Who - or what - is he? Hollywood superstar? Bono of U2? You're getting warmer with U2 as spy planes, but still no. The mystery man, it turns out, is no stranger to the undercover worlds of the CIA and FBI. He is Gibson. Ed Gibson. Microsoft's UK Chief Security Advisor. And you'd better hope that this one-time FBI agent manages to pull off the almost superhuman task set for him by Bill Gates & Co. If not, he warns, the Internet could be taken over by dark forces and rendered unfit for most of us.

Just as security comes in many different forms - military, economic, social, psychological, environmental - so does insecurity. And who do we blame when our computer is invaded by a virus,

Trojan or worm? Well, that's simple. Not the hacker, but our software supplier.



Ed Gibson is the UK Chief Security Advisor for Microsoft

Visit Microsoft's website, for example, and you are treated to details of the latest threats, including the Zotob-A worm when I last looked. There will also be a promise that the company can help you keep security threats at bay. Well, up to a point. Like the dreadnought builders of the early 20th century or the H-bomb builders of the latter part of the century, software developers are caught in a dizzying, arms race with rogue software writers. And sometimes these people break through the IT world's equivalent of levees, causing spectacular economic damage in the process.

So what to do if you're a software company? Traditionally, you found a super-geek, maybe even a former hacker, and you turned them

on your e-foes. This time, however, Microsoft took a different tack, headhunting the man in shades. And, in doing so, they acknowledged the fact that cyber attacks and scams have moved from kids and hobbyists experimenting to criminals who are both organised and increasingly sophisticated in their scams and crimes.

So, in the spirit of his G-man past, I ask Gibson whether he stepped into a dead man's shoes at Microsoft? No, he replies. He took over earlier this year from Stuart Okin, who had moved to Accenture. "I know Stuart very well and have great respect for his expertise," Gibson says. "But I hail from a completely different background - legal and law enforcement." Prior to his five year diplomatic assignment at the US Embassy in London with the FBI, Gibson was an FBI expert in the investigation of complex white-collar crime, intellectual property rights theft, and other forms of financial crime. As far as the technical side goes, "Microsoft UK is bringing on board a technical advisor, so when I'm working at the 30,000 foot level we also have someone who is comfortable with bits and bytes."

And the shades? He took to wearing them when he moved to the UK as the FBI's assistant legal attaché, *(Continued, Page 19)*

Identity Theft and the Information Security Breaches of 2005: What Have We Learned?

by Maeve Dion, CIP Program



In this Information Age, liabilities and regulations regarding the flow of information affect both critical

and non-critical industries.

Businesses and governments should be establishing strategies and gathering the data necessary to assess risk, demonstrate reasonable security, or justify additional legislation / regulatory controls.

Identity theft was one of the hottest topics of 2005. Although the level of attention was high, there was little consensus on (1) how to define the "identity theft / security breach" problem (if there even is one); (2) how to quantify the problem; (3) how to measure its costs; (4) who should correct the problem (industry self-regulation or legislation by states or Congress or both); and (5) what oversight mechanisms should be established to monitor the problem.

Congress opened 2006 with a Supreme Court confirmation process, hearings on warrantless government eavesdropping, discussions of lobbying and Congressional ethics, and further PATRIOT Act debates. These issues might legitimately divert

attention from what some have called an "identity theft crisis," but one more large-scale security breach could bring this debate back into the spotlight. Without the immediate pressure of reactive legislation, now is a good time for business and policy analysts to reassess identity theft concerns in order to provide better guidance to both the private sector and state and federal governments.

Impediments to Risk Analysis

Definitions / Language

The phrase "identity theft" is often used without the speaker first defining its meaning. Definitions are important because the speaker may be alluding to only one aspect of identity theft (e.g., credit card fraud). Most people think of identity theft in terms of financial loss from identity fraud, yet identity theft may lead to numerous consequences, not all of which appear on a credit card statement or consumer report.

In very general terms, when someone takes another person's identity information with the intent to commit a crime or transfer the information to another wrongdoer, the initial taking itself is a crime. Thus identity theft can occur without the victim¹ having experienced monetary or reputational loss. The victim may addi-

tionally suffer harm from (1) financial fraud, (2) impersonation by the wrongdoer during criminal acts (the wrongdoer proffers the stolen identity to a law enforcement officer when detained for committing a crime), and (3) impersonation during other acts (leasing an apartment, getting a job, etc.).

Specific language is also important when discussing security breaches and identity theft statistics. Media may report that "2005 saw the most computer security breaches ever,"² but this phrase may – or may not – be true. In fact, 2005 saw the most *disclosures* of security breaches, due to a California law. Also, claiming that more than 55 million Americans faced the possibility of identity fraud from "130 major intrusions"³ is not conducive to good consumer education when (1) security breach disclosures reference the number of accounts potentially affected, not the number of individuals (one person may suffer account compromises in multiple security breaches); (2) forty of the 55 million (more than 70% of the reported statistic) occurred from one incident – CardSystems; (3) more than nine million account compromises occurred from loss of storage media or theft of hardware – neither of which are traditionally categorized as an "intrusion" into
(Continued, Page 8)

2005 in Review

- Disclosures of security breaches by businesses, universities, and government departments, potentially compromising more than 50 million accounts.
- Ten separate Congressional hearings on information security breaches and identity theft.
- The introduction of more than a dozen different Congressional bills relating to consumer notification and safeguards, and another half-dozen bills addressing other aspects of identity theft.
- The enactment of identity-theft-related legislation in twenty-seven states.
- A handful of new state security freeze laws regarding consumer reports (resulting in a total of about twelve states with such laws).

Identity Theft (*Cont. from Page 7*) a computer system, and both of which require different solutions for remediation and prevention; and (4) a "major intrusion" is not defined – a compromise of 1,000 university student identification numbers is not the same as 10,000 credit card accounts or 100,000 social security numbers.

Part of the language problem the media suffers is the same problem facing business, regulatory bodies, and legislators – we cannot reliably talk about identity theft and its consequences when we do not have the proper metrics for identifying the costs, diagnosing the causes, or suggesting solutions.

Metrics

While the lack of consensus regarding the identity theft "crisis" may be merely a result of the traditional give-and-take of business and consumer interests, a stronger rationale may be the absence of the necessary data to

properly analyze the risks⁴ of identity theft. Data regarding an identity theft may be collected from three sources – the entity who suffers the compromise, the victim whose identity was stolen, and law enforcement. However, this data may be ascertained out of sequence or may never be discovered at all.

For example, law enforcement officers may unearth a stash of stolen identities while investigating a methamphetamine operation. There may be little evidence as to how the wrongdoer obtained the identities – they could have been purchased on the black market, acquired by hacking into a computer system, or obtained via non-technological methods like stealing mail. If the wrongdoer pleads to the methamphetamine charge, law enforcement may drop the lesser identity theft charge, and therefore investigation of the identity theft is not a priority. It thus remains a question as to (1) whether the individuals whose

identities were stolen will ever be informed of law enforcement's discovery, and (2) whether the entity whose security was compromised will ever learn that someone accessed its property and stole the information.

On the other hand, a victim may find fraudulently-opened accounts listed in the victim's consumer report. The victim will then work with credit reporting agencies, and maybe law enforcement and financial services providers, to report the fraud. However, skillfully concealed behind false addresses and identities, the wrongdoer may never be identified. Once again, the victim may not be able to determine how the wrongdoer acquired the victim's identity. Further, if the identity information was not stolen from the victim directly, but was taken from another entity, that entity may never learn about the information security breach (unless the breach was independently detected).
(Continued, Page 20)

Jose Padilla

by Colleen Hardy, J.D., CIP Program



The horrific terrorist attacks on September 11th 2001 generated several changes within the United States. Primarily, it changed U.S. citizens' perceptions and understandings that the U.S. is not immune from terrorist attacks. On an individual level, it changed the way U.S. citizens travel, as demonstrated by more stringent security at airports and other transportation venues, such as subway screening. Additionally, the terrorist acts affected U.S. laws focusing on national security. The United States Government determined that changes to current laws were needed to protect the United States from another tragedy like September 11. These adaptations have caused concern that the government may have exceeded their breadth of authority and led to a key question - how far can and should the government go to protect citizens from another attack? The apprehension of an American citizen in Chicago, declared an enemy combatant by the government, addresses the primary issue of whether a U.S. citizen detained on American soil can be held without trial in the name of the war on terrorism.

