

Removing the Barriers to Intelligence Information Sharing

by

Manager, Shelly Greene

Fremont Police Department

September, 2009

COMMAND COLLEGE CLASS 45

The Command College Futures Study Project is a FUTURES study of a particular emerging issue of relevance to law enforcement. Its purpose is NOT to predict the future; rather, to project a variety of possible scenarios useful for strategic planning in anticipation of the emerging landscape facing policing organizations.

This journal article was created using the futures forecasting process of Command College and its outcomes. Defining the future differs from analyzing the past, because it has not yet happened. In this article, methodologies have been used to discern useful alternatives to enhance the success of planners and leaders in their response to a range of possible future environments.

Managing the future means influencing it—creating, constraining and adapting to emerging trends and events in a way that optimizes the opportunities and minimizes the threats of relevance to the profession.

The views and conclusions expressed in the Command College Futures Project and journal article are those of the author, and are not necessarily those of the CA Commission on Peace Officer Standards and Training (POST).

© Copyright 2008

California Commission on Peace Officer Standards and Training

Removing the Barriers to Intelligence Information Sharing

Introduction

Nearly eight years have passed since the tragic events of September 11, 2001 when jet airliners were piloted into the World Trade Center, the Pentagon and a field in rural Pennsylvania. In the aftermath of this attack, we learned there were ample clues that pointed to the intended actions of those responsible; tragically, there was not a protocol, system, or organizational philosophy in place to share and analyze such data in time to prevent the crimes. In spite of this fact, almost a decade later, there is still no effective means to share intelligence information that could protect America against another act of terrorism.

While the 9/11 Commission Report places responsibility for the tragedy squarely at the feet of the Federal intelligence community (IC), the report also establishes that it was not necessarily a failure to collect the appropriate intelligence, but rather the barriers to intelligence sharing between agencies that led to the largest terrorist attack in American History (911 Commission Report, 2004). In the following analysis, we will learn strategies to remove those barriers amongst federal, state and local agencies to ensure the right intelligence information gets to the right people in time to thwart future acts of violence.

Information Intelligence sharing

The challenges related to the sharing of classified intelligence information are multifaceted and complex, yet we know all too well that the repercussions of failed intelligence can be calamitous. Intelligence information sharing is not the broadcast of what color the current threat level is, nor is it the collection and distribution of information on unsuspecting citizens. Intelligence information sharing is the dissemination of intelligence products designed to “inform law enforcement decision making at both the tactical and strategic levels” for the

purposes of crime prevention and, ultimately, national security (IACP, 2003, p.4). A critical and straightforward enough task it would seem; however, the intelligence strategies employed today in the fight against terrorism reign from the Cold War era and are counterproductive in addressing current and future threats to our national security.

According to Gregory Trevorton, a Senior Policy Analyst at the Rand Corporation, the legacy of U.S. intelligence from the Cold War is an organization of collection sources or “stovepipes,” which may have been appropriate when the individual intelligence agencies had a common focus, (i.e. the Soviet Union) but is lacking when faced with today’s multiple threats, inundation of information from a variety of sources and of varying quality, and accountability to an ever-growing assortment of consumers (Trevorton, 2005, p7). Trevorton suggests the stove-piping of information as preferred during the Cold War “is not the right way to organize U.S. intelligence” today or in the foreseeable future (Trevorton, 2005, p7).

The Problem

An ever-present component of the Cold War intelligence legacy, and a major impediment to information sharing, is the classifications systems. Classification is simply the “process of identifying information that requires protection in the interests of national security” (Maus, 1996, p1). Under the current system, this requires the receiver of classified information to not only have a security clearance, but a security clearance from the issuing agency.

Classification is not a new concept, and can be dated as far back as 300 BC when General Sun Tzu wrote “The Art of War”(Maus, 1996, p.1). Historically, each of the present-day intelligence agencies has developed their own classifications policies specific to their mission requirements, and with little regard to their counterparts. For example, information that would be

classified under FBI rules may not meet the threshold for classification at the Department of Homeland Security because their mandates are different.

At present, thirty-eight federal agencies can grant security clearances (PNSR, 2008, p.302). The flaw in this system becomes readily apparent when, for example, “a contractor working on black [covert] operations programs for both the National Security Agency and the National Reconnaissance Office would need two different Sensitive Compartmented Information Facility (SCIF) permissions—even though he would be operating at the same level of clearance for both agencies” (PNSR, 2008 p. 302). Clearly, to meet current and emerging threats, this complex web of divergent clearances must change.

