

***OVER-CLASSIFICATION AND PSEUDO-CLASSIFICATION OF
GOVERNMENT INFORMATION***

TESTIMONY OF
ASSISTANT COMMISSIONER MARK ZADRA
FLORIDA DEPARTMENT OF LAW ENFORCEMENT

THURSDAY, APRIL 26, 2007

PREPARED FOR THE
UNITED STATES HOUSE OF REPRESENTATIVES COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

OVER-CLASSIFICATION AND PSEUDO-CLASSIFICATION OF GOVERNMENT INFORMATION

Good morning Madam Chair and distinguished members of the Subcommittee.

My name is Mark Zadra and I am a 29-year member of the Florida Department of Law Enforcement (FDLE). FDLE is a statewide law enforcement agency that offers a wide range of investigative, technical and informational services to criminal justice agencies through its seven Regional Operations Centers, fifteen Field Offices, and six full service Crime Laboratories. Our primary mission is to promote public safety and strengthen domestic security by providing services in partnership with local, state and federal criminal justice agencies to prevent, investigate, and solve crimes while protecting Florida's citizens and visitors. FDLE utilizes an investigative strategy that comprises five primary focus areas including Violent Crime, Major Drugs, Economic Crimes, Public Integrity and Domestic Security.

I was recently appointed as FDLE's Assistant Commissioner of Public Safety Services however, prior to that appointment I served as the Special Agent in Charge of Domestic Security and Intelligence and the state's Homeland Security Advisor. In those roles I have overseen the development and implementation of various intelligence and information sharing programs and systems for FDLE and subsequently for the State of Florida. I have also overseen the development and implementation of the prevention component of Florida's Domestic Security Strategy and Florida's implementation of national information-sharing initiatives such as the Homeland Security Information Network (HSIN) and Florida's fusion center. I have further been an active participant on the Global Justice Information Sharing Initiative – Global Intelligence Working Group (GIWG). The goals of the GIWG include seamless sharing of intelligence information between systems, allowing for access to information throughout the law enforcement and public safety communities, creating an intelligence sharing plan, determining standards for intelligence sharing, developing model policies, determining training needs, and creating an outreach effort to inform law enforcement of the result of this effort. Over the last ten months I have been afforded an opportunity to provide input to the GIWG regarding the development of the recommended common protocols for sharing and protecting sensitive information and intelligence among multiple agencies with a role and responsibility in homeland security.

I am pleased to speak to the Committee today about the importance of common federal information-sharing protocols and the impact they have on state, local and tribal governments.

Prior to 9/11, law enforcement agencies at all levels had little need to share sensitive information with non law enforcement agencies. We had generally accepted practices for sharing information with one another but, because local and state law enforcement had minor involvement in the counterterrorism arena, we had limited experience with federally classified information. Little consideration was given to sharing sensitive information outside the law enforcement community, and sharing information with the private sector was generally not done.



The paradigm shifted after 9/11 when it became known that fourteen or more of the hijackers had lived, worked, traveled and trained across Florida while planning the atrocities they would ultimately commit. In their daily activities they left many clues that, if viewed together, may have predicted the plan and given authorities an opportunity to avert the catastrophic consequences. One month after the horror of 9/11, Florida experienced the first of several nationwide deaths from Anthrax which once again terrorized our nation. In light of these grim realities, we recognized that local, state and tribal resources – together with a whole new set of non-law enforcement partners including the private sector– represent the front line defense against terror and our best hope for terror prevention. Appropriately shared information is the key weapon in moving from the role of first responder to that of first preventer.

Sharing information with agencies such as health, fire, emergency managers, and even non-governmental entities with a role in the fight against terror presented new challenges, not just the inherent cultural ones, but those relating to law, policy/procedure, technology and logistics. Over the years since 9/11, collectively, we have made great strides in overcoming the cultural barriers to sharing information. In Florida, through our Domestic Security Strategy and governance structure, we routinely work with and share information across all entities that have a role in protecting the safety and security of our citizens.

Despite these successes and a new culture that encourages information sharing, barriers that impede the establishment of the desired national Information Sharing Environment (ISE) remain.

Common Document Markings and Dissemination Protocols

Perhaps the single largest impediment to an effective national ISE is the lack of nationally accepted common definitions for document markings and standard policy/procedure for handling, storing, and disseminating non-classified information. Sensitive but unclassified information, which is routinely received from federal and other state agencies, is needed by state, local, tribal and private sector partners that have a duty and responsibility to utilize it to provide for our safety and security. Consistency in definition and protocol is paramount to both fully sharing useful and actionable information, and protecting information that should not be shared.

Some states, like Florida have open record laws that mandate revealing information compiled by governmental agencies unless a specific “chapter and verse” exemption or confidentiality provision applies. Other states impose very restrictive dissemination requirements and afford broad protections from release to those without a need to know. Florida’s reputation as an open records state is widely known. While Florida law exempts certain information from public disclosure, the most likely exemptions applicable to the type of information that I am discussing are limited to criminal intelligence/investigative information and information that pertains to a facility’s physical security system plan or threat assessment. Exemptions provided by Florida’s Public Records Law are insufficient to protect against public disclosure of all types of sensitive information needed by Florida’s



domestic security partners. For example, there is no specific exemption in Florida's public records law for information provided to Florida by a non-Florida agency unless it is intelligence or investigative information—both of which have fairly narrow definitions under Florida law. The fear that sensitive information may not be protected under state law has a “chilling effect” on the free flow of important information from out-of-state agencies and non governmental entities to and from Florida. We also believe that the lack of a standard designation results in federal agencies over-classifying their information in an effort to protect it. Information and intelligence sharing partners need to know, with certainty, that the information they share will be appropriately protected. At the same time, we understand there must be appropriate limits on what is removed from public scrutiny and review, and a balance achieved between properly informing the public and ensuring the safety and security of our state and nation.