The United States Constitution

affords definitive and manifest rights to United States citizens. An imperative right is under the Sixth Amendment, which grants a citizen the right to counsel when charges have been filed against him or her. Another key right critical to this discussion is found under the Fourteenth Amendment, which grants a citizen the right to due process of law. Customarily, U.S. citizens may not be detained without being charged for a crime. However, this has not been the case for Jose Padilla.

The government has asserted that Padilla is an enemy combatant, and as such, is not entitled to an attorney and may be detained without any charges filed against him. An enemy combatant is defined in the Joint Doctrine for Detainee Operations as an additional classification of detainees who through, their own conduct, are not entitled to the privileges and protection of the Geneva Conventions.

Jose Padilla was born in New York City, and after his father died when Padilla was four years old, his mother moved the family to Chicago. As a teenager, Padilla joined a street gang, the Latin Kings. Padilla's first run in with the law was when he was 14. Allegedly, he and six other juveniles robbed and viciously attacked two members of a rival gang, one who died from his injuries. Padilla was convicted of the juvenile equivalent to aggravated assault and armed robbery.

After his release from the juvenile detention center, Padilla moved to Florida. In October 1991, he was arrested for brandishing a gun out of his car window during a road-rage incident. In 1996, Padilla married his girlfriend, Cherie Stultz.

It is unclear when Padilla's curiosity towards Islam matured. Some speculate he became inquisitive while in jail and others state that one of his fellow Taco Bell employees, who was Muslim, influenced him. Subsequently, Padilla informed his coworkers at Taco Bell that he and his wife had converted to Islam and his name was now Abdul al Muhajir. According to Seamus McGraw, an author for Court TV's Crime Lab, this name is commonly associated with Muslim warriors.

Padilla's wife filed for divorce in 2000 and informed the court that she had not seen him since 1998 when he had moved to Cairo. Although Padilla's whereabouts and actions are indeterminate from this point forward, the United States government at this time became interested in Padilla. The government maintains that he attended an al Qaeda training camp in Afghanistan. They also claim he spent time in Pakistan where he was trained in radiological weapons and wiring bombs. The government's attention and curiosity in Padilla grew in February 2002 when he tried to get another (*Continued, Page 11*)

Jose Padilla Timeline

DATE	EVENT
May 8, 2002	Jose Padilla is apprehended by FBI agents at Chicago O'Hare Airport
June 9, 2002	President Bush declares Padilla an "enemy combatant" and orders Padilla to be transferred to military custody in South Carolina
June 11, 2002	Donna Newman, Padilla's attorney, files Habeas Corpus* as next friend, in New York against George W. Bush, Donald Rumsfeld, and Commander M.A. Marr
June 26, 2002	Government files motion to dismiss stating that Newman lacks standing to establish next friend status and that the court lacks jurisdiction over respondents and finally that the case should be transferred to South Carolina
Dec 4, 2002	The District Court for the Southern District of New York denies transferring the case to South Carolina and rules that Newman may act as next friend to Padilla and finally <i>dismisses</i> case against all but Rumsfeld
July 2003	Both parties appeal to the United States Court of Appeals for the Second Circuit
Dec 18, 2003	The United States Court of Appeals for the Second Circuit ruled that Padilla cannot be held as an enemy combatant and ordered his release
Jan 16, 2004	The government files a petition with the United States Supreme Court for a writ of certiorari*
Jan 16, 2004	The government files a motion with the Supreme Court to expedite consideration of the petition for writ of certiorari
Jan 23, 2004	The Supreme Court grants the government's motion to expedite consideration of the petition for writ of certiorari
Feb 20, 2004	The Supreme Court grants the petition for writ of certiorari
June 28, 2004	The Supreme Court rules that the case has been improperly filed in New York and should have been filed in the District Court for the District of South Carolina
July 2, 2004	Padilla files a petition for writ of Habeas Corpus in District Court of South Carolina and asserts that he has not been allowed to meet with or communicate with his attorney from June 9, 2002 to March 2004. Padilla also files a motion for summary judgment
Feb 28, 2005	The South Carolina District Court grants Habeas Corpus and orders Rumsfeld to release Padilla within 45 days and also grants Padilla's motion for summary judgment
Spring 2005	The government files an appeal to the Court of Appeals for the Fourth Circuit
Spring 2005	The government files with the United States Supreme Court a petition for a writ of certiorari before judgment to the United States Court of Appeals for the Fourth Circuit
June 13, 2005	The United States Supreme Court denied petition for a writ of certiorari before judgment to the United States Court of Appeals for the Fourth Circuit
Sep 9, 2005	The Court of Appeals for the Fourth Circuit reverses the District Court's order to release Padilla
Oct 25, 2005	Padilla appealed to the United States Supreme Court
Nov 17, 2005	Padilla indicted by Miami federal grand jury for conspiracy to murder U.S. nationals, conspiracy to provide material support to terrorists and providing material support to terrorists
Nov 22, 2005	The government filed a motion with Court of Appeals for the Fourth Circuit to authorize the immediate transfer of Padilla from military custody to civilian law enforcement custody in the state of Florida

(Padilla Timeline Continued)

DATE	EVENT
Dec 21, 2005	The Court of Appeals for the Fourth Circuit denied both of the government's request
Dec 28, 2005	The government filed a request to the United States Supreme Court for Padilla's immediate transfer from military custody to law enforcement in Florida
Dec 30, 2005	Padilla's attorney seeks to have Padilla remain in military custody until the Supreme Court decides his constitutional challenges
Jan 4, 2006	The United States Supreme Court ordered Padilla to be transferred from military custody to stand trial in Miami, Florida HOWEVER the Supreme Court is still considering his constitutional challenge
Jan 6, 2006	Padilla is transferred from military brig in South Carolina to Miami Florida
Jan 6, 2006	Padilla makes his first court appearance since May 2002 at a hearing where he was asked if he understood his rights as a criminal defendant. Padilla replied that he did understand them
Jan 12, 2006	Padilla's arraignment. Padilla pleaded not guilty and bail was denied because of the seriousness of the charges
Jan 13, 2006	The United States Supreme Court met behind closed doors to determine whether the case is moot since Padilla is no longer in military custody or they will define the president's power over United States citizens who are detained in the U.S. on suspicion of terrorist activity – Their decision has not been released as of yet.
Fall 2006	Padilla's trial is set to begin The four other men charged with Padilla trial is set to begin

*Habeas Corpus: it is a writ (court order) which directs the law enforcement officials (prison administrators, police or sheriff) who have custody of a prisoner to appear in court with the prisoner to help the judge determine whether the prisoner is lawfully in prison or jail.

*Certiorari: a writ (order) of a higher court to a lower court to send all the documents in a case to it so the higher court can review the lower court's decision.

Jose Padilla (*Cont. from Page 9*) passport from a U.S. Consulate in Pakistan, after claiming he had lost his.

In June 2002, Abu Zabaydah, the senior deputy to al Qaeda leader Osama bin Laden, was apprehended in Pakistan. Zabaydah divulged information about an American recruit to al Qaeda. Zabaydah stated he could not identify the American's name but knew that he had planned to manufacture and detonate a radiological bomb in the United States. Zabaydah stated that he directed the American to operatives in Pakistan to help him carry

out his attack. Based on this information and Padilla's previous actions, Padilla was placed on a watch list.

