Department of Justice

FOR IMMEDIATE RELEASE
THURSDAY, JUNE 20, 2013
WWW.JUSTICE.GOV

NSD
(202) 514-2007
TTY (866) 544-5309

REMARKS AS PREPARED FOR DELIVERY BY JOHN CARLIN, ACTING ASSISTANT ATTORNEY GENERAL FOR NATIONAL SECURITY AT THE AMERICAN BAR ASSOCIATION HOMELAND SECURITY LAW INSTITUTE

WASHINGTON, DC

- Good morning. I would like to thank the ABA Homeland Security Law Institute for inviting me today, and particularly Joe Whitley and Holly Hampton for putting on this program. They have brought together some very distinguished speakers. It is great to be a part of this event again this year.

- Thanks also to all of you for being here. This audience is made up of experts from all corners of the national security world, and this event gives us all an opportunity to share knowledge, exchange views, and learn from one another.

The Shifting Landscape

- We've seen changes in the nature of the threat landscape, and today I will discuss what those changes—and the government's response to them—mean for the roles and responsibilities of national security lawyers in the government.

- In particular, I will focus on the National Security Division of the Department of Justice, the organization I am proud to represent today. Created only seven years ago—as the first new litigating division in the Department in about half a century—NSD has already evolved to face growing and changing threats to this nation. As the ground shifts underneath us once again, we are ready to continue that evolution.

- In my career, I have been privileged to learn from some legendary public servants. They have taught me a lot about the transformative power of lawyers in our government—and the sense of duty and mission that comes with it. While serving as FBI Director Mueller's Special Counsel and, later, as Chief of Staff of the FBI, I watched as lawyers helped the Bureau evolve from a law enforcement agency into a threat-based, intelligence-driven national security organization.

- As the transformation of the FBI reflects, it no longer makes sense to talk about a law enforcement approach versus an intelligence, or even a military, one. National security

successes demand integration – putting every available tool on the table, and picking the combination that will disrupt the threat.

- And as all of you know, that threat continues to shift:

    - over the past decade, terrorism has become increasingly diverse and decentralized – and the threat posed by homegrown violent extremism is now in stark relief after the tragic attacks on the Boston Marathon;

    - the cyber threat continues to present risks to our security and prosperity; and

    - the delicate balance of collecting and using intelligence while safeguarding privacy and civil liberties is a topic of national conversation.

- Each of these changes highlights the critical role played by lawyers in the national security apparatus. Lawyers help define our toolsets, our options, and our solutions. And you also protect our privacy, our civil liberties, and our values.

- NSD in many respects is on the front lines of these efforts. To understand how we approach that mission, I'd like to tell two brief stories.

The Advent of Oversight

- The first is about the creation of the Foreign Intelligence Surveillance Act (or "FISA"), which put in place the legal structures and oversight mechanisms that continue to govern some of the most important and sensitive national security programs in our government.

- The second is about the lessons learned from 9/11. In response to that event, we made significant adjustments – legal, cultural, and organizational – in our approach to counterterrorism. These changes magnified the importance of FISA and the legal architecture it created.

- FISA was passed in 1978 in the wake of a series of public scandals involving abuses of wiretaps and surveillance for political purposes. The history of these abuses is exhaustively documented in the Church Commission report.

- To address abuses, the Church Report called for a stronger regime of oversight led by the Attorney General. The Church Commission believed that the Attorney General, "as the chief legal officer of the United States," was "the most appropriate official to be charged with ensuring that . . . intelligence agencies conduct their activities in accordance with the law."

- In enacting FISA, Congress designed the exclusive means by which the government could conduct electronic surveillance to obtain foreign intelligence information within the United States.

- FISA created a framework of checks and balances to bring to bear the constitutional authority of *all three* branches of Government in the service of oversight.

    - The first check is judicial oversight. The statute created the Foreign Intelligence Surveillance Court (known as the "FISC"), and designates Article III judges to serve on the FISC on a rotating and part-time basis.

