Testimony of Wayne M. Murphy
Assistant Director
Directorate of Intelligence
Federal Bureau of Investigation
Intelligence, Information Sharing and Terrorism Risk Assessment
Subcommittee of the House Homeland Security Committee
26 April 2007

Good morning, Chairman Harman, Ranking Member Reichert, and members of the Subcommittee. I am pleased to be here today to demonstrate the commitment of the Federal Bureau of Investigation (FBI) to strengthening our nation's ability to share terrorism information. We are diligently working to fulfill the expectations Congress set forth in the Intelligence Reform and Terrorism Prevention Act of 2004. As the Assistant Director for Intelligence and the FBI Senior Executive for Information Sharing, I am at once responsible for, accountable to and have a vested interest in a successful Information Sharing Environment.

I am particularly pleased to be testifying today with Ambassador Ted McNamara, the Information Sharing Environment Program Manager, and Dr. Carter Morris, Director for Information Sharing and Knowledge Management, Intelligence and Analysis from the Department of Homeland Security. It has been my privilege over the past many months to work with these professionals and others as we seek to craft an outcome that matches both the letter and spirit of the task before us.

I join them today to discuss our collective efforts to develop a standardized framework for marking, safeguarding, and sharing "Controlled Unclassified Information" (CUI), or as it is more commonly known, "sensitive but unclassified" information.

On December 16, 2005, the President issued the "Guidelines for the Information Sharing Environment" as mandated by the Intelligence Reform and Terrorism Prevention Act of 2004. These Guidelines, among other things, set in motion a process for standardizing the handling of controlled unclassified information.

My nearly 24 years in the intelligence community have largely been served in an environment where I dealt almost exclusively with classified national security information. While those regimes could be complicated and required great discipline and attention to detail, by comparison they are far less challenging than my experience has been in working to organize a functional CUI framework. This is not because of a lack of commitment, focus and creativity in trying to address that framework, but because of the myriad of issues and interests that one encounters in the transitional world of information between what is controlled and what is not.

It is essential that we get it right, because it is information in this environment that can be of greatest utility when we need to share across a broad range of interests and constituencies. This framework provides a measure of protection for sensitive information to reassure those who might seek to hold such information in a classified or overly restrictive regime, which would deny others access and cause us to fail on our "duty to provide."

From an FBI perspective—getting it right is essential. The Information Sharing Environment, which is the lifeblood of our mission, spans the range from classified

national security information to fully open source. We must have the capacity to interpose information from all of these regimes and do so in a dynamic manner. We must have the agility to rapidly move information across security boundaries and into environments that make it more readily available and therefore of greater value to the broadest set of players. And across all of our partners, we must have a framework that allows for an immediate and common understanding of information's provenance and the implications that imparts. We must make the sharing of CUI a benefit, not a burden—especially on State, Local and Tribal police departments who would be disproportionately affected if asked to sustain a complex and expensive control framework. We must manage information in a way that sustains the confidence of people and organizations who share information that puts them at risk. Most important of all, we must respect the power of that information and the impact it holds for the rights and civil liberties of the American people who have entrusted us as its stewards. That also means that we must never use "control" as a way to deny the public access to information to which they are entitled.

For the FBI, achieving a streamlined CUI framework is much more than establishing a process, it's about shaping mindsets so we can fully shift from "need to know" to "duty to provide." This shift does not diminish our responsibility to properly protect the privacy rights and civil liberties of all Americans. It does not set up a framework that puts at greater risk our sources and methods and it does not compromise our capacity to conduct both an intelligence and law enforcement mission with full vigor and impact. Rather, this framework seeks to level the information sharing playing field through a common lexicon and a shared understanding of goals.

Unfortunately, the present set of policies and practices make it extremely difficult for well meaning individuals to act responsibly, appropriately and completely in this regime. There are well over 100 separate markings for CUI and there is no easy way for the recipient of information bearing an unfamiliar marking to find out what that marking means. Moreover, the same marking means different things in different parts of the Federal Government.

The FBI, working in close coordination with the Department of Justice, have jointly drawn upon the experience and the wisdom of state and local law enforcement personnel to help us understand better what kinds of CUI policies would be most helpful to them as we strive to share information without compromising either privacy or operational effectiveness. The Criminal Intelligence Coordinating Council (CICC) of the Global Justice Information Sharing Initiative has played an active role in advising us on this matter, including the convening on December 6, 2006 for an all-day meeting to discuss the practicability at the state and local level of various proposed "safeguards" for CUI. I would like to acknowledge here the particularly constructive role played by the CICC Chair, Col. Bart Johnson of the New York State Police. Col Johnson is forthright in explaining what Federal policies would be most helpful in enabling state and local law enforcement to play their part in preventing terrorism, but he is also sophisticated in his understanding of the many other factors that must be taken into account.

In our view there are three aspects of the current draft framework that are particularly important:

1. Every marking that appears on any CUI document in the future must have a clear and unambiguous meaning. There should be a website – accessible over the

Internet to everybody – on which the approved markings are defined, and no markings should ever be used that are not defined on this website. This will mean that recipients of shared information who want to do the right thing will easily be able to find out what protective measures are expected of them. I believe that this change will both increase sharing and decrease the risks of sharing.

2. All CUI information must be marked with a standardized level of safeguarding. For most CUI this safeguarding will be no more than ordinary prudence and common sense – don't discuss CUI when you can be overheard by people you don't intend to share it with, store it in an access controlled environment, as needed protect it with a password.
3. All CUI information must be marked with appropriate dissemination guidance so that recipients can easily understand what further dissemination is permitted.

All of us who have been part of this process wish we could have moved more quickly in reaching the point where we are today, but I believe the investment of time, the level of effort and the openness and commitment that has marked our dialog has done justice to the expectations of the American people.

Thank you for time, I look forward to answering your questions.