Jose Padilla, who maintained his United States citizenship, was apprehended by federal agents on May 8, 2002 at Chicago O'Hare Airport upon returning from Pakistan. In New York, U.S. District Court Judge Michael Mukasey authorized the material witness warrant. Padilla was brought to New York before Judge Mukasey, who appointed Padilla an attorney. On June 9, 2002 President Bush declared Padilla an enemy combatant and ordered him to

be detained in a military brig in South Carolina. The next day, Attorney General John Ashcroft stated, "We have captured a known terrorist who was exploring a plan to build and explode a radiological device or 'dirty bomb' in the United States."

Jose Padilla was detained in South Carolina as an enemy combatant from June 2002 through January 2006. During this time, Padilla did not have any contact with his family. According to Padilla's petition for habeas corpus, he was not allowed to meet with, nor communicate with his attorney from June 9, 2002 to March 2004. (*Continued, Page 23*)

CFIUS and Critical Infrastructure Protection

A New CIP Program Monograph

Randall Jackson and Maeve Dion

It is with great pleasure that the George Mason University School of Law's Critical Infrastructure Protection (CIP) Program will be publishing a monograph on the Committee on Foreign Investment in the United States (CFIUS). With the recent attempts by foreign interests to acquire high-profile US energy and technology assets fresh in the nation's mind, a rich debate is brewing over the CFIUS process and the degree to which it is or is not adequately addressing the needs of the United States.

The monograph features articles by leading thinkers representing diverse points of view on CFIUS and its role in protecting critical infrastructure. Authors include Rep. Donald Manzullo (R-IL); Mr. Todd Malan, Executive Director of the Organization for International Investment; David Marchick, Esq., Mark Plotkin, Esq. and David Fagan, Esq. of Covington and Burling (Mr. Marchick has recently authored a book on the subject); Kristen Verderame, Esq., Chief Counsel BT Americas Inc. and Chair of the British-American Business Council; and Commissioner Patrick Mulloy of the US-China Economic and Security Review Commission. The monograph is available through the CIP Program website.

Traditionally, critical infrastructure protection and foreign direct investment have intersected over the issues of companies supplying the Pentagon or companies involved with "dual use" technologies. Policymakers were leery of (1) putting Pentagon supplies in the hands of non-US entities and (2) providing foreign militaries and third-party purchasers with technology that could be put to a dual use (e.g., in weapons used against the US). These issues were deemed too big of a threat to allow to go unregulated.

The legislation behind the Committee on Foreign Investment in the US (CFIUS) is Section 5021 of the Omnibus Trade and Competitiveness Act of 1988. This Act amended Section 721 of the Defense Production Act of 1950 to provide authority to the President to suspend or prohibit any foreign acquisition, merger or takeover of a US corporation that is determined to threaten the national security of the United States. The President can exercise this authority under section 721 (also known as the "Exon-Florio provision") to block the potential private business transaction. In 1993 the Exon-Florio provision was further amended under Section 837(a) of the National Defense Authorization Act for Fiscal Year 1993, called the "Byrd

Amendment." The Byrd Amendment required an investigation anytime "the acquirer is controlled by or acting on behalf of a foreign government and the acquisition 'could result in control of a person engaged in interstate commerce in the U.S. that could affect the national security of the U.S.'"

Recently, lawmakers have been suggesting that "national security" needs to be more broadly defined in the context of CFIUS. Senator Richard Shelby (R-AL) and Congressman Donald Manzullo (R-IL) have led the charge to restructure the CFIUS mechanism to include issues of economic and energy security along with the more traditional military procurement and dual use issues. Two recent cases illustrate the new focus.

The first case is the Lenovo-IBM case. IBM agreed to sell its PC division to the Lenovo Group, Ltd. for \$1.7 billion. The Lenovo Group is partially owned by the Chinese government, and would therefore allow the Chinese government access to important PC technology and research and development. Critics envisioned a scenario in which the US government would find itself buying important PC technology from the Chinese government. While this is similar to (*Continued, Page 13*)

CFIUS (Cont. from Page 12) the traditional fears addressed by CFIUS, in this case there was a further concern of a loss of competitiveness should Lenovo gain not just the technology, but also the distribution network and recognition held by IBM. Such a contingency was described as a real threat to US national security through its economic threat to competitiveness and market access. For some critics, the situation is exacerbated by the lack of a "level playing field" as regards US investment in China – i.e., the absence of reciprocal agreements.

Specifically, opponents point out that if the US allows investment opportunities to companies partially owned by the Chinese government, the Chinese government must be required to allow US firms equal access to purchases of Chinese companies, including those publicly held. Another minor concern voiced in these debates was the historical Chinese lack of respect and enforcement of foreign intellectual property ownership. In the end, the Lenovo deal was accepted by CFIUS and went through.

In the second case CNOOC, again a company partially owned by the Chinese government, bid to purchase Unocal, a US oil company. With tremendous growth rates over the last decade, the Chinese economy's need for oil has expanded and will continue to grow rapidly in the future. For this reason, the Chinese government has been urgently trying to acquire new, secure sources of

oil. In addition to trying to buy Unocal, other Chinese initiatives have included entering into extensive deals with Zimbabwe, Venezuela and Sudan. Opponents to the CNOOC deal, and to the current CFIUS structure in general, argue that access to oil (and other key energy sources) is as much a critical infrastructure to the US as any other, and therefore must be carefully protected. For this reason, they wish CFIUS to explicitly take into consideration energy issues when evaluating a proposed investment. Additionally, because CNOOC is government-owned, it receives access to vast amounts of capital that would not usually be attainable in normal capital markets - another unfair business advantage in the eyes of critics. Such concerns have not been traditionally a part of the lexicon of issues thought about when evaluating foreign direct investment legislation, but some would argue that now they should. Due to the opposition against the deal, CNOOC ultimately withdrew its Unocal offer before reaching the CFIUS review stage.

Further important issues that flow from CFIUS evaluations of foreign direct investment are the issues of offshoring and greenfield investments (e.g., foreign companies establishing factories in the US). Except in limited circumstances, neither of these actions are covered by CFIUS or any other standardized regulatory scheme. Yet, by offshoring, US firms are outsourcing or setting up shop in foreign countries and

hiring local people to carry out various functions which could have an impact on US security. For example, many software companies now outsource to India, but with the recent string of fraud accusations coming out of India, one could question the security of allowing companies to write important code in Indian plants (or any other low-wage country where law enforcement regimes may lack needed resources). As regards greenfield investment, at present there is nothing to stop a foreign company from (1) establishing facilities that interact with or supply US critical infrastructure businesses, or (2) setting up shop in a technology-rich part of the US and hiring leading experts. To this point, trying to regulate such actions were seen as overly intrusive and as creating huge disincentives to investment and economic expansion. But if the debate on CFIUS leads to an expansion of the level of rigor applied, and an expanding of the areas in which national security is protected, perhaps it is time to think about a similar regime for offshoring and greenfield investments – especially since the rate of offshoring is rapidly increasing. At least it may be important to think about these areas and make an informed decision to not intervene. We would then know that actions or the lack thereof are based on a considered decision and not on neglect.

There is an additional issue which has received a fair amount of attention amongst legislators, but is not (*Continued, Page 14*)

CFIUS (Cont. from Page 13) really a critical infrastructure protection issue. It is an issue that emerged in the CNOOC case and involves the impact upon key allies of the purchase of a US company. Unocal is a large producer of natural gas in Indonesia. CNOOC (prior to a Unocal purchase) is also a large natural gas producer in Indonesia. Should CNOOC have acquired Unocal, it would have had control over a significant percentage of that country's production of natural gas. At the same time, Indonesia is a key supplier of natural gas to Taiwan (60%), as well as Japan and South Korea. Therefore an indirect outcome of a sale of Unocal to CNOOC would have been to put a significant portion of Taiwan's energy source under Beijing's control. Similarly, Unocal holds a significant interest in Azerbaijan in the Caspian region. China has put pressure on the Azeris to do more business with members of the Shanghai Cooperation Organization (Russia, China, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan). Obtaining Unocal's interest in Azerbaijan could have pushed Baku to be more accommodating

to Beijing's and Moscow's wishes. Such concerns have not been traditionally a part of the lexicon of issues thought about when evaluating foreign direct investment legislation, but some would argue that now they should. Again, this is a bit distinct from critical infrastructure per se, but may come up in discussions around the need to strengthen CFIUS oversight.

