Remarks on Classification
The Hon. Lee H. Hamilton
Information Security Oversight Office
October 18, 2005

Good morning. Thank you, Dr. Weinstein, for that introduction. It is my pleasure to be with you at this important symposium on classified national security information.

You are the experts on secrecy; I am not. Let me say how pleased I am to see you, the real experts, come together this morning to seriously address classification and declassification related topics.

I will offer some reflections based on several decades dealing with classified information, and from my experience on several national security committees in the Congress, the Moynihan Commission on secrecy, and the 9/11 Commission.

Let me begin by assessing the broad challenges presented by over-classification. I will then offer my thoughts on key principles that should guide our handling of secure information.

The Problem of Over-Classification

The United States government collects and handles an awesome amount of information.

We collect millions of bites of data every minute. We generate assessments on everything under the sun:

-- The actions and intentions of every government and leader in the world;

-- The identity of every group that means us harm;

-- What happens when OPEC leaders get together;

-- Which world leader has the flu;

-- What is being said in a cave halfway around the globe;

-- The anticipated results of this or that election.

This information works itself through many channels. As we found on the 9/11 Commission, it leaves an extensive paper trail:

-- In the policymaking process;

-- In the communication within and among agencies;

-- In decision-making from the unit in the field to the President;

-- and in legal, policy and political considerations across the government.

How should we handle all of this information? Who should have access to what information? How should we provide – or restrict – that access?

Over-classification

To begin, too much information is classified.

Some estimates of the number of classified documents reach into the trillions. Several senior officials have estimated that more than 50% of classified information does not need to remain secret. During our work on the 9/11 Commission, we repeatedly came across information that was classified that was already publicly known.

Tom Kean, chairman of the 9/11 Commission – and one not accustomed to dealing with classified material – must have asked me scores, if not hundreds, of times: why is this material classified? I never had a very satisfactory answer for him.

And the trend is toward more and more classification:

-- There were over 15 million national security classification decisions made in 2003 – up from a low of around 4 million in 1994.

-- The Information Security Oversight Office declassified 100 million pages of documents in 2001, and only 28 million in 2004.

Why is this over-classification a concern?

-- **Cynicism**. An abundance of secrecy leads to cynicism on the part of the American people.

At a time when the U.S. intelligence community is under intense scrutiny in the aftermath of 9/11 and the failure to find weapons of mass destruction in Iraq, we only increase public skepticism about our government by denying the public information.

Secrecy breeds suspicion. For instance, when a few paragraphs were redacted from the Congressional Joint Inquiry into 9/11, there was great speculation about what was in those paragraphs – particularly concerning one foreign country. To some, it seemed sinister. To others, it was downright amusing. To most, it was unnecessary. To all, it was frustrating.

Conversely, sunshine breeds satisfaction among the American people. During the 9/11 Commission, I was impressed by the intense hunger for facts, manifested in the interest in our hearings and final report. One feature that drew praise was the absence of redactions from our staff statements and report.

I was pleased by the amount of declassification that we achieved during the 9/11 Commission. The report would not have been as well received as it was had there been extensive redactions. It took a lot of hard work – principally by staff – to achieve that result.

The American people learned the full, unvarnished story of 9/11. Because they achieved a fuller understanding of 9/11, they had an opportunity to learn the lessons of the past and apply them to the future: without the full airing of the facts, I do not think that Congress would have acted to reform our intelligence agencies.

I want more information made publicly available. Representative democracy demands the free flow of information, so that the American people can be informed about the activities of their representatives and their government.

I want more journalists, scholars, archivists and citizens learning about our past and our government, because I want people to know what their government does – or does not – do, and because I believe it is essential for us to actually learn the lessons of the past; only then can we prepare for the future.

-- Stove-piping. An abundance of secrecy leads to stove piping – instead of sharing – within the government.

The 9/11 Commission found countless examples of information not being properly shared in the run-up to 9/11:

> -- In some cases, information could have been accessed if it was asked for – but it wasn't.
>
> -- In some cases, specific information was asked for and rejected because it could not be shared horizontally – within an agency; or vertically – among agencies.
>
> -- In some cases, information could only be distributed via compartmented channel, so it could not get to the right person, or be part of a comprehensive or competitive analysis.