During the cold war, the need for “coordinated and trusted interagency partnerships was not universally recognized and thus gaps and seams existed in the sharing of information across all levels of government” (Treverton, 2008, p.7). Exacerbating the issue today is the some 700,000 local law enforcement officers who have a legitimate and critical need for classified information related to Homeland Security, but who would be required to go through multiple vetting processes to get information relevant to their jurisdictions. For example, Chief Joseph Polisar of the Garden Grove CA Police Department waited nine months for his Top Secret Security Clearance through the Department of Homeland Security, only to find out it was not recognized by the FBI. He said;

“Until my DHS Top Secret clearance was recognized by the FBI, any top secret information that the FBI had supplied to one of my officers assigned to our local Joint Terrorism Task Force could be held from me. Because I held a DHS Top Secret Clearance and the officer held an FBI Top Secret Clearance, I was forced to submit my information to the FBI through the DHS and had to wait eight months before the Bureau recognized my DHS Top Secret clearance.” (U.S. House Committee, 2005, p18)

Chief Polisar's experience is not unique. Though his clearance attempts were prior to 2005, counterterrorism intelligence and information sharing by the federal intelligence community continue to be constrained by the same archaic infrastructures, technologically and culturally speaking, as during the Cold War.

The pitfalls of classification

The need for classification and security clearances are genuine, but over-classification is counter productive to protect national security secrets, and could have tragic consequences. Regrettably, under the current system, a tremendous amount of information that is classified simply does not need to be, and often prevents or delays actionable intelligence information from reaching the appropriate personnel and agencies. In 2007 national security expert Suzanne E. Spaulding testified to the U.S. House of Representatives that "just as getting the classification process right is vital for protecting true secrets, it is essential that information that can be shared without jeopardizing national security is not prevented by over-classification from getting to those who could make use of it" (Spaulding, 2007, p2).

According to John H. Locher III of the Project on Nation Security Reform, the classification system as it exists today promotes classification over sharing for two basic reasons: "Few penalties exist for classifying documents that need not be protected," [and] "to decide not to classify a document entails a time-consuming review to evaluate if that document contains sensitive information" (PNSR, 2008 p. 304). One of the arguments for classification reform is to ensure "those handling classified documents will have greater respect for that 'Top Secret' stamp if they know that things are only classified when their disclosure would truly harm national security" (Spaulding, 2007, p1). In fact, the problem is so prevalent that Congress recently passed the *Reducing Over-classification Act of 2009* specifically to address this issue. "When

things are classified whose disclosure clearly would not harm national security, it tempts some individuals to believe that they can decide what is really sensitive and what is not” (Spaulding, 2007, p1).

Over-classification also comes with a significant price tag. Apart from costs to both openness and security, classifying and declassifying comes at a heavy financial burden. In 2005, the cost to secure classified information was \$7.7 billion; \$57 million of which was spent on declassification. This means that for every dollar the federal government spends to release old secrets, it also spends \$134 to create new ones (Aghast, 2007, p.5).

The local perspective

Law enforcement agencies (LEA) are generally very good at developing information sources, and have well established networks for sharing information. Their intelligence capabilities, however, vary widely from agency to agency. Most are ill-equipped to participate in international intelligence work for the purpose of counterterrorism, particularly if their intelligence personnel do not have security clearances. Agencies with personnel assigned to a FBI Joint Terrorism Task Force (JTTF) have a bit of a leg-up on their counterparts, but only if personnel in the local department have the appropriate clearances.

Large police agencies like the New York City Police Department (NYPD) have sidestepped this issue by deploying their own personnel to various locations around the globe to gather intelligence that can be shared within the organization. This has created some conflicts between the NYPD and the Federal Intelligence Community, but has served them well by getting intelligence information into the hands of the appropriate people within their agency. Unfortunately, most local jurisdictions do not have the capacity to conduct intelligence activities on that scale, leaving them to rely on their own local intelligence gathering. In reality, without

sufficient security clearances, classified information relevant to their jurisdiction remains in the stovepipe and out of reach.

Why include the locals

Previous to 9/11, responsibility for international intelligence gathering in support of Homeland Security fell primarily with the Federal intelligence community. Executive Order 12333 specifically requires the FBI to conduct counterintelligence, coordinate counterintelligence activities, and “conduct counterintelligence activities outside the United States in coordination with the Central Intelligence Agency.” (Cummings, 2004, appendix 2) In the years since, though, the need for interagency cooperation and multi-jurisdictional information sharing has been at the heart of most discussions surrounding Homeland Security and counterterrorism intelligence. (911 Commission Report, 2004) The Federal Intelligence Community has also come to realize that local LEA are uniquely suited to assist in both arenas. With experience as a Federal Prosecutor and judge, former U.S. Secretary of Homeland Security Michael Chertoff has argued that LEA know their communities most intimately; therefore, are best placed to function as the “eyes and ears’ of an extended national security community” (Rollins, 2008, p.7).