In sum, US critical infrastructure businesses could be impacted by:

- Insider threats at a foreign-owned domestic company because of lax security (the CFIUS issue - this currently does not apply to greenfield investments).
- Third-party infiltration of a foreign-owned domestic company because of lax security (the CFIUS issue this currently does not apply to greenfield investments).
- Economic and security disadvantages of foreign exclusionary control of necessary resources for critical infrastructure (CFIUS and expanded CFIUS).
- Economic disadvantages from lack of competitiveness (the argument for expanding CFIUS).
- Economic disadvantages from lack of access to natural resources (the argument for expanding CFIUS).
- Insider threats at lesser secured offshored facilities, whether domestically-owned or outsourced (application of CFIUS concerns to offshoring).
- Third-party infiltration at lesser secured offshored facilities, whether domestically-owned or outsourced (application of CFIUS concerns to offshoring).
- Technological threats to our interconnected information infrastructure by entities who gain access to lesser secured offshored facilities (application of CFIUS concerns to offshoring).
- Third-parties acquiring knowledge and technology after gaining access to lesser secured offshored facilities (application of CFIUS concerns to offshoring).

The CIP Program is very pleased to undertake this project. We look forward to the spirited debate it will hopefully bring forth. ❖

Posse Comitatus (Cont. from Page 3) military's chief mission of protecting the country from external threat. Statutes such as the Stafford Act wherein the military is empowered to play a role, but still prohibited from enforcing domestic law, do not affect *posse comitatus* standing. The question is whether or not lawless activity following a catastrophe such as Katrina can be defined as rising to the level of insurrection, even if the activity is aimed not at insurrection *per se*, but rather general looting and lawlessness.

It would seem that the federal government did not see the activity surrounding Katrina as rising to the level of insurrection because it did not invoke the Insurrection Act. However, upon closer look, it appears that political considerations more than technical legal considerations may have carried the day. In a September 9, 2005, article in the *New York Times*, it was reported that President Bush's advisors had debated whether or not to invoke the Insurrection Act to speed federal intervention and more quickly stop lawless behavior. However the Administration became wary of the reaction to President Bush overriding a southern Democratic governor. A senior Administration official was quoted in the article as saying, "[c]an you imagine how it would have been perceived if a president of the United States of one party had pre-emptively taken from the female governor of another party the command and control of her forces, *unless the security situation made it completely clear that she was*

unable to effectively execute her command authority and that lawlessness was the inevitable result?"¹⁷ The clear message here is that the necessary legal authority existed through the Insurrection Act (the italicized language very strongly reflects the language of the Act); the concern was the politics of the specific situation.

Had the political situation been perceived differently, the federal government could have intervened under the authority of the Insurrection Act. Such an invocation would have suspended *posse comitatus* and allowed the military to act as law enforcement officers to restrict the looting and general lawlessness. No additional legislation or statutes would have been needed - simply an appropriate usage of the structure already in place.

Under the Stafford Act, and appropriate to the federal structure of the US, disaster relief remains under the purview of the state governor. The President may act directly if the event transpires on federally controlled land, such as the Oklahoma City bombing, but otherwise requires a request from the governor in order to send federal support. In the case of Katrina, a request was sent by Governor Blanco on August 27 to receive federal assistance. That request did not include a request that the Louisiana National Guard change to chapter 10 status. Other than by request from the governor, federalization may only occur by Congress if (Continued, Page 16)

Issues for Further Study (Cont. from Page 3) for guidance as to whether or not to turn to the Act.

b. Change the language of the statute and rename. Perhaps it is appropriate to more explicitly state the circumstances which entail "unlawful obstructions, combinations, or assemblages, or rebellion against the authority of the United States, make it impracticable to enforce the laws of the United States in any State or Territory by the ordinary course of judicial proceedings."² Instances of looting and other lawless behavior in the aftermath of a major catastrophe perhaps should be explicitly cited as grounds for invoking this Act in order to empower the military to temporarily enforce domestic law until civilian authorities can recover. Perhaps a clause could be added pointing to a situation in which an extreme disaster may have eliminated local and state authority. Adding language regarding a possible role for the military in enforcing a quarantine might also help to clarify and appropriately empower the military to help.

There is precedence for this in the Immediate Response Authority DoD doctrine which allows commanders to provide resources and assistance to civil authorities without or prior to a declaration under the Stafford Act when a disaster overwhelms the capabilities of local authorities and necessitates immediate action. The immediate response authority may also include law enforcement activities that would ordinarily be prohibited by *posse comitatus*. The controlling directive does not require a request from state or local officials, but states that

"DoD Components shall not perform any function of civil government unless absolutely (Continued, Page 16)

Posse Comitatus (Cont. from Page 15) it determines "that more units and organizations are needed for the national security"¹⁸; or by the President if needed to repel invasion or put down insurrection.¹⁹ Governor Blanco came under a lot of pressure to make the request, but ultimately decided to retain state control, informing the White House minutes before a news conference at which the President had hoped to announce the switch to chapter 10 status.

Retaining the state National Guard under state control is important for maintaining critical resources for the governor. By keeping the National Guard under state control, it can continue to play a role in domestic law enforcement. By switching to chapter 10, the National Guard can no longer play this role, leaving it to state and local police officers. If they had been previously relying upon National Guard units, this can create a serious vacuum.

When the National Guard remains in chapter 32 status and federal troops also aid in disaster relief, a shared command structure is created. In the case of Katrina, Louisiana's Adjutant General, Maj. Gen. Bennett Landreneau and the commander of Joint Task Force Katrina, Lt. Gen. Russel Honore, shared command. This essentially means that they kept control of their respective forces and coordinated their efforts. The White House had proposed creating a dual-reporting structure. In this

unusual scenario the Louisiana National Guard would have been federalized (thus putting all operations under Lt. Gen. Honore's control) but Lt. Gen. Honore would have reported to both Gov. Blanco and the President. The Governor rejected this proposal for fear of losing control of the Guard and undermining the efforts of Maj. Gen. Bennett Landreneau.²⁰

In a major disaster, the military can play an important role by bringing to bear equipment, training and expertise vital to rapid and efficient relief efforts. But these skills are not law enforcement. They include providing shelter, clearing debris, providing rescue operations and other physical operations requiring sophisticated logistical coordination and execution. Regardless of *posse comitatus*, the military can and should perform this role. *Posse comitatus* is simply not relevant to these functions. Where it does become critical is law enforcement. The military can not, and should not be asked to function as a domestic law enforcement entity. The Department of Defense (DoD) is amongst the most vocal supporters of this position. To begin with, DoD sees its mission as war fighting. Redirecting resources to domestic operations can serve to weaken the military's war fighting capability. Therefore relief undertakings should be quick and limited to the immediate needs that the equipment and training of the military can fulfill. Furthermore, training appropriate to war zones, (Continued, Page 17)

Issues for Further Study (Cont. from Page 15) necessary on a temporary basis under conditions of Immediate Response. Any commander who is directed, or undertakes, to perform such functions shall facilitate the reestablishment of civil responsibility at the earliest time possible.¹³

The immediate response authority is not provided for in any statute, but is said to have deep historical roots. The 1906 San Francisco earthquake and fire are noted examples. There, the commanding general of the Pacific Division, on his own initiative, deployed all troops at his disposal to assist civil authorities to stop looting, protect federal buildings, and to assist firefighters.⁴

c. Leave the Insurrection Act as is.

There is adequate language in the statute as is and only needs to be better understood and utilized when needed.

