STATEMENT OF

KENNETH L. WAINSTEIN
PARTNER, O'MELVENY & MYERS LLP

BEFORE THE

SENATE COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON TERRORISM AND HOMELAND SECURITY

CONCERNING

THE ESPIONAGE STATUTES: A LOOK BACK AND A LOOK FORWARD

PRESENTED ON

MAY 12, 2010

Chairman Cardin, Ranking Member Kyl and Members of the Subcommittee on Terrorism and Homeland Security, thank you for inviting me to testify before you today about the legal framework for defending our government against espionage and the disclosure of sensitive information.

My name is Ken Wainstein, and I am a partner at the law firm of O'Melveny & Myers. Prior to my leaving the government in January of last year, I served in a variety of capacities, including Homeland Security Advisor to the President, Assistant Attorney General for National Security at the Department of Justice, United States Attorney, General Counsel and Chief of Staff of the FBI and career federal prosecutor. I was honored to work with the men and women of the Intelligence Community and the many others who defend our national security apparatus against those who seek to access or disclose its most sensitive information for unauthorized purposes. I am also honored to appear today alongside my two co-panelists, both men with tremendous expertise in the field of counter-espionage.

Since the attacks of September 11, 2001, I have spent much of my professional career in the national security world, where sensitive sources and methods are the lifeblood of our national security operations. Whether it was a particular electronic surveillance we secured at the Justice Department that gave us insight into our adversaries' terrorist plans or source information that factored into decision making at the White House, I have seen the vital role that sensitive information plays in our national security operations and how those operations can be put in jeopardy whenever that information is compromised. And unfortunately, that information is compromised all too frequently.

While every disclosure of sensitive information is different in terms of motive and parties, for purposes of this discussion I would like to focus on two general categories. The first category includes those instances where a government official passes sensitive information to an agent of a foreign government or other foreign power -- the classic espionage scenario with spies like Aldrich Ames or Robert Hanssen who betray their country for money, out of resentment against their government or agency, or out of misplaced loyalty or affinity for another country or foreign power. The second, and more common, scenario is the leak of sensitive information to the press by a government official whose motive may range from base self-interest to a laudable whistleblower's desire to change government operations for the better.

We are all quick to condemn the traitorous actions of the classic spies, and the Justice Department has mounted strong prosecution efforts whenever such spies have been identified over the years. We must also recognize, however, that the media leaker can do grievous damage to our national security.

While I appreciate that some of those responsible for media leaks -- i.e. the "whistleblowers" -- may genuinely feel they are acting in the country's best interests, I share the concern expressed by many in Congress about the need to enhance our defenses against such disclosures. An important part of that effort is ensuring that, in the

appropriate cases, we investigate and prosecute those who disclose our operational secrets. As you know, however, the Department of Justice does not have a lengthy record of successful leak prosecutions. While it has brought many strong espionage cases over the years, there have been very few prosecutions for leaks to the media.

That thin track record is not for a lack of effort on the part of the investigators and prosecutors. Rather, it is a result of the myriad obstacles that stand in the way of building a prosecutable media leak case. Those obstacles are many, and they include the following:

First, it is often very difficult to identify the leaker in the first place, given the large universe of people who often are privy to the sensitive information that was disclosed. It is not uncommon for many people to be read into the most highly-classified program or to be recipients of intelligence derived therefrom -- a problem which has only gotten worse with the increased integration and information-sharing we have seen in the intelligence and law enforcement communities since the 9/11 attacks.

Second, our leak investigations operate under the limitations in the Justice Department's internal regulations, which make it difficult to obtain information from the one party who is in the best position to identify the leaker -- the member of the media who received the leaked information. These regulations have been in place for years, and they serve the important purpose of ensuring that "the prosecutorial power of the Government [is] not . . . used in such a way that it impairs a reporter's responsibility to cover as broadly as possible controversial public issues." United States Attorneys' Manual, Section 9-13.400. The upshot is, however, that an investigator who wants to use a subpoena to compel information from a reporter can do so only after the Attorney General personally grants his or her permission -- a process that has resulted in only about two dozen subpoenas to the press over the past couple decades.

Third, even when the leaker is identified, the agency whose information was compromised is often reluctant to proceed with the prosecution. The concern is that charging and trying the case will both highlight the compromised information and likely result in the disclosure of further sensitive information that may come within the ambit of criminal discovery or admissible evidence. While the Classified Information Procedures Act helps to minimize the effects of the latter, there is always a concern about disclosure when a national security crime is prosecuted and brought to a public trial.