LEA have the demonstrated ability to develop information sources where federal agencies cannot, and have well established networks for sharing information and coordinating activities with other agencies (Treverton, 2005, p.1). Case in point: since the mid 1970’s many states have had regional narcotics task forces comprised of local officers and governed by a council made up of local Police Chiefs and other law enforcement executives such as the County Sheriff, District Attorney, and Chief of Probation. These task forces work across jurisdictional boundaries developing street level informants in support of their investigations. This is not

something that can be easily done on the federal level. For example, a FBI agent conducting surveillance out of the San Francisco region would be required to terminate the surveillance if the subject crossed over into the Sacramento region. The agent would have to have written permission from the Sacramento Special Agent in Charge (SAC) prior to conducting any investigative work in the Sacramento area, to include active surveillance.

According to the Joint Task Force on Intelligence and Law Enforcement, LEA are believed to be well-positioned to develop information on crimes, activities, and organizations that support terrorist operations, and recent history supports this theory. The arrest of Timothy McVeigh, convicted bomber of the Alfred P. Murrah Building in Oklahoma City in 1995, was the result of a traffic stop by a state trooper. And, as recent as 2005, two Torrance CA police officers searching the apartment of a robbery suspect uncovered Jihadist material that exposed a terrorist plot just days away from being carried out in the City of Los Angeles. These are only two examples of many where local law enforcement officers have contributed to Homeland Security, and affirm the role of local law enforcement in Homeland Security as a critical one.

Removing the barriers

Some LEA have been successful developing their own “workarounds” to obtain the information they need. Developing one-on-one relationships with individual Intelligence Community personnel seems to be the approach that is most effective to get through the federal door. One San Francisco Bay Area agency has essentially created its own version of a JTTF; hosting a FBI Agent, an Intelligence Investigator from a neighboring agency and developing co-case relationships with larger agencies such as NYPD, DEA, IRS, Albuquerque PD and the Denver JTTF. Most cities would not have the demographic requiring the same level of outreach; however, it presents a convincing argument for reform of the current systems.

To address the barriers to information sharing created by over-classification and multiple security clearance requirements, reform and standardization of the current systems is the first steps to meet that challenge. Such action, however, will require a fundamental shift, both organizationally and culturally, from “a bureaucratic command-and-control model to an integrated, collaborative, network enterprise.” (McConnell, 2008, p.20) This would, in theory, lead to an open and reciprocal exchange of information, and facilitate a coordinated approach to counterterrorism by federal, state, and local intelligence agencies.

To start, “the key will be addressing the root causes of these challenges rather than making cosmetic changes to improve information sharing.” (Meyerrose, 2008) The Director of National Intelligence has set four strategic goals to initiate this process, one of which has the stated objective to “create a common classification guide for the intelligence community” (Meyerrose, 2008, 10) This could substantially increase the flow of information between agencies, reduce redundancy, promote collaboration, and create a more effective system of checks and balance.

Once a standardized classification protocol is in place, the volumes of disparate intelligence data must be organized so that it is not just retrievable, but discoverable in the first place. Dale Meyerrose, Associate Director and Chief Information Officer for the Director of National Intelligence says “Intelligence Analysts often don’t know what they don’t know” because they only have access to specific data or silos of information (Meyerrose, 2008, p.10). “We need to move to a collaborative information environment ... [where] regardless of classification or compartment, intelligence analysts and collectors can be aware of the existence of all intelligence information.” (Meyerrose, 2008, p.13) This can be specifically addressed through standardized classification of metadata, applications to facilitate information

transparency, retrieval protocols, and integration of “information networks at each security level.” (Meyerrose, 2008, p.13)

How do we do it?

These two initiatives alone could move intelligence information sharing light years ahead, but one should not be fooled that technology or new policies will change the current situation. According to a study by the firm of Booz, Allen and Hamilton on *Human Capital in the Intelligence Community* “the rate of progress of the federal government’s intelligence community (IC) toward building a culture of collaboration rests largely on its people and their skills” (Booz, 2008, p.1). In the years since the terrorist attacks of 9/11 there have been the appointments of the Director of Homeland Security, an Intelligence Czar, and a Director of National Intelligence. America has watched countless congressional hearings, read commission reports, and witnessed the creation of a multitude of departments, task forces, and Fusion Centers just to mention a few, and yet the status quo somehow prevails when it comes to the sharing of intelligence information. Why?

During his confirmation hearing, Admiral Dennis Blair, the most recently appointed Director of National Intelligence, emphasized that there is a “need for a shift in intelligence community culture” (OMB, 2009, p.1). Blair also concluded that “there are many penalties for those who disclose classified information and few rewards for those who take the additional effort to write at lower levels of classification” (OMB, 2009, p.1).

