REMARKS OF J. WILLIAM LEONARD
DIRECTOR, INFORMATION SECURITY OVERSIGHT OFFICE (ISOO)
AT THE
NATIONAL CLASSIFICATION MANAGEMENT SOCIETY'S (NCMS)
ANNUAL TRAINING SEMINAR,
RENO, NV
JUNE 15, 2004

THE IMPORTANCE OF BASICS

Anyone who has traveled the Capital Beltway at rush hour in the vicinity of the Wilson Bridge outside of Washington, DC, recognizes that at times it can be a very fine line between civilization as we know it and anarchy. Most of the times, folks will do what is expected of them, patiently waiting in long lines of traffic, knowing that for traffic to move, drivers need to do what is expected of them – that they must observe the basic rules of the road. However, all it takes is a couple of yahoos driving on the shoulder at 50 mph with relative impunity, and the social order as we know it can rapidly break down. And if it's the governor or mayor disregarding the traffic laws – watch out!

The security classification system is not much different. To bring to bear the capabilities of the classification system for national security information, the information's originator need simply affix certain classification markings. However, it is not the security markings on the media that protects truly sensitive information from unauthorized disclosure; rather it is the people who deal with the information, their knowledge and understanding of the program, their faith in the integrity of the system represented by the markings, and their belief that everyone, to include agencies, will do what is expected of them. This knowledge, understanding, confidence, and expectation cannot be taken for granted. If they break down, chaos can ensue.

While the policy for security classification as set forth by the President is fundamentally sound, lately I have become increasingly concerned with respect to how the basics are being implemented in some quarters. The classification system is no different than other systems, in that it requires continuous attention and upkeep. Left to its own, the system will likely corrode and lose its overall effectiveness, placing in jeopardy all information cloaked in its protective measures. This, of course, has more than theoretical consequences in time of war; especially with respect to the resulting damage to the common defense should such information be subject to unauthorized disclosure. Yet, if we are not attentive, the demands of war can distract us from doing what is necessary today to ensure the continued efficacy and integrity of the classification system. Unfortunately, I have lately found some to use war as an excuse to disregard the basics of the security classification system. Yet, the classification system is not self-directing – which brings me to Basic #1 – the security classification system works, and its integrity is preserved, only when agency leadership demonstrates personal commitment

and commits senior management to make it work. President Bush called for nothing less when he issued his amendment to Executive Order 12958 last year.

The Order is replete with measures to ensure the classification system's continued effectiveness. For example, agencies must appoint senior officials to oversee the agency's program, promulgate internal regulations, establish and maintain security education and training programs as well as an ongoing self-inspection program, and commit the resources necessary to ensure effective implementation of the program, among other requirements. Many agencies are excelling at fulfilling these requirements; others are not. For example, 15 months after the President amended Executive Order 12958 in response to recommendations from a number of agencies, I am disappointed to note that many of these same agencies have yet to implement in their own internal regulations the new authorities they actively sought. This brings me to Basic #2 – the administrative aspects of the program, such as implementing regulations as well as education and training, are essential. Regulations are both empowering and limiting in that they permit agencies and their cleared employees to fully leverage the classification authority delegated to them by the President consistent with its intended purpose.

Nonetheless, as evidenced by a review of newspaper headlines over the past several months, agencies are finding it is increasingly difficult for them to hold their own cleared employees accountable for adhering to the requirements for protecting classified information unless the agencies likewise adhere to the same provisions. These headlines include reports of a Federal grand jury investigating leaks of classified information suspected as emanating from the highest levels of our Government; a former Secretary of a Federal Department finding himself a party to an investigation into the suspected unauthorized disclosure of classified information; members of the military and others finding themselves subjects of criminal prosecutions for mishandling of classified information; the disclosure of classified reports that feed the perception that the security classification system is used to conceal violations of law; and lately, the almost daily media reports quoting from purportedly leaked classified documents.