II. How can local authorities, first responders and local/state police best communicate with the military on the ground? That is to say, if the military is to play a supporting role as outlined in the Stafford Act, what kinds of communication structures are needed to assure that the resources are applied as needed?

III. This paper has looked to the National Guard to play a key role in disaster relief by remaining in chapter 32 status. In the context of the Total Force Structure of the US military, are National Guard units less able to undertake the kind of disaster relief activities required (such as law enforcement)? The fear is that through integration within the Total Force Structure, National Guard units will be less able to address state-specific needs; or (Continued, Page 25)

Posse Comitatus (Cont. from Page 16) e.g. rules of engagement, are not going to be appropriate in a disaster situation. Mixed training or training some units in non-war fighting scenarios can again take away from the overall preparedness of the military for its primary mission.

In the event of a direct terrorist attack on the United States, the military would most likely be called upon to play a role, particularly if chemical, biological, radiological or nuclear weapons were used. In regards to *posse comitatus*, this is a situation in which the government would likely waive the statute. Whether it would fall under the Insurrection Act specifically, or perhaps fall under the inherent power of the government to repel attack or invasion, it would constitute a situation in which the government would suspend *posse comitatus*.

In 2002 Congress reiterated its support of *posse comitatus*.²¹ It is an important part of the civilian controlled military central to the form of government and government-military relations of a functioning democracy. *Posse comitatus* does not impede the military from performing important functions in the assistance of state and local officials in the event of a major catastrophe. The only function prohibited is that of domestic law enforcement. Yet this function can be carried out by state National Guard units if state and local police are overwhelmed. It is therefore important for the governor to retain the National Guard in its chapter 32 status. It is also important for local and state police, as well as

first responders, to communicate well with invited military units so that the muscle and might of the military can be efficiently and helpfully applied. This is the best role for the military and one which requires no new legislation. It does require that all relevant leaders understand the roles they are to play, what they may and may not do, and with whom they need to be communicating.

Conclusion

The really big question remaining is whether all of this is believed to be adequate. *Posse comitatus* does not in any way hinder the military from applying the kind of specialized expertise and equipment it has to catastrophic events. All it does is prohibit military personnel from enforcing domestic law, a function which can be carried out by local and state police as well as the National Guard as long as it remains under state control. Should the situation further deteriorate into lawlessness, the Insurrection Act is available to empower a vibrant military role in re-establishing order, including through domestic law enforcement.

It would seem that rather than enacting new structures or eliminating something like *posse comitatus*, it would make more sense to more fully and efficiently make use of the structures already in place. Establishing clear lines of communication and confirming that leadership understands the roles and limitations of key players can ensure that resources are best applied in disaster situations. An important concept in the

American democratic system is that of the ultimate control of military power resting in civilian hands. With the Stafford Act, subject to *posse comitatus*, that structure is retained without sacrificing the capabilities held by the military that can be of great assistance in a catastrophe. It is appropriate for those skills, funded by US taxpayers, to be used in a time of great need by US taxpayers. ❖

¹ "Posse Comitatus Act" 18 USC §1385.

² 10 USC §375.

³ "Posse Comitatus Act" 18 USC §1385.

⁴ See 14 USC §89.

⁵ 10 USC §§331-334.

⁶ 10 USC §332.

⁷ e.g. 10USC §381.

⁸ e.g. 10USC §371.

⁹ 10USC §382 and 18USC §831, respectively.

¹⁰ See Trebilcock, Maj. Craig T., USAR, "The Myth of Posse Comitatus," *Journal of Homeland Security*, October, 2000.

¹¹ 42 USC §5121 et seq.

¹² 10 days - 42 USC §5170(c)(1).

¹³ 42 USC §5170(c)(6)(B).

¹⁴ *Gibbons v. Ogden*, 1824; *Compagnie Francaise de Navigation a Vapeur v. Louisiana State Board of Health*, 1902.

¹⁵ 42 CFR § 70.2.

¹⁶ Elsea, Jennifer and Kathleen Swendiman, CRS Report for Congress, *Federal and State Quarantine and Isolation Authority*, pp. 22-23, December 12, 2005.

¹⁷ Lipton, Eric, Eric Schmitt and Thom Shanker, "Storm and Crisis: Military response; Political Issues Snarled Plans For Troop Aid," *New York Times*, September 9, 2005, section A, page 1, column 5, *italics added*.

¹⁸ 10 USC 1003, §10103.

¹⁹ 10 USC 1211 §12406.

²⁰ Moller, Jan and Robert Travis Scott, Governor, White House detail response, *Times-Picayune*, September 8, 2005.

²¹ See 6 USC §466.

Call to Arms (Cont. from Page 5) the judicial branch of government. By contrast, looters in New Orleans were making no political statement and had no intention to overthrow the government. The chaos that ensued after Katrina was just that - chaos. This rationale explains why a senior Administrative official was quoted as saying President Bush would not have sent in troops to enforce law "unless the security situation made it completely clear that [the Louisiana governor] was unable to effectively execute her command authority."²⁵ Thus, the Bush administration could not act until the state government had been overthrown. While the disorder and lawlessness of an insurrection and a natural disaster may look similar, the Insurrection Act would not apply to a natural disaster scenario. This necessitates the need for a natural disaster exception to the PCA.

D. The Armed Forces would be the Best Actor

The lack of manpower in state and local police forces, combined with the vast disaster area in need of policing and the slow response of National Guard troops, creates a situation where first responders are set up to fail. Amending the PCA to allow military personnel to enforce domestic laws in the wake of a natural disaster would be a much more efficient method to react to crime and looting after a natural disaster. First, the U.S. military currently performs a wide range of duties in disaster relief, and

therefore is already deeply engrained in the disaster relief process. It was noted after Katrina that "the military ended up playing a central role in the federal government's relief work."²⁶ This was due to the sheer number of troops deployed to the disaster site.²⁷ At its peak, military forces reached nearly 72,000, with almost 50,000 National Guardsmen and 22,000 active duty personnel in the Gulf Coast.²⁸ Under the current system, military personnel are able to perform a wide range of functions in disaster relief efforts, such as coordinating evacuation efforts, providing aid and medical care, and assisting in search and rescue operations. Therefore, creating a natural disaster exception to the PCA would only result in a minimal expansion of the military's role in natural disaster response to include law enforcement efforts.

Second, military forces are already trained and organized. Unlike a National Guard unit, which must be called up and organized before it can be deployed, the U.S. military is organized into standing battalions. United States Senator John Warner, chairman of the Senate Armed Services Committee stated, "The only entity in the United States that has the personnel, the equipment, the training, and the logistical capacity to lend support to the National Guard and other state entities in an emergency of this scale, is the Department of Defense."²⁹ Opponents to a change in the PCA argue that the role of the

military is to fight wars against international powers. Moreover, opponents argue that the military is trained to defeat the enemy and shoot to kill, not to conduct basic law enforcement and policing functions. However, the nature and role of the military has been evolving over the past few decades. U.S. military troops already perform law enforcement and policing functions.³⁰ For instance, in Iraq, U.S. military forces currently perform a variety of law enforcement functions while they train Iraqis for these policing responsibilities.³¹

Third, the U.S. military is highly mobile and can be deployed expeditiously to restore order. The United States always keeps a force ready to be deployed anywhere in the world at a moment's notice at the direction of the President.³² As President George W. Bush stated, the U.S. military was "the institution of our government most capable of massive logistical operations on a moment's notice."³³ Regrettably, due to the PCA, the President is generally unable to utilize the expediency and skills of the U.S. military for domestic law enforcement.

Conclusion

Status quo law enforcement mechanisms in the wake of large-scale natural disasters are inadequate. State and local police and National Guard troops cannot effectively quell lawlessness following a major disaster. Maintaining law and order in the wake of a (Continued, Page 25)

Ed Gibson (*Cont. from Page 6*) building intelligence alliances between police agencies, security services and private sector companies. It was done in fun. He had decided to play to the FBI stereotype, before opening out his audience to his real message.