Woodrow Wilson once said “if you want to make enemies, try to change something,” but transitioning from a culture of caution and evasiveness, to one of transparency is possible in the federal intelligence community. One way is through “performance management that align, and integrate institutional, unit, and individual performance with organizational goals” (Booz, 2008,

p.1). This creates incentives, as well as an environment of accountability for sharing information. Implemented community-wide, a common approach to policy and operations development, while “preserving the unique characteristics of each agency,” is achievable (Booz, 2008, p.2).

What’s it going to take

If the collapse of the Twin Towers taught us anything, it was that terrorists are not necessarily half a world away, and could be right next door. How tragic and inexcusable it would be if another 9/11 type event were to take place given all the pieces of the puzzle were at hand, but unobtainable by the people who could have used them to prevented the attack. As submitted by former CIA analyst John A. Gentry to the Congressional intelligence committees in 1995, “Presidential leadership is critical” to the reform of the federal Intelligence Community (Gentry, 1995, p.7). “The firm involvement of the president in intelligence matters is essential to the coherent conduct of the agencies... Intelligence professionals are adept at nothing if not obfuscation and bureaucratic infighting.” (Gentry, 1995, p.32) It should be cause for alarm that this conversation is still taking place, and even more disturbing that it began before the terrorist attacks of 9/11.

As the debate continues over how best to reform the federal intelligence community, local police chiefs and sheriffs also have a role to play by strengthening their intelligence capabilities and forging partnerships with their federal partners. By bridging the gap between the national intelligence community and state and local police departments, the payoff will be more than the random car stop or search warrant that inadvertently thwarts a terrorist plot. It can be a response by agencies coordinating intelligence and effort to achieve the intended goal of countering terrorism. The choice is ours.

WORKS CITED

- 911 Commission Report*. By Thomas H. Kean, Chairman. New York, N.Y.: W.W. Norton & Company Inc, 2004.
- Agrast, Mark D., "Over-Classification and Pseudo-Classification: Making DHS the Gold Standard for Designating Classified and Sensitive Homeland Security Information," in *Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment held in Washington, D.C., June 28, 2007*, by Hearing of the U.S. House of Representatives Committee on Homeland Security (Washington, D.C.: U.S. House of Representative, 2007).
- Booz, Allen, "Human Capital in the Intelligence Community." Booz Allen Hamilton 2008. <http://www.boozallen.com/publications/article/40617265> (accessed July 29, 2009).
- Cummings, Alfred and Todd Masse. *FBI Intelligence Reform Since September 11, 2001: Issues and Options for Congress*. Washington, D.C.: Congressional Research Service. The Library of Congress, RL32336.
- Gentry, John A., "A Framework for Reform of the U.S. Intelligence Community". Congressional Intelligence Committees 1995. <http://www.fas.org/irp/gentry/index.html> (accessed July 29, 2009).
- International Association of Chiefs of Police (IACP). *The National Criminal Intelligence Sharing Plan*. Washington, DC: Bureau of Justice Assistance, 2003.
- Maus, N. Cathy. "Office Of Classification History Of Classification And Declassification." *U.S. Department Of Energy, Opennet*, July, 22, 1996. <https://www.osti.gov/opennet/forms.jsp?formurl=od/history.html#I3/> (accessed July 16, 2009).
- McConnell, John M. *Vision 2015: A Globally Networked and Integrated Intelligence Enterprise*. Washington, D.C.: Office of the Director of National Intelligence. Office of the Director of National Intelligence.
- OMB, "New Director of National Intelligence Promotes Smarter Classification." OMB Watch 2009. <http://www.ombwatch.org/node/9692> (accessed July 29, 2009).
- Project on National Security Reform (PSNR). *Forging a New Shield*. Arlington, VA: Project on National Security Reform, 2008.

- Rollins, John. *Fusion Centers: Issues and Options for Congress*. Washington, D.C.: Congressional Research Service. The Library of Congress, RL34070.
- Spaulding, Suzanne E., "Over-Classification and Pseudo-Classification: Making DHS the Gold Standard for Designating Classified and Sensitive Homeland Security Information." In *Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment held in Washington D.C., June 28, 2007*, by Hearing of the U.S. House of Representatives Committee on Homeland Security, 2. Washington D.C.: U.S. House of Representative, 2007.
- Treverton, Gregory F. *The Next Steps in Reshaping Intelligence*. Santa Monica, A: RAND Corporation. RAND Corporation, ISBN: 0-8330-3857-5, 2005.
- Treverton, Gregory F., *State and Local Intelligence in the War on Terrorism*. Santa Monica, CA: Rand Corporation, 2005.
- U.S. House Committee on Homeland Security Democratic Staff. *Beyond Connecting the Dots*. Washington, DC: Congress, 2005.
- Woodrow Wilson, "Woodrow Wilson Quips And Witticism," *Woodrow Wilson Presidential Library*, www.woodrowwilson.org/ (accessed February 2, 2009).