Added to the above is my experience that many senior officials will candidly acknowledge that the Government classifies too much information, although oftentimes the observation is made with respect to the activities of agencies other than their own. The potential issue of excessive classification is supported, in part, by agency input to ISOO that indicates that overall classification activity is up over the past several years. Yet, some individual agencies are not certain – others are largely unaware. They have no real idea how much information they generate is classified; whether the overall quantity is increasing or decreasing; what the explanations are for such changes; which elements within their organizations are most responsible for the changes; and most importantly of all – whether the changes are appropriate i.e., whether too much or too little information is being classified and whether for too long or too short a period of time. The absence of rudimentary baseline information such as this makes it difficult for agencies to ascertain the effectiveness of their classification efforts. I believe that it is no coincidence that some of these same agencies are currently experiencing a veritable epidemic of leaks –

part and parcel of what occurs when individuals begin to lose confidence in the security classification system.

I believe many of these issues arise when officials fail to recognize that when classifying national security information, they are employing the delegated constitutional authority of the President. The Order is clear that the employment of classification is an inherently discretionary act, based in large part upon the judgment of an original classifying authority. However, Basic #3 states that it is much more than an act of administrative convenience based upon a simple assertion. In delegating classification authority, the President has established clear parameters for it use, and certain burdens that must be satisfied. Unfortunately, some officials, at times, appear to believe that a simple assertion is all that is required for information to assume the legal safeguards of the classification system.

They forget, for example, that every act of classifying information must be able to trace its origin to an explicit decision by a responsible official who has been specifically delegated original classification authority. In addition, when required, the original classification authority must be able to identify or describe the damage to national security that would arise if the information was subject to unauthorized disclosure. Finally, the information must be owned by, produced by or for, or under the control of the United States Government and must fall into one or more of the categories of information specifically provided for in the Order. I am increasingly troubled by the number of times I need to remind certain officials of these basics.

Basic #4 acknowledges that like all authority, classification authority is not without limits. There are some very clear prohibitions with respect to the use of classification. Specifically, in no case can information be classified in order to conceal violations of law or to prevent embarrassment to a person, organization or agency. Nonetheless, you are all probably aware of certain information dealing with the abuse of detainees in Abu Ghraib prison that has apparently been classified. The Department of Defense is currently in the process of addressing a number of concerns I have raised with them in this regard and I await their formal reply. In the meantime, however, I am struck by a simple question when I see examples of classification such as what we have recently seen reported in the media. Specifically, "exactly from whom are we keeping the information secret?" In the case of detainee abuse, we are obviously not keeping it secret from the detainees – they experience the abuse and interrogation techniques first hand. And I assume we do not expect them to sign a nondisclosure agreement upon their release from custody based upon the premise that they had been exposed to classified information when they are subjected to abusive techniques.

And what is gained by classifying such activity? Our values as a society are such that they will invariably serve as a self-correcting measure when confronted with such abuses – thus the inevitability that such information will eventually become widely known. At the same time, the initial act of classification can negatively impact the timeliness and completeness of notifications provided to certain Government officials, thus impairing their ability to deal with ensuing issues. In the final analysis, we only

succeed in keeping the information from those who need to know it the most – the American people and their leaders – and even then, we only delay the inevitable.

While reflecting upon this issue, I was struck by a recent article in the *Los Angeles Times* entitled "Abu Ghraib Intelligence Soldier Describes Iraq Abuse In Detail." In the article, one military intelligence soldier related how, after a session in which abuse was inflicted upon some detainees, as he got ready to leave the cellblock amid anguished pleas for help from the prisoners, another soldier looked at him and asked, "Izzy, you're not going to tell anybody, are you?" In some regards, I believe that the affixing of classification markings to official reports of abuse and the employment of certain interrogation techniques can be akin to asking Izzy, out of a sense of shame and fear of being found out, not to tell anybody.