Even so, I muse, turning to the FBI for talent still seems a strange step for Microsoft to take. "Yes, it does," he agrees. "Five years ago, Microsoft wouldn't have thought of hiring someone like me. But as the threats online have changed, the company has realised the value of people with diverse expertise that goes beyond understanding how to develop software. We now have 23 chief security advisors, including persons with experience in the intelligence world."

But isn't this running the risk of overkill? "Not at all," he shoots back. "Computer crime is moving into a different realm, with virtual gangs, often organised on a cellular basis. The members don't know each other. But increasingly they have the power - and some have the ambition - to take down a company."

When I ask whether much of this isn't still done by teenage social misfits in their back bedrooms, with no understanding of the consequences, he disagrees. "No, most of these people know what

they are doing. Even in countries like Bulgaria and Romania, where they have a less developed technology infrastructure, they get it. They know what they're doing, and if we don't get on top of the problem they are going to take the Net to the point where people may fear to venture into it."

OK, so where is Microsoft headed in this area? "Because of our market share, we have a huge responsibility to address this issue, and we are," he says. "We've made a lot of fundamental changes to improve our development process so our products are more secure and resilient to attack. But the scale and sophistication of cybercrime are growing all the time, so we also have a world-class response process to help our customers manage their networks and home computers, both over time and in the event a worm or virus hits. Beyond our technology efforts, we are making investment in helping law enforcement agencies around the world identify and prosecute these criminals. That's where people like me come in."

Gibson notes that Scott Charney, the company's Vice President of Trustworthy Computing, is driving the company's changes in these areas. And Charney himself had served as chief of the Computer Crime and Intellectual Property Section of the US Department of Justice. As the leading federal prosecutor for cybercrime, he

helped prosecute nearly every major hacker case in the US from 1991 to 1999.

Microsoft, Gibson insists, "has the size and weight to make a difference" in these areas. When I ask what he thinks about the controversial area of encryption, he replies that Microsoft is all for it. Indeed, it has just acquired FrontBridge Technologies, Inc, which specialises in areas like e-mail and instant message archiving for compliance, content and policy enforcement, spam and virus protection, disaster recovery, e-mail encryption, and e-mail continuity.

But, in the end, Gibson stresses, the ultimate challenge in computer security lies with individuals, with each of us. Computer users, he says, have responsibility too, to make sure they understand the risks and to keep their computer updated with the latest protections. "In the internet age, we can no longer just plug in the computer and forget about it. There are people looking to take advantage of unprotected computers to cause a lot of damage. But if consumers take a few simple safety steps - like turning on a firewall, using anti-virus software and making sure their computer has the latest security updates - they can help make the Internet safer for everyone." ❖

SustainAbility and Radar online:
www.sustainability.com/radar

Identity Theft (Cont. from Page 8)

Finally, an entity may discover a compromise in its security – the computer system detects unauthorized access, or a shipping vendor reports data tapes were lost in transit, or an audit reveals insider wrongdoing. Depending on the quality of the entity's information systems, the entity may or may not be able to provide details regarding how the information was accessed, what pieces of information were compromised, or whether the information was compromised in a usable format.

These scenarios show that although evidence of a security breach, theft, or fraud may be separately discovered, none of this evidence may ever be linked. An entity suffering a breach cannot measure the actual loss to the victims. Without the connections necessary to show causation, it is impossible to determine the relative responsibility of each piece of stolen identity information to the accomplished (or attempted) crime and resulting harms. Thus, the reported "statistics" of identity theft and security breaches suffer various flaws:

- Reliance on self-reporting by victims and credit reporting agencies. According to almost all evidence, most identity thefts are not reported. For example, at all the Congressional hearings on identity theft, at least one witness mentioned the FTC survey result that almost 10 million people in the U.S. became victims of identity

theft in 2004; however, the number of identity thefts reported to the FTC Clearinghouse in 2004 was fewer than 250,000 (less than 2.5% of the survey results). Further, the reports which are compiled may lack a causal connection to disclosed security breaches because many victims do not know how their information was stolen.

- Reliance on law enforcement / conviction rates. Since identity thieves are often apprehended after committing more grievous crimes and may not be charged with the lesser identity theft, identity theft convictions may not reliably indicate the frequency of identity thefts or any connections to security breaches.
- Focus on ultimate crimes rather than methods of identity theft. Most statistics focus on how the stolen information was used to commit crimes, not how the information was originally stolen.

Therefore, while (1) the aggregate number of individual accounts potentially compromised by security breaches, and (2) the number of identity thefts determined by survey, are both daunting, we still lack reliable statistics correlating security breaches to identity theft. Remedying the absence of correlative data may be merely a matter of reorganization (defining who should be collecting this information, and how it should be

managed), but it may also be that this kind of data (a) is not susceptible to identification and collection, or (b) is too costly to identify and collect. However, this absence of data is not fatal to providing "solutions" to the identity theft and security breach problems because, although a court would not allow recovery without a causal connection, policy-makers operate under different imperatives.

Given the current knowledge of identity theft and security breaches, some might argue that governments and the private sector would not be offering their panoply of solutions if the "identity theft crisis" did not relate directly to the increasing commercial market in personal information. Thus, both private sector and public sector decision-makers must look to the harms threatened by identity theft and security breaches, as well as the incentives provided by market and regulatory solutions.

Harms

Both identity theft and information systems security breaches can result in a wide spectrum of harms. The "victims" of identity information theft may include (a) the entity suffering the breach; (b) the individual whose information was stolen; (c) the retailer bearing the cost of the fraudulent purchase; (d) individuals victimized by crimes accomplished with the stolen identity; and, from a broader point of view, (e) taxpayers, consumers, and the general society, who (Continued, Page 21)

Identity Theft (*Cont. from Page 20*) ultimately shoulder the costs of fraud, as well as the harms from terrorist acts perpetrated under stolen identities. A brief review of the various kinds of harms includes:

Harms to Entities Suffering a Security Breach

- Financial costs of (1) investigating the security breach, (2) communicating disclosures of the breach, (3) offering fraud prevention measures to affected consumers (credit monitoring, identity theft insurance, etc.), (4) paying contractual liabilities to vendors or partners, (5) losing competitiveness in the market, and (6) withstanding a drop in stock prices.
- Regulatory actions. Businesses may (a) face monetary sanctions, and (b) be forced to implement additional security measures mandated by regulators under various authorities, including the FTC Act, the safeguards and privacy provisions of the Gramm-Leach-Bliley Act and section 404 of the Sarbanes-Oxley Act.
- Liability to victims who suffer actual losses. Courts have traditionally limited recovery only to plaintiffs who (a) have either a contract or other special relationship that establishes a duty to reasonably secure the information, and (b) can prove actual losses caused by the breach.

Harms to the Individual whose Identity was Stolen

- Harms from compromised social security numbers. These costs may not be easily quantified because a social security number is a key identifier that allows a wrongdoer to access more information about the victim (e.g., pretexting to get a consumer report) and to create more identification documents and accounts under the victim's name. Getting a new social security number is not really a viable option because (a) the old and new numbers will be linked together in many systems, (b) many agencies and organizations maintain records under the old number, and (c) the lack of credit history under the new number may cause future insurance and credit problems for the consumer. If a social security number was disseminated, these harms could be perpetrated repeatedly, even if the initial identity thief was caught. Since a fraud or impersonation could be committed at any time by any person, the victim suffers the financial and emotional costs of monitoring and remedying financial and criminal records that wrongdoers could be establishing.
- Financial costs from compromised (1) brokerage accounts (which may not have the fraud protections of credit accounts); (2) credit card accounts; and (3) checking or

savings accounts. Since credit card issuers generally will relieve consumers of fraudulent charges, consumer victims will likely suffer only the additional costs related to the time needed to challenge fraudulent charges, as well as the inconvenience of a new credit card number. Financial services providers often require additional information (e.g., PIN numbers) to access checking and savings accounts, so the chance of loss is less, and again, the victim will likely suffer only the additional costs related to changing account numbers.

