STATEMENT OF AMBASSADOR PATRICK KENNEDY
UNDER SECRETARY FOR MANAGEMENT
U.S. DEPARTMENT OF STATE
Before the Senate Committee on
Homeland Security and Governmental Affairs
"Information Sharing in the Era of WikiLeaks:
Balancing Security and Collaboration"
March 10, 2011

Chairman Lieberman, Ranking Member Collins, Members of the Committee, good afternoon and thank you for this opportunity to appear before you today to address the status of information sharing in light of the WikiLeaks disclosures, and in particular to discuss efforts within the executive branch both to improve the security of its systems, and to ensure that information is shared effectively and in a manner that continues to advance national security objectives. The Department of State and our interagency partners here today have long been closely engaged in achieving the dual objectives of appropriate information-sharing and protection, and in light of the WikiLeaks compromises, we are working together with renewed attention on achieving these dual objectives.

As you may be aware, I bring a rather unique perspective to the challenges of sharing and protecting information. I have served most of my career at the State Department -- overseas, at the United States Mission to the United Nations and here in Washington, and I was also honored to serve as the first Deputy Director of

National Intelligence for Management at the creation of the Office of the Director of National Intelligence (ODNI). Given this experience, I especially appreciate the commitment of this Committee to work with us in addressing the challenges of information security and sharing. Despite events of the past eight months, I want to assure Members of this Committee at the outset that we at the State Department maintain our commitment to fully share our diplomatic reporting on which our interagency partners rely. Our collective challenge is to do so in a manner that provides safeguards and protections that are reasonable, pragmatic, and responsible, not to stop sharing.

The focus of my testimony this afternoon is threefold: first, to explain briefly the Department's unique role within the executive branch as a source of diplomatic reporting that is essential to a variety of different agencies; second, to provide an overview of the State Department's mitigation efforts; and finally, to highlight the challenges as we move forward to share and protect our classified information.

Role of Diplomatic Reporting

The State Department has historically accomplished basic communication between Washington and overseas posts through the use of diplomatic telegrams or cables. These communications serve as the vehicle for our internal deliberations

relating to all aspects of our foreign relations and include candid assessments of conditions overseas and of diplomatic instructions that are vital to national-level decision-making. This formal channel between Washington and our overseas posts provides the Department and other U.S. Government agencies crucial information about the context in which we collectively advance our national interests on a variety of issues. For example, these communications may contain information about promoting American export opportunities, protecting American citizens overseas, and supporting military operations. We consider this reporting from posts around the world to be one of our most valuable contributions to every facet of national security, and we share this diplomatic reporting through automatic dissemination to over 65 agencies based on profiled requirements these agencies provide to the Department. Recent events have not changed our commitment to sharing this vital information.

WikiLeaks Disclosures and State Department Mitigation Actions

July 2010

When DoD material was leaked in July 2010, we worked with DoD to identify any alleged State Department material that was in WikiLeaks' possession. We immediately asked Chiefs of Mission at affected posts to review any purported State material in the release and provide an assessment, as well as a summary of

the overall effect the WikiLeaks release could have on relations with the host country.

Following the completion of the review in August, when it was believed that purported State cables might be released, the State Department instructed all Chiefs of Missions to familiarize themselves with the content in the Net Centric Diplomacy (NCD) database should a release actually occur.

November 2010

When the press and WikiLeaks announced that they were going to release purported State cables starting on November 28, 2010, the State Department took the following immediate actions: 1) Established a 24/7 WikiLeaks Working Group composed of senior officials from throughout the Department, notably our regional bureaus; 2) Created a group to review potential risks to individuals; and 3) Suspended SIPRNet access to NCD (SIPRNet is a DOD network).

The Department also created a Mitigation Team to address the policy, legal, security, counterintelligence, and information assurance issues presented by the release of these documents. During this period, the Department kept Congress apprised of both the international fallout caused by the WikiLeaks' disclosure and the steps undertaken to mitigate them. The Department convened two separate briefings for members of both the House of Representatives and the Senate within

days (December 2, 2010) of the first disclosure by WikiLeaks and appeared twice before the House Permanent Select Committee on Intelligence (December 7 and 9, 2010).

Ongoing Mitigation Efforts

State continues its thorough review of policies and procedures related to information security to ensure that they fully meet the current challenges. Efforts are being coordinated throughout the Department, as well as with the interagency, to ensure that we share classified information in an effective and secure manner with those who need it in their work to advance our national security.

- While the Department already had strong safeguards in place, we have further enhanced and updated our computer security policies that prohibit the downloading of classified information to removable media (e.g., thumb drives, CDs/DVDs) on the Department's classified network.
- The Department continues to deploy an automated tool that audits and monitors the Department's classified network to detect anomalies that would not otherwise be apparent. This capability is backed up by professional staff who promptly analyze detected anomalies to ensure that they do not represent threats to the system.