My current concerns extend to the area of declassification as well. Basic #5 acknowledges that one of the principal procedures for maintaining the effectiveness of the classification system is the purging from the safeguarding system of information that no longer requires protection in the interest of national security. In addition to processes such as automatic and systematic declassification, as well as mandatory declassification reviews, the Executive order clearly states that "information shall be declassified as soon as it no longer meets the standards for classification" (§ 3.1). Elsewhere, the Order specifically prohibits the use of classification "to prevent or delay the release of information that does not require protection in the interest of the national security" (§ 1.7 (a) (4)). Declassification cannot be regarded as a "fair weather project," something we tend to when resources are plentiful but which quickly falls off the priority list when times get tough, especially in times of national security challenges. Nonetheless, it is disappointing to note that declassification activity has been down for the past several years.

In some quarters, when it comes to classification in times of national security challenges, when available resources are distracted elsewhere, the approach toward classification can be to "err on the side of caution," by classifying and delaying declassification "when in doubt" and "asking questions later." Yet, the classification system is too important, and the consequences resulting from improper implementation too severe, to allow "error" to be a part of any implementation strategy. Error from either perspective, both too little and too much classification, is not an option. Too much classification unnecessarily impedes effective information sharing, and inappropriate classification undermines the integrity of the entire process. Too little classification can subject our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations to potential harm.

In this regard, Basic #6, proactive oversight by an agency of its security classification program, is crucial – it is not a luxury. To allow information that will not cause damage to national security to remain in the classification system, or to enter the system in the first instance, places all classified information at needless increased risk.

In response to these concerns, I have recently written to all agency heads asking them to closely examine their efforts in addressing the basics in establishing and maintaining an effective security classification program at their agency. Each has been asked to give special emphasis to reviewing how they provide their personnel who deal with classified information the knowledge and understanding required to make the program work, and what positive steps they take to ensure the continued integrity of the system. This includes ensuring that information that requires protection is properly identified and safeguarded; and, equally important, that information not eligible for inclusion in the classification system remains unclassified or is promptly declassified.

The integrity of the system will not be maintained on its own. It requires clear, forceful and continuous effort by senior leadership to make it happen! They cannot, however, do this without the expert assistance of you, the information security professional. Upon your return from this seminar, I ask you to perform your own assessment as to how well your organization adheres to these basics and then to confer with your senior leadership in crafting a strategy to make it even better.

In a related manner, this summer I plan to issue a special report to the President highlighting agency progress in fulfilling his direction set forth in the Order to achieve complete implementation of automatic declassification by December 31, 2006. It is essential that agencies recapture the momentum of prior years in their declassification efforts, especially with respect to interagency process improvements, particularly in the areas of joint training, increased empowerment of reviewers, and increased delegation of authority between agencies. And it is important to be mindful that 2006 is just the beginning, not the end. The goal is to institutionalize automatic declassification so that it becomes an integral part of the process in 2007 and every year thereafter.

While, as your theme suggests, security may be a sure bet, we cannot afford to gamble with the framework that protects classified national security information. The integrity of the security classification program is essential to our nation's continued well-being. The consequences of failure are too high. Thus, the American people expect and deserve nothing less than that we get the basics right each and every day.

I'd like to close by acknowledging the life long contributions to national security in general, and the industrial security program in particular, by your recently deceased president, Lonnie Buckles. You and your society can take justifiable pride in the fact that Lonnie was a well recognized leader in the National Industrial Security Program. Our nation has benefited from Lonnie's membership on the National Industrial Security Program Policy Advisory Committee, which I have the privilege of chairing. As a member of this group, Lonnie was responsible for recommending changes in industrial security policy to the President, the Secretary of Defense, and other executive branch officials. It's a role that Lonnie fulfilled with relish. He was committed to making a difference for the better in everything he did – a responsibility he repeatedly fulfilled. We can all take solace from the tremendous good that has come from Lonnie's dedication and professionalism. He has left a lasting legacy in the field of national security in service to his country. He will be missed.