Harms to Consumers / Society

- Passed-through costs of fraud and identity theft. Under credit card agreements, retailers must refund to victims the costs of fraudulently-purchased items. Businesses calculate the costs of fraud as a price of doing business; these costs thus affect prices for goods and services. Compromised credit card numbers may cause the card issuer to incur costs for cancelling the stolen numbers and reissuing new cards – costs for which the entity suffering the breach may be contractually liable, and which will ultimately be passed-through to consumers. Similarly, compromised student identification numbers may cause the school to incur costs to institute new numbers and audit and improve security (*Continued, Page 22*)

Identity Theft (Cont. from Page 21)

– costs which will be passed-through to students and taxpayers. Further, healthcare fraud directly impacts the costs of healthcare to consumers in general.

Solutions

As already discussed, various forces offer incentives to businesses to provide information security (market forces, contractual and tort liability, regulatory sanctions, etc.). As governments offer additional legislative solutions to the problems of identity theft and information security breaches, these solutions should (1) recognize the panoply of threatened harms to all victims, (2) take into account the various ways that information security may be breached, and (3) be targeted toward providing incentives to mitigate the identified harm.

In addition to the spectrum of harms from information security breaches, there is also a wide range of methods by which information may be compromised (hacking, storage tapes lost in transit, dishonest insider with permission to access the information, pretexting, other frauds, etc.). Remedial measures to prevent one kind of threat will not necessarily work against other threats. Also, information managed in digital form faces dynamic predators – the wrongdoers are constantly learning how to circumvent new technologies. Therefore, currently-existing security mandates emphasize the rea-

sonableness of the security plan rather than specific technological requirements.

Following in California's footsteps, more and more states are requiring businesses to disclose security breaches. Some businesses favor a preemptive federal security breach disclosure law that provides a common regulatory approach so that businesses do not have to comply with numerous different state laws. Some consumer advocates argue that states have the right to mandate stricter security for their citizens' information.

Wherever you stand on this issue, the proper policy analysis should begin with identifying the threat: (1) identity theft or (2) the problem of lax security in critical or interdependent information systems or (3) something else. The analysis should proceed by determining: (a) whether disclosure lessens the threat; and (b) whether the proposed law encourages efficient disclosure (the varied costs of disclosure, including potential consumer apathy, do not outweigh the degree to which the threat was lessened).

Yet again, the importance of definitions arises. Disclosure laws may not be an optimal solution if the threat is defined as either credit card fraud or the proliferation of social security numbers as the sole unique commercial and governmental identifier. Lawmakers should prioritize the identified threats and address each threat individually, under-

standing (1) that solutions may not apply to all harms arising from identity theft and information security breaches, and (2) that the costs of compliance are ultimately borne by consumers (who should therefore be receiving a security benefit worth more than this cost).

Conclusion

Today there is no comprehensive mechanism to directly correlate information security breaches to resulting damages from identity theft crimes. The lack of reliable correlative data renders traditional risk management analyses impossible. If legislators attempt to frame solutions to a generic "identity theft" threat based upon equally generic, non-correlative "statistics," the proposed new law may be more a guessing game than a viable and cost-effective solution. As governments address these issues, they should not only tailor the solution to the specifically-identified threat, they should also investigate our ability to gather the data needed to perform better risk analyses. Similarly, as businesses begin to comply with rule-making promulgated under existing laws like Gramm-Leach-Bliley and state disclosure laws, the private sector should incorporate standards and data-gathering techniques necessary to assess risk – to both demonstrate the required "reasonable" security and to defend against the charge that information security breaches have caused our "identity theft crisis." ❖
(Endnotes on Page 25)

Jose Padilla (Cont. from Page 11)
Padilla's procedural history is very extensive and demonstrative of the importance of the issue. Please see the Padilla timeline for a comprehensive review of the procedural history of this case (see pages 10-11).

In June 2002, Donna Newman, Padilla's appointed attorney, filed a writ of habeas corpus on his behalf. She filed the petition in New York against President Bush, Defense Secretary Donald Rumsfeld, Attorney General John Ashcroft and Commander M.A. Marr, the warden of the military brig at Charleston. The government responded arguing, among other things, that the court in New York no longer had jurisdiction because Padilla had been moved to South Carolina. The jurisdictional challenge was finally resolved in 2004, after numerous appeals, when the United States Supreme Court ruled that the case was improperly filed in New York and should be refiled in South Carolina.

Newman filed another writ for habeas corpus in South Carolina District Court. This time she named Commander C.T. Hanft, a Naval Officer and Padilla's custodian at the brig, as respondent. The district court ordered Commander Hanft to release Padilla from his custody within 45 days. The government appealed to the Fourth Circuit Court of Appeals who reversed the district court's ruling. The Court of Appeals stated that, "The Congress of the United States, in the Authorization for

Use of Military Force Joint Resolution, provided the President all powers necessary and appropriate to protect American citizens from terrorist acts by those who attacked the United States on September 11, 2001." *Padilla v. Hanft*, 423 F.3d 386 (2005). They went on to hold that "Those powers include the power to detain identified and committed enemies such as Padilla, who associated with al Qaeda and the Taliban regime...entered the United States for the avowed purpose of further prosecuting that way by attacking American citizens and targets on our own soil..." *Id.* Therefore, the Court of Appeals refused to transfer Padilla.

On November 23, 2005 Padilla was indicted by a Miami federal grand jury on criminal charges that he conspired to "murder, kidnap and maim" people overseas. The three charges included: conspiracy to murder U.S. nationals, conspiracy to provide material support to terrorists, and providing material support to terrorists. The charges did not include the earlier allegations that he planned to build and detonate a dirty bomb in the United States. Attorney General Alberto Gonzales stated, "Padilla's previous status as an 'enemy combatant' has no legal ramifications for the criminal charges."

On January 4, 2006, the Supreme Court ordered, at the request of the government, Padilla transferred from military custody to stand trial in Miami, Florida. Padilla's attorney argued

that the Court should wait to transfer Padilla until they had ruled on the issue concerning the President's authority to detain enemy combatants. On January 13, 2006, the Supreme Court met to determine if the case is moot or to define the extent of presidential power over U.S. citizens who are detained within the United States on suspicion of terrorist activity. They have not yet released their decision.

Padilla was arraigned on January 12, 2006. He pleaded not guilty to all charges against him. The judge denied his bail because of the seriousness of the charges. Padilla's trial is set to begin in the fall of 2006. Four other men were charged with Padilla: Adham Amin Hassoun, Kifah Wael Jayyousi, Mohamed Hesham Youssef, and Kassem Daher.

Padilla's case is not unique. There have been two other enemy combatants, Yaser Hamdi and Ali Saleh Kahla-al-Marri. Hamdi, a U.S. citizen born in Louisiana, spent most of his life overseas. He was captured in December 2001 in Afghanistan. The government contended that he was armed and was traveling with a military unit of the Taliban. He was held at Guantanamo Bay. However, he was later transferred to a military brig in Norfolk, Virginia and then subsequently to South Carolina. Hamdi raised the same issues as Padilla. The Supreme Court of the United States affirmed the right of the President to detain citizens as "enemy combatants" during a military conflict, but held that such detainees (*Continued, Page 25*)

Call to Arms (Cont. from Page 18) disaster is vital to evacuation and rescue efforts. Currently, the federal armed forces and federalized state militia may not enforce domestic laws, unless there is an uprising against the government. Simple chaos and lawlessness do not trigger Insurrection Act powers. Therefore, Congress should enact an exception to the Posse Comitatus Act to allow for federal military assistance in civil law enforcement in the wake of a large-scale natural disaster. ❖

¹ See generally Sandra K. Schneider, *Government Response to Disaster, the Conflict Between Bureaucratic Procedures and Emergent Norms*, PUB. ADMIN. REV. March/April 1995, at 135.

² Id.