These difficulties in information sharing led to missed opportunities. The FBI Director did not find out about Moussaoui – described as interested in flight training for the purpose of using an airplane in a terrorist attack – until after 9/11, even though the CIA Director knew about it; the CIA never told the FBI that one of the future hijackers had acquired a U.S. visa; indications of an impending attack were not connected to Moussaoui's interest in flying, or the known presence of al Qaeda operatives in the U.S.

To put it simply: the intelligence community did not know what it knew about al Qaeda before 9/11, in part because stove-piping and secrecy prevented the pooling and analysis of all intelligence on terrorism.

That is why we recommended the creation of a National Counter-terrorism Center – to serve as the center in the government for all information, foreign and domestic, on the terrorist threat. And that is why we recommended new systems and methods of information sharing across the government.

-- Selective-Use: An abundance of secrecy enables the selective use of intelligence to "sell" certain policies: the "politicization" of intelligence.

This received much attention after the failure to find weapons of mass destruction in Iraq. Looking back at the pre-war debate, the most dire assessments of Iraq's capabilities received a full and prominent airing; the more measured assessments were buried in footnotes, or left out of widely dispersed intelligence assessments altogether.

This is sadly nothing new. Intelligence has often been used selectively over the year to influence public debate. He who controls the information has a decided advantage in the policy debate.

People look for information that supports their views; subordinates look for information that satisfies their superiors.

To a large extent, all eight presidents I have worked with looked for – and received – intelligence that justified their preferred policy.

But intelligence should be used as a tool to make good policy – not as a tool to make a policy look good. By providing the public with more information, greater openness can help ensure – even if it does not guarantee – that the public debate about policy choices takes place, to the maximum extent possible, with more, not less information where it should be: in the open.

Indeed, openness is a safeguard against the selective use – or politicization – of intelligence. As Justice Brandeis said: "Sunlight is the best of disinfectants."

-- Cost-Effectiveness. An abundance of secrecy costs the American people an extraordinary amount of money.

It is simply not cost-effective to spend billions of dollars unnecessarily keeping information secret. Indeed, it has cost this government $7 billion to keep its secrets since 2001.

If we classified only what is valuable, we could focus our resources to protect that information.

-- Lack of Focus. Finally, an abundance of secrecy diminishes the attention paid to safeguarding information that really does need to remain out of the public's view.

Our efforts should be focused on that information that really does need to be kept secret to protect the nation's security. Needlessly stamping information "secret" breeds a lack of regard for material that is properly classified, and a carelessness among all of us who handle it. It also overloads our capacity to protect truly sensitive information. To paraphrase Justice Potter: when everything is classified, then nothing is classified.

As we said in the Moynihan report: Secrecy can be protected more effectively if secrecy is reduced overall.

Need to Know versus Need to Share

So why do we have so much trouble declassifying information?

Part of the problem is the "need to know" versus "the need to share."

The need to know approach, which has been sacrosanct in the intelligence community, assumes that it is possible to know, in advance, who will need access to a piece of information. But in a fast-changing world, that approach is incomplete.

In the Cold War, we assumed that there was a greater risk in the inadvertent disclosure of secret information; in the war on terror, there may be a greater risk in the failure to share information.

This is true within government: the local police commissioner needs to be aware of the piece of intelligence gathered in Pakistan, or the FBI agent needs to be aware of the communication intercepted by the NSA.

This is true outside of government: for instance, before 9/11, the American people were far too ill-informed about the threat of terrorism – a threat that was well-known, and widely feared, within the American peoples' intelligence community. We do not want to make that mistake with future threats to our security.

That is why the 9/11 Commission recommended information procedures that provide an incentive for sharing information, and a better balance between the security of information and the sharing of it.

Right now, all of the incentive is for classifying information. You might say the motto is: "when in doubt, classify."

People in government think they can get into trouble declassifying information, but that they cannot get in trouble if they stamp "Secret" on a document. There are risks for mistakenly declassifying information – administrative, civil, and criminal – but no risks for classifying – and not sharing – information.

We need to readjust that balance. We need to make it clear that the American people can be hurt by the disclosure of certain information, but they are also hurt by the over-classification of information.

Now don't misunderstand me. We cannot and should not do away with the need to know principle. A security clearance should not entitle an individual to everything, nor should information be declassified haphazardly.