- The NCD database of diplomatic reporting and the State Department's classified web sites, although now inaccessible through SIPRNet, remains available via the more limited distribution Joint Worldwide Intelligence Communications System (JWICS). Throughout, the State Department has continued to share its diplomatic reporting among federal agencies through its traditional system of cable dissemination.
- To heighten awareness of what is and is not permitted when working on the Department's classified network and on classified systems, user awareness reminders are now available for Department employees on its classified network, in addition to the standard in-person briefings about handling classified material and a soon-to-be-released computer-based course on identifying and marking classified and sensitive information.

In addition, the Department is exploring solutions to improve how we share and protect information with those who are not direct recipients of our telegrams. One such solution would involve the creation of a website with a searchable database that would allow appropriately cleared personnel to use key word searches to discover relevant State cables; the search would reveal cable metadata, such as the subject line, but would not provide the full text of the cables in a potentially vulnerable database. This would ensure that cleared personnel are aware of cables they have an operational or strategic need to see. Cleared

personnel from other agencies would then be able to seek cables necessary for their work functions through their own organization's internal distribution system. The responsibility will be on the receiving, not the originating, agency to disseminate information to its internal personnel.

The Department has continued to work with the interagency on information management issues by participating in meetings of the new Interagency Policy Committee (IPC) chaired by the Special Advisor for Information Access and Security policy as well as existing IPCs such as the Information Sharing and Access IPC.

Challenges

The interagency is grappling with the complexities of three main challenges in the aftermath of WikiLeaks.

The first main challenge is ensuring information sharing policies are consistently directing the use of technology to solve problems, not the other way around. The post-9/11 mindset was focused on providing technical solutions to information sharing problems. As a result, technical experts were asked to develop solutions to the barriers inhibiting information sharing. The post-WikiLeaks environment reminds us that technology is a tool to execute solutions but is not in

itself the answer. Simply put, we must more consistently sort out what we share before determining how we share it. Connecting systems and networks may provide the means to share information, but we must still manage and share the content in the most appropriate way.

Mr. Chairman, the national security community must do a better job of articulating what information is appropriate to share with the widest appropriate distribution, and what is more appropriately confined to a narrower audience, in order to ensure adequate safeguards. The State Department believes that the way in which we share cables through our traditional means of dissemination and the steps we have taken already since November are leading us firmly in this direction.

The second main challenge involves each agency's rigorous adherence to existing, or improved, information security policies. This includes improved training of cable drafters in the use of labels to indicate appropriate breadth of dissemination based on the sensitivity of a cable's content. The executive order on classified information (E.O. 13526) establishes the basic levels of classification within the Executive Branch. From that foundation, individual agencies may still have their own captions that denote how information should be disseminated because not all cleared personnel need to see every diverse piece of classified information. Agencies that receive information need to understand how to handle

that captioned information, so that it is not inappropriately made available to a wide audience, which would undermine the intent of the captions.

The Office of Management and Budget (OMB) directed agencies to create teams to address security, counterintelligence, and information assurance issues. We believe that the State Department's Mitigation Team serves as a model for broad, cross-discipline coordination, or governance, because it brings together various subject matter experts from different fields to address information sharing and security issues in a coordinated manner. Many information sharing and security issues can be resolved at the agency level as long as there are standards in place for agencies to execute. For the most part, standards have been created by existing interagency bodies, but there are some areas where further coordination is needed.

The third main challenge involves the coordination, or governance, of information management in the interagency community. Numerous interagency groups are wrestling with issues related to the technological aspects of information sharing, such as those dealing with data standards, systems, and networks. Others are wrestling with the policy decisions of who should have access to what classified information. New interagency governance structures to coordinate information sharing have been developed, including those focused on sharing with state, local, and tribal governments, as well as with foreign partners. In keeping

with the first main challenge, these new structures should maintain or increase their focus on defining the content to be shared and protected as well as on the technology by which it is shared and protected. Each agency must be confident that security processes and procedures are applied in a uniform and consistent manner in other organizations. In addition, it must be understood that material originating in one agency will be treated by other agencies in accordance with mutually understood handling instructions.

The State Department shares information with the intent of providing the right information to the right people at the right time. We will continue to share this reporting appropriately so that we can continue our diplomatic mission as well as our role in the national security community. We recognize the imperative to make diplomatic reporting and analysis available appropriately with the interagency community. We continue to review how our information is disseminated at other agencies.

Conclusion

To recap, the State Department has long been, and remains, committed to both appropriately sharing and protecting information critical to our national security. This commitment requires ongoing efforts to confront multiple, complex challenges associated with information sharing. First, national security agencies must consistently put policies about content ahead of technological solutions.

Second, each agency must manage the sharing and protecting of information it originates and receives. Third, the interagency as a whole must continue to coordinate better to improve all facets of information sharing.

Thank you for this opportunity to appear here today. I look forward to working with the Committee on the challenges of sharing and protecting diplomatic and other sensitive information, and would be pleased to respond to any questions you may have.