³ See CNN Security Watch *Special: Is America Prepared?* (CNN television broadcast Sept. 25, 2005) Transcript 092501CN.V79 [hereinafter *CNN Security Watch*].

⁴ See David Hill, *Crime Hindered Evacuation*, THE HILL, Sept. 14, 2005, at 14.

⁵ Id.

⁶ Id.

⁷ *Entergy Implements Business Continuity Plan by Establishing Interim Corporate Headquarters in Jackson Metro Area; Company Intends Return to New Orleans*, PR NEWSWIRE, Sept. 4, 2005

[hereinafter *Entergy Implements Business Continuity*].

⁸ CNN Security Watch, *supra* note 3.

⁹ Id.

¹⁰ See Schneider, *supra* note 1, at 136.

¹¹ *Entergy Implements Business Continuity*, *supra* note 7.

¹² *Evacuation of Hurricane-Struck U.S. City of New Orleans Nears Completion; Death Toll; Cost Estimates Grow; U.S. President Bush Faces Sharp Criticism*, FACTS ON FILE WORLD NEWS DIGEST, Sept. 8, 2005, at 597A1 [hereinafter *Evacuation of Hurricane*].

¹³ Id.

¹⁴ White House, *Fact Sheet: America Responds to the Katrina Disaster*, Sept. 3, 2005, available at <http://www.whitehouse.gov/news/releases/2005/09/20050903-3.html>.

¹⁵ *A Police Force in Chaos*, WASH. TIMES, Sept. 10, 2005, at A12.

¹⁶ *Evacuation of Hurricane*, *supra* note 12.

¹⁷ Id.

¹⁸ Mike Dunn, *Strain Forges Stronger NOPD; Officers Carry on Despite Conditions*, ADVOCATE (Baton Rouge), Sept. 5, 2005 at 1B-2B.

¹⁹ Rone Tempest, *State's National Guard May Be Getting Spread Thin; L.A.'s Blackout Focuses Attention on Whether There Are Enough Troops to Handle an Emergency*, LOS ANGELES TIMES, Sept. 26, 2005, at 2.

²⁰ *Evacuation of Hurricane*, *supra* note 12; see also Julian Borger & Jamie Doward, *Bush Sends Marines as Flood Fury Grows*, THE OBSERVER (Baton Rouge), Sept. 4, 2005, at 1.

²¹ 10 U.S.C. § 331 (2000).

²² BLACK'S LAW DICTIONARY (8th ed. 2004).

²³ 77 C.J.S. Riot; *Insurrection* § 29, at 579 (1994).

²⁴ Mark Mazzetti, *Military Sees Limits to Role in U.S. Disasters; A Defense Official Says 'Catastrophic' Events, Including a Pandemic, Would Be the Threshold*, LOS ANGELES TIMES, Oct. 13, 2005, at A11.

²⁵ Lipton et al., *Storm and Crisis: Military Response, Political Issues Snarled Plans for Troop Aid*, NEW YORK TIMES, Sept. 9, 2005, at A1.

²⁶ Keith J. Costa, *Rumsfeld Confirms DoD Has No Plans to Alter Posse Comitatus*, INSIDE THE PENTAGON, Vol. 21 No. 41, Oct. 13, 2005.

²⁷ See Id.

²⁸ Department of Defense Hurricane Relief Funds: Hearing Before Def. Subcomm. of the H. Appropriations Comm., (Sept. 28, 2005) (statement of the Honorable Paul McHale).

²⁹ Vince Crawley, *Laws on Military's Homeland Role May Get Review*, FEDERAL TIMES, Sept. 26, 2005, at 6.

³⁰ See *Political Headlines* (Fox television broadcast June 8, 2004) Transcript # 060801cb.254.

³¹ Pail Richter, *The Conflict in Iraq; Rapid Personnel Shifts Hinder U.S. Efforts to Rebuild Iraq*, LOS ANGELES TIMES, Nov. 17, 2005, at A1.

³² Julian E. Barnes & Kenneth T. Walsh, *A Uniform Response?*, U.S. NEWS & WORLD REPORT, Oct. 3, 2005, at 28.

³³ *Rumsfeld Demurs When Asked About Changing Posse Comitatus*, NAT'L JOURNAL'S CONGRESSDAILY (AM edition), Sept. 21, 2005.

Jose Padilla (*Cont. from Page 23*) could contest the merits of their captivity before a neutral fact-finder.¹ Hamdi was released in the fall of 2004. The terms of his release mandated that he had to renounce his United States citizenship. Additionally, he is not permitted to travel to Afghanistan, Iraq, Israel, Pakistan, Syria, the West Bank or Gaza. And finally, for the next fifteen years, he has to report any intention to travel outside Saudi Arabia.

The second enemy combatant, al-Marri, was arrested in December 2001. Contrary to the other enemy combatants, he is not a U.S. citizen (he is from Qatar and arrived in the U.S. the day before the terrorist attacks on September 11, 2001) and he was indicted at that time for credit card fraud and lying to the FBI. He was declared an enemy combatant on June 23, 2003. al-Marri is currently still being detained at the South Carolina military brig. He was prohibited for sixteen months to meet with his attorney, but has since met with an attorney and has two cases pending. One case is challenging his treatment and the second concerns the legality of his detention.

There has been much public outcry over the Padilla case and the issues concerning enemy combatants. There have been several harsh critics concerning the government's actions towards enemy combatants. Several organizations have filed briefs on behalf of Padilla. For example, the American Bar Association filed a brief as *Amici Curiae* in support of Padilla. They argued, "Padilla must have the opportunity to challenge the basis for detention; he must have access to counsel to assist him in making that challenge; and the government must substantiate the basis for its detention under a meaningful standard of review." The American Bar Association further asserted, "Anything less would be inconsistent with this nation's core principles." However, there have been some arguments defending the government's actions. Paul Rosenzweig from the Heritage Foundation stated, "The information regarding [Padilla and Hamdi's] intention was based on intelligence and military sources and not suitable to be aired in a conventional criminal-court setting." He went on to assert, "History has taught us that during wartime, executive flexibility is not merely desirable, but essential." ❖

¹ *Hamdi vs. Rumsfeld*, 542 U.S. 507 (2004)

Issues for Further Study (*Cont. from Page 16*) those with specific needs may be located in another state, requiring the governor to reach an agreement with that state's governor to obtain the resources. Should state National Guard units prepare more thoroughly for potential state-specific scenarios? Will that undermine the larger US military capability and the Total Force Structure? ❖

¹ 10 USC §332.

² 10 USC §332.

³ U.S. Dep't of Defense, *Military Support to Civil Authorities*, DoD Dir. 3025.1 § 4.4.10 [1993].

⁴ Elsea, Jennifer, CRS Report for Congress, *The Use of Federal Troops for Disaster Assistance: Legal Issues*, PP. 5-6, September 16, 2005.

Identity Theft (*Cont. from Page 22*)

¹ There may be many "victims" of the wrongdoer's actions (see *infra*), but for the purposes of this article, the phrase "victim" refers to the person whose identity was stolen.

² CNNMoney.com, citing USA Today.

³ *Id.*

⁴ Knowledge of the extent of exposure to identity theft through security breaches (i.e., how much personal information is in the marketplace and who owns and controls the information) is factor valuable to assessing risk. A discussion of consumer awareness and access to such knowledge is beyond this article, but is included in the CIP Program's ongoing Identity Theft research project.

The CIP Program is directed by John A. McCarthy, a member of the faculty at George Mason University School of Law. The CIP Program works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems and economic processes supporting the nation's critical infrastructure. The CIP Program is funded by a grant from The National Institute of Standards and Technology (NIST).

The CIP Report is published by Zeichner Risk Analytics, LLC on behalf of the CIP Program. ZRA is the leading provider of risk and security governance knowledge for senior business and government professionals. ZRA's vision is to be a consistent and reliable source of strategic and operational intelligence to support core business processes, functions, and assurance goals.

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://techcenter.gmu.edu/programs/cipp/cip_report.html