Developing and implementing a nationally accepted designation, with clear and appropriate handling and dissemination standards for sensitive information, will provide Florida and other states with the justification they need to encourage modification of state laws so that sensitive information can be protected in compliance with an accepted national standard.

Fortunately, there appears to be a workable solution to the concerns I have identified. Florida supports the implementation of the Controlled Unclassified Information (CUI) framework to replace the existing Sensitive But Unclassified (SBU) designation. The SBU designation contains numerous confusing designations used to mark unclassified information. The recommended CUI framework streamlines existing designations and provides handling requirements that facilitate wide distribution among law enforcement, homeland security, other government sectors and the private sector. We strongly believe that the information sharing environment mandated by Presidential Guideline 3 cannot be fully achieved without the implementation of a model such as the CUI framework. In the absence of common protocols, existing classification schemes will continue to be over utilized and/or improperly utilized, resulting in the inability of persons who receive information to adequately distribute it to those with a duty and responsibility to take action to protect our citizens.

We believe that the recommendations made by the Sensitive But Unclassified Working Group reflect workable solutions that could be accepted and replicated by most states. As a state representative I have been afforded an opportunity to review and comment on these recommendations during their formulation. I have also had the pleasure of personally meeting with Ambassador Thomas E. McNamara, Office of the Program Manager for the Information Sharing Environment and espousing Florida's views with respect to this and other information sharing topics.

Implementing CUI

In the absence of federal guidance and standards, many states, including Florida, have already expended resources in building systems and programs to fill the information needs of their consumers. Implementation of the new standard will involve varying degrees of fiscal and legislative impacts, however it is my opinion that acceptance will be facilitated if:



1. Guidelines are straight-forward and delivered in a clear, concise language;
2. A single, nationally accepted, encrypted communications system and federal information sharing encryption standard that can be used by non-law enforcement homeland security partners is designated;
3. Fiscal impacts are mitigated through grants for training and awareness programs, as well as for new equipment and system re-programming; and
4. Implementation timeline considers the potential need for state, local, and tribal governments to:
 - a. Change policy and/or rules to comply with new information dissemination requirements;
 - b. Purchase new equipment and/or system programming changes; and
 - c. Train appropriate personnel in markings, handling, storage and dissemination requirements.

For Official Use Only Tear Line Reporting

In response to post 9/11 criticism regarding failure to share information vertically and horizontally across the spectrum of homeland security partners, federal agencies are now providing state and local agencies with significant amounts of threat information. Much of the information that is still needed, however, is classified at the national level in order to protect sources, methods and means of collection and national security interests. State and local law enforcement fully understand and appreciate the need to protect certain information and restrict dissemination to only those with a need or right to know. Under most circumstances, however, we do not need to know the identity of federal sources or means and methods of intelligence collection - only whether or not the information has been deemed credible and specifically what actions that the state, local and tribal entities should take.

Florida believes the implementation of state and regional fusion centers is key to the establishment of the desired Information Sharing Environment. These centers bring properly trained and equipped intelligence professionals with appropriate clearances to connect the pieces of the puzzle and disseminate actionable intelligence. The problem remains that once the classified material is fused with the non-classified information from which analysis is performed, the information takes on the restrictions with the classified information which significantly narrows to whom and how it can be shared. Unfortunately, most of the operational components at the state and local level that may be benefit from the information, and would be otherwise available to report on the indicators and warnings being observed within the field, will not ever have access to this information. Tear line reports forwarded to fusion centers can help address this particular concern so that state, local and tribal law enforcement in addition to other discipline partners and the private sector receive information that they can act upon.

In conclusion, I would like to compliment our federal partners for recognizing the value of state, local and tribal representative's expertise and allowing input on such a critical initiative prior to its implementation. This has not always been the case, but is a testament



to the positive change in the information sharing culture and established and improved partnerships. I have been honored to be a member of the Global Intelligence Working Group and would like to acknowledge the work done by those professionals under the guidance of their Chairman, New York State Police Deputy Superintendent, Bart Johnson.

Lastly, Madam Chair and Members of the Sub Committee, thank you for the opportunity to have appeared and testified before you today. I can assure you the State of Florida is encouraged by your interest in facilitating an enhanced information sharing environment across the nation. It is my hope that this testimony and the understanding of Florida's desire to be a strong participant in the flow of critical sensitive information and intelligence nationally will be helpful in your endeavor.

Statement Follow-up Contact Address:

Assistant Commissioner Mark Zadra
Florida Department of Law Enforcement
Post Office Box 1489
Tallahassee, Florida 32302
850/410-7001
markzadra@fdle.state.fl.us