Finally, even if the Justice Department succeeds in identifying and indicting the suspected leaker, it can expect to face a vigorous defense. These cases typically feature legal challenges from defense counsel invoking everything from first amendment principles to allegations of improper classification to arguments that their client's alleged leak was actually an authorized disclosure within the scope of his or her official duties. The Rosen and Weissman case that was recently dismissed after years of litigation is an example of the difficult issues that these cases present.

For all these reasons, leak cases are exceptionally challenging, and successful prosecutions are few and far between.

The question for today is whether any of these obstacles can or should be addressed by changes to the governing legislation. While I agree with those who find the espionage statutes cumbersome and antiquated in their approach and terminology, I do not see a legislative silver bullet that would overcome all of these obstacles.

There are, however, a few areas of legislative initiative this Committee might wish to consider.

First, the committee might examine whether government contractors are adequately covered by the espionage laws. These statutes were drafted before the influx of contractors into the government's most sensitive operations. The past few decades have seen a dramatic increase in the number of private contractors who carry the highest clearances and share in the government's most closely-guarded secrets. While prosecutors can reach private contractors with most of the provisions in the espionage statutes, there is one important provision prohibiting the disclosure of classified information by a government official to a foreign power -- 50 U.S.C. Section 783 -- which does not extend to contractors. While prosecutors may still succeed in developing a case based on other statutes -- which, unlike Section 783, are not limited to government employees -- there are scenarios where a contractor's espionage would be more difficult to prosecute because of that gap in the statute. In the absence of any principled reason for treating them differently, Congress could consider putting government employees and contractors on the same footing in that provision.

Second, Congress could consider amending the Classified Information Procedures Act to ensure better protection of sensitive information in criminal trials. Experience with that statute since 9/11 has pointed up a number of areas where CIPA could do a better job of accommodating the government's concerns about classified information in public criminal proceedings. As Senator Kyl has proposed, the statute can be improved by: (1) mandating that the government can submit its arguments for protecting classified information in the discovery process directly to the court without having to share those arguments and the classified information with the defendant; and (2) clarifying that the government can appeal any trial judge's ruling that runs the risk of causing classified information to be disclosed at trial. Others have suggested different amendments, such as clearly authorizing courts to keep the public from seeing sensitive information being used at trial -- an issue that was vigorously litigated in the Rosen and Weissman case -- or explicitly allowing for anonymous testimony by intelligence officials operating under cover. With the current national discussion about prosecuting more international terrorism cases in Article III courts, this would be a good time to consider these and other suggestions for amending CIPA and enhancing our ability to protect sensitive information that is used in the criminal process.

Third, Congress might consider providing a definition of protected "defense information" that fully covers the foreign affairs information -- such as information about

other governments' personnel, plans and policies -- that is so vital to formulating our foreign policy and calibrating our posture vis-à-vis other countries.

In a more general sense, Congress can use this hearing -- and any ensuing hearings -- to encourage respect for our nation's operational secrets. Congress can send the basic message that it does not condone the unauthorized release of classified information about our national security operations. It can point out, for instance, that whistleblowing is no longer a sufficient justification for divulging secrets. In the situation where a well-meaning government official sincerely feels the need to "blow the whistle" on perceived government misconduct, there are now lawful channels for doing so. Congress has passed whistleblower statutes that facilitate and protect genuine whistleblowing, including the Intelligence Community Whistleblower Protection Act, which provides a procedure for whistleblowers to advise the Intelligence Committees about alleged wrongdoing in an intelligence program without publicly disclosing sensitive information about that program.

Congress can also encourage the Administration in its efforts to staunch the outflow of sensitive information by pursuing investigations into those leaks that are particularly egregious or damaging.

Finally, Congress can encourage the intelligence agencies in their effort to use administrative sanctions to deter leaking within their ranks. Recognizing the difficulties of using the criminal process -- even when the leaker can be identified -- agencies have instead focused on sanctioning the responsible employee with personnel action or withdrawal of his or her security clearances. Although they do not pack the punch of a criminal conviction, such sanctions nonetheless have a significant deterrent effect on the rest of the workforce.

* * * * * * * *

No matter where one stands on the political spectrum or in the current national security policy debates, we should all recognize that the unchecked leaking of sensitive information can cause grave harm to our national security. Congress plays an important role in addressing that problem -- whether by legislation, by oversight or by simple exhortation -- and I applaud this Committee for the initiative it is showing with today's hearing.

I appreciate your including me in this important effort, and I stand ready to answer any further questions you many have.