    - The second check is Congressional oversight – and in particular, a searching form of oversight by the Intelligence Committees, which are kept fully and currently informed about all activities under FISA. From the beginning, FISA required extensive interaction between the Executive Branch and Congress, and the oversight role of Congress has only grown over time.

    - Finally, the third check is the dramatic enhancement of Executive Branch oversight. Not only are there civil and criminal penalties for misuses of FISA, there are Inspectors General reviews, and oversight and compliance programs throughout the intelligence community.

- Congress required such extensive oversight in part because it recognized that the details of these activities must remain secret from our adversaries at the price of also remaining secret from the general public. In place of direct oversight by the public, FISA depends upon—and puts in place a legal structure that demands—repeated interactions among all three branches of government.

- Indeed, in one of its few published opinions, the FISC remarked upon the statutory requirement that the Intelligence Committees receive copies of FISC opinions "that include significant construction or interpretation of [FISA] provisions," suggesting that such a requirement reflects "an understanding on the part of Congress that even legally significant decisions [of the FISC] would not routinely be available to the public."

- Because of the classified nature of its work, few institutions in government are as little understood as the FISC. Although the applications to the court are necessarily classified, its qualifications are a matter of public record. Currently, eleven Article III judges sit on the FISC on a rotating basis. Although all were at one time nominated by the President and confirmed by the Senate, these judges were selected for the FISC by the Chief Justice of the United States. All are distinguished jurists with a broad and varied set of experiences. Even while serving on the FISC, these judges spend the bulk of their time in their home districts deciding their routine civil and criminal matters.

- That the FISC ultimately denies very few applications is simply a reflection of the unique nature of *ex parte* FISC proceedings. As former Attorney General Mukasey explained, the government's low denial rate in the FISC is attributable in no small measure to the fact that the Department of Justice has "an independent obligation to determine that every FISA application meets the statutory standard before we submit it" and treats that obligation with the utmost seriousness and care. In addition, the FISC at times requests additional information prior to approval of an application, which the Government

endeavors to provide in an effort to satisfy any questions or concerns that the Court may have. On other occasions, the FISC modifies the authorizations that it grants in response to Government applications.

- In a rare public statement about the court's operations, Judge Walton, the Presiding Judge of the FISC, explained that "[t]here is a rigorous review process of applications submitted by the executive branch, spearheaded initially by five judicial branch lawyers who are national security experts and then by the judges, to ensure that the court's authorizations comport with what the applicable statutes authorize." He called the notion "that the court is a rubber stamp . . . absolutely false."

- Having had the experience of appearing before Judge Walton as a prosecutor handling violent crime cases in D.C. superior court and in federal court, I can speak firsthand to his ability to be a forceful and thoughtful critic of the government. As is equally true of his distinguished colleagues, Judge Walton exhibits no less independence in his work on the FISC than he does in his everyday job.

The Post-9/11 Imperative

- This backdrop provides good context for the creation of the post-9/11 national security community, and the creation of NSD.

- As you know, after September 11, there was significant criticism of legal and procedural impediments to information sharing—the so-called "wall" between U.S. law enforcement agents and intelligence officers. Where did the wall come from?

    - As originally drafted, FISA required senior national security officials to swear, in support of surveillance applications, that "the purpose" of the application was to obtain "foreign intelligence."

    - And court decisions of the FISC and legal interpretations inside the Executive Branch took a relatively narrow view of what qualified as "foreign intelligence purpose" such that it excluded a purpose to assist a criminal prosecution – even when the case involved a spy or terrorist.

- The exclusion of a purpose to assist a prosecution created an anomaly in the law: A FISA application could be filed to acquire information for a military operation designed to *capture* a suspected terrorist. But an application could *not* be used against that same terrorist to obtain evidence in a criminal investigation to effect an *arrest*.