The point is that a better balance is needed between these two important principles: the need to know and the need to share.

Of course, we have to protect our sources and methods. The intelligence community deals with the most sensitive matters in the United States government; seeks information people don't want to give us; carries out clandestine operations; and protects the lives of a lot of people who carry out missions. It must inform policymakers with discretion. These are awesome responsibilities.

Leaks – for instance – can be terribly damaging. In the late-90s, it leaked out in *The Washington Times* that the U.S. was using Osama bin Ladin's satellite phone to track his whereabouts. Bin Ladin stopped using that phone; we lost his trail.

But we can make more information available without compromising sources and methods. For instance, the 9/11 Commission proposed separating more intelligence data from the sources and methods by which it is attained – so that people can be made aware of intelligence conclusions without knowing where the "raw intelligence" came from.

There are also technological fixes that can streamline the handling and declassification of information. We need networks that enable the sharing of information within and among agencies. And we need more rapid systems of declassifying information that is needlessly, and expensively, held secret.

Within agencies, and within the government as a whole, we need a culture that supports sharing and openness as vigilantly as it keeps necessary secrets.

Principles for Handling Classified Information

Let me conclude by offering some general principles that should guide the handling of secure information.

1. Some information must be kept secret

There are secrets worth protecting: to protect national security, to engage in effective diplomacy, to fight terrorism and to stop the proliferation of weapons of mass destruction.

The challenge is to seriously examine what really does need to be kept secret, and to fully protect that information – but to make public all other information.

Some intelligence work – and policy deliberation – necessarily takes place in the shadows. The need to know principle must not be abandoned. Sources and methods must be protected.

2. Information must be more widely shared within government

The status quo on sharing has not been working. It tilts decisively, if not dangerously, toward secrecy.

Information must be shared vertically within an organization, and horizontally across the agencies of the intelligence community. It will take new rules and new technologies and new leadership so that our analysts can work from the full set of facts – from all sources, foreign and domestic – to uncover future 9/11 plots.

It is costly and counter-productive if, in government, the left hand does not know what the right hand is doing. We need to leverage the information revolution so that we maximize our resources, and find ways to get the right information to the right person at the right time.

3. Information must be made available – to the maximum extent possible – to the American people.

Few attitudes I encountered in government frustrated me more than the view that says: "Trust me. I know what is best for the national security of the U.S., and you are not trustworthy."

National security agencies should be more forthcoming in making information available.

Because of secrecy:

-- there is little media coverage of the intelligence community;

-- there are few academic studies of the intelligence community;

-- there are not active interest groups lobbying on intelligence issues, other than those who make expensive intelligence-gathering technologies;

-- and there is little public input into how the intelligence community conducts its business.

If more information about the intelligence community were available, public understanding of intelligence would improve. If public understanding were improved, cynicism would decline, and public support for policies and the mission of the intelligence community would increase.

When we over-classify information, we avoid public debate on important matters of national security. Secrecy should not be used as a means of avoiding public debate on a policy. Doing so denies the American people the accountability and transparency that is at the core of American democracy.

Openness can also save lives. Informed citizens can make more alert citizens – think of those people who tackled Richard Reid, the alleged shoe bomber, when he tried to light a match. What if more people were informed of the terrorist threat before 9/11? Armed with information, people would have been more alert.

What must be better understood is how much damage is done to our country when we deny information to the people through excessive secrecy.

Conclusion

George Marshall once explained to one of his officers: "We have a great asset and that is that our people, our countrymen, do not distrust us and do not fear us. Our countrymen, our fellow citizens, are not afraid of us. They don't harbor any ideas that we intend to alter the government of the country or the nature of this government in any way. This is a secret trust."

To earn and keep that trust, the United States government must keep its end of the bargain. We must:

-- hold secret information that, if made public, could endanger American lives or interests;

-- ensure that a "need to share" permeates the government, so that information is shared instead of stove-piped;

-- declassify as much information as possible, so that the American people are informed about the activities of their government.

The basic paradox is that secrets fit awkwardly into a democracy, but secrets are sometimes necessary to protect our democracy.

You and I know that representative democracy depends upon an informed, two-way dialogue. As you ponder the various ways to solve the complicated problems that come with handling secure information, I applaud your efforts to consider how that dialogue can be stronger, more open, and more free.