- In essence, the law recognized a false dichotomy between law enforcement and national security: it denied the possibility that law enforcement could itself be used as a tool to further national security, because it could disrupt the threat by taking bad actors off the streets and, at times, encouraging them to cooperate.

- As a result, a culture and practice developed within the Department and more broadly in which coordination between intelligence personnel and law enforcement personnel was restricted.

- In the wake of September 11, reform measures focused on legal and procedural impediments to information sharing, and as a result of combined legislative, executive, and judicial decisions, the FISA wall came down. For the first time, federal prosecutors and law enforcement were explicitly permitted under law to participate in intelligence investigations.

- Our government also made other sweeping efforts to integrate its national security elements. Congress created a Director of National Intelligence and a Department of Homeland Security. The national security elements of the FBI were merged into a new National Security Branch.

- But as the WMD Commission noted in its report, the changes at Justice were slower to come. And that absence of change, coupled with the critical role of lawyers in modern national security operations, highlighted the need for, as the WMD Commission put it, "thoughtful, innovative, and constructive legal guidance."

- As information flowed more freely in a post-9/11 world, it became even more important for lawyers to have a seat at the table, both to ensure adherence to new and changing legal requirements and to facilitate consideration of all legally available options.

- As a result, in 2006, Congress created NSD to ensure unity of purpose among intelligence professionals, on the one hand, and prosecutors and law enforcement, on the other. Before that time, intelligence attorneys were in an entirely separate division of Justice, walled off from counterterrorism and counterespionage prosecutors. Today, however, NSD brings the Department's national security elements together to carry out the Department's highest priority: to combat terrorism and other threats to national security.

- Over the years, the number and prominence of legal questions dealing with national security has grown significantly. This raises an important question: Where does a "new" Division like NSD fit in?

- Coordination and integration represent a significant part of the answer. Lawyers who are *part* of the mission they serve are better at their jobs. We are more attuned to operational realities and better versed in the field. Quite simply, we are more relevant. Legal decision-making becomes a part of operational planning rather than an afterthought. But to do so successfully requires coordination and integration.

- At NSD, we cannot stand by and wait for legal questions to be brought to us, or to provide advice on operational decisions that have already been made; we must be present at the beginning and throughout. It is standard procedure now for agents planning and conducting national security investigations to consult throughout the process with NSD to

ensure that all potential avenues for disruption, intelligence gathering, investigation, and prosecution are preserved.

- Lawyers in our Office of Intelligence work day-in and day-out with the Intelligence Community to secure authorities under FISA from the FISC, and conduct oversight of intelligence activities. These same attorneys also work closely with our prosecutors to ensure that foreign intelligence obtained from FISA can be used to bring terrorists and spies to justice, while safeguarding national security information.

- Likewise, our Office of Law and Policy plays an important role in ensuring that operators have the authorities they need to keep the country safe and to oversee the development and implementation of policies on critical national security matters.

- And this is just a sampling of what we do. From the work of all of these offices, to our efforts to examine foreign investments in the United States, to providing services to victims of overseas terrorism, NSD takes a holistic approach to security, which is necessary in light of the gravity of the threats we face.

Evolution of Terrorism

- The changing nature of those threats demands a balanced approach that makes use of every tool in our arsenal—including military operations, intelligence operations, prosecution in federal court, the use of military tribunals, and collaboration with our partners around the world to confront common enemies.

- It is important that we remain nimble and flexible – because as we have all seen, over the past decade terrorism is increasingly diverse and decentralized. As we make progress against core al Qaeda, and as the cadre of al Qaeda affiliates around the globe continues to grow, terrorists have turned to a wider range of tactics. As we adapt, they adapt.

- And in the wake of the horrific Boston Marathon Bombings, the threat posed by homegrown violent extremism is now in stark relief.

- But this threat was a focus of our efforts and a growing area of concern since well before the Boston attacks. And we continue to evolve to meet it. In Boston, we quickly coordinated across the government to respond, bringing together intelligence lawyers, prosecutors, and analysts, and drawing upon all of the integration developed in the post-9/11 model. NSD worked closely with the FBI, and other agencies, to provide on-the-ground and around-the-clock support as the investigation unfolded.

Cyber Threat

- Another shift in the threat landscape that bears emphasis is the growth of cyber threats to the national security. The President calls the cyber threat "one of the most serious economic and national security challenges we face as a nation." Hardly a day goes by when cyber events don't show up in the news.

- We keep valuable date on networks so that is where the spies and the terrorists will go. And General Keith Alexander, Director of the National Security Agency (NSA), has said that cyber intrusions have resulted in "the greatest transfer of wealth in history."

- We often think of national security threats, like that of a catastrophic terrorist attack, as questions about prevention. But given the exploitations that have occurred and continue to occur, we cannot focus our efforts on prevention alone; the threat is here, present and growing. We must focus on disruption.

- The Department of Justice has a long history of success in investigating and prosecuting cyber crime – the Criminal Division's Computer Crime and Intellectual Property Section, and U.S. Attorneys' Offices across the nation have strong enforcement programs.

- But over the past two years, we have combined the lessons learned from the Department's cyber enforcement programs with the lessons learned in the post-9/11 counterterrorism arena. We must use an all-tools approach, including investigation and prosecution, against a broad range of cyber threats, including cyber thefts of sensitive information that could be used to harm us, economic espionage, and cyber attacks.

- In particular, NSD put in place structures both within the Division and in the field to deal with cyber threats to the national security – such as cyber-based terrorism and state-sponsored cyber intrusions.

- Last year we established the National Security Cyber Specialists' Network (NSCS), with members from across components of Main Justice, and from each and every U.S. Attorney's Office. We hosted extensive training for these network members and for all of NSD, to ensure we have the skills we need to tackle the threat.

- We've been working closely with the FBI's National Cyber Investigative Joint Task Force (NCIJTF) to assess cyber issues in real time as they arise.

- And we've launched a 24/7 cyber response capacity, and now have dozens of open matters related to cyber threats to the national security. We have aimed to become a one-stop shop and resource for cyber matters across the country.

- We have drawn from the current experience and expertise of our counterespionage and counterterrorism prosecutors, as well as those in our export control enforcement program, but we are also building new capabilities in other areas of law to ensure that we are well positioned to meet the changing threat. An "all-tools" approach means we need to be prepared not only to prosecute cyber intrusions, economic espionage, and export control violations, but also to explore a wealth of other civil and regulatory laws that are violated by these activities.

- But we can't do it alone - our "all tools" approach includes integration with operational and legal experts in the private sector.

- As Director Mueller says, there are only two types of companies -- those that have been hacked and those that will be. NSD would like to help our private sector partners to be ready for what may happen to them in the near future. Private companies will have to form the first line of defense, and their legal teams must be prepared to face difficult questions and complex matters as far ranging as:

    - responding to cyber breach investigations;
    - complying with the SEC's guidance on cyber security;
    - understanding the new cyber Executive Order;
    - advising Directors on their oversight role; and
    - staying on top of the evolving "standard of care" for cyber security.

- All of us – lawyers in the public and private sectors – will need to cooperate closely. We know that success requires reporting from, and close relationships with, victims. We've already met with a number of private entities and received a positive response, and we will continue these meetings to keep the dialogue going.

- We believe that there are criminal cases to be brought against these actors, and we are committed to using law enforcement tools to disrupt our adversaries' activities and prevent damage to U.S. national interests—just as we do in the counterterrorism and counterespionage arenas.

Modern Day

- All of these significant changes in the nature of the national security threat, the legal architecture, and the way the government is organized—are essential to understanding lawyers' unique roles in intelligence collection activities, including those that are the subject of recent media reports.

- As you know, protecting the United States requires intelligence about plots and threats *before* they happen, and we face a very different threat picture today than we did a decade ago.

- This reality means that we must adapt our intelligence practices to stay ahead of the enemy, and we must continue to keep certain sensitive intelligence activities outside the public sphere, to protect our safety and national security.

- Indeed, that is the central premise of the legal and oversight system FISA created 35 years ago, to ensure that all of these critical operations are conducted within the bounds of the law and consistent with our nation's values.

- Our nation's intelligence and national security professionals are committed to this balance, and I am proud that lawyers in particular play an important role in striking it. Ours is a very special responsibility.

- We follow the law where it takes us and sometimes that means our answer will be "no."

- And even more importantly, when it's yes, we have the responsibility of helping other national security professionals take the steps needed to protect the nation while simultaneously protecting the rights, values, and liberties that are so important to all of us.

- We take the initiative to look for ways to do what *can* be done, and to do it lawfully, providing safeguards for privacy without sacrificing operational efficiency and effectiveness. In other words – we look for the win-win.

- There is good reason behind the extensive oversight of our nation's intelligence efforts. Intelligence authorities reflect a careful balancing of national security imperatives with privacy and civil liberties. Collection must be broad enough to allow us to connect the dots and unearth terrorist plots before they can be realized, but it must also be bounded by a system of checks and balances that involve the FISC, the Executive Branch, and Congress.

    - Even more so in the post-9/11 environment, it is essential that the FISC provides independent judicial authorization and oversight of these activities. Its judgment ensures that we can all be confident that these sensitive operations are conducted in accordance with strict legal requirements, and consistent with the rule of law.

    - Congress also plays a critical oversight role. Even as there remains a need—as there has been throughout our history—for some of the details of our sensitive intelligence activities to remain classified, we must work diligently to ensure that our elected representatives in Congress remain informed about our intelligence collection authorities and how they are used.

    - And finally, oversight is highly valued within the Executive Branch. We at NSD have our own oversight section, and we work with our partners in the intelligence community, who conduct oversight - including through Inspectors General - and who have designed strong internal compliance programs with the strong support of Congress.

- These extensive oversight programs and strict legal requirements depend in part upon lawyers to ensure that the law is followed and that the protections for U.S. persons are enforced. Even for persons outside the United States, our legal architecture provides protections comparable to, if not greater than, those used by our foreign partners. A recent study comparing U.S. law to that of other countries found that the FISA Amendments Act "imposes at least as much, if not more, due process and oversight on foreign intelligence surveillance than other countries"—including those in the European Union"—"[would] afford in similar circumstances."[1] That same study also found that as

[1] [Hogan Lovells White Paper, "Sober Look at National Security Access to Data in the Cloud," *available at: http://www.hldataprotection.com/files/2013/05/A-Sober-Look-at-National-Security-Access-to-Data-in-the-Cloud.pdf*]

compared to many of our allies, the "U.S. is much more transparent about its procedures and requires more due process protections in investigations involving national security, terrorists, and foreign intelligence."

- Through rigorous oversight from every Branch, the Government can evaluate whether changes are needed to relevant procedures or guidelines, and what other steps may be appropriate to safeguard the privacy of personal information. This approach is designed to ensure that we are ever mindful of the careful balance between privacy and security.

Looking Ahead

- So in summary, the threats we face have changed, but so have we.

- To keep pace with the changing threat, we must use an intelligence-led, threat-driven approach – undergirded by info sharing – to identify priorities and threats and place appropriate resources against them.

- We need to employ all available legal resources for continued success against the evolving threat from terrorists, malicious cyber actors, and other criminal enterprises.

- But we also need to ensure that these resources are subject to strict oversight within the Executive Branch and by Congress so that the integration and information-sharing that is necessary to protect our safety also protects our privacy and civil liberties.

- As lawyers, we will continue to contribute to both sides of that balance, and I hope that through our efforts, this nation will be safe from harm.

- Thank you.