Remarks for Christopher Painter
Coordinator for Cyber Issues, U.S. Department of State

INTER-AMERICAN COMMITTEE AGAINST TERRORISM (CICTE)
SIXTEENTH REGULAR SESSION
25-26 February 2016
Washington, D.C

Background: The Sixteenth Regular Session of the Inter-American Committee Against Terrorism (CICTE) will focus on three themes that Chile, the incoming CICTE Chair, selected: 1) Use of the Internet for Terrorist and Criminal Purposes; 2) Cybersecurity: Critical Considerations for the Development of the Economy and a Digital Society; and 3) Confidence Building Measures in Cyberspace. In 2015, the CICTE Secretariat conducted 62 activities, training courses, and technical assistance missions that benefited more than 3687 participants in five thematic areas including cybersecurity. The United States is a major contributor to CICTE's training programs and has provided funding and expert trainers for capacity building programs focused on aviation security, travel document security and fraud prevention, cybersecurity, legislative assistance and counterterrorism financing, supply chain security, and Customs and Immigration.

Remarks/Notes:

- I would like to begin by thanking the Organization of American States (OAS) and the Inter-American Committee Against Terrorism (CICTE) for organizing this meeting and for your continued recognition of the importance of cyber policy, particularly cybersecurity as a top priority for our region.

- We are all increasingly dependent on networked information systems for the daily functioning of our societies. With that dependency has come increasing concern about new and existing vulnerabilities, the exploitation of which can make individuals targets of criminal actors operating on the Internet, and can now affect whole populations through threats to cyber- enabled infrastructures.

- We all face increasing risks from state and non-state actors that conduct malicious cyber activity for unacceptable ends, including stealing trade secrets or personal information for commercial or financial gain, interfering with the exercise of freedom of expression, and intentionally damaging or even destroying critical infrastructure. These threats can range from everyday email spam, to serious

transnational criminal behavior, to activity that could constitute a threat to national security.

- As the U.S. Director of National Intelligence recently noted, the "likelihood of a catastrophic attack from any particular actor is remote at this time," we are likely to see "an ongoing series of low-to-moderate level cyber attacks from a variety of sources" that will, over time, "impose costs on U.S. economic competitiveness and national security." Given the global, interconnected nature of cyberspace and infrastructure, these threats and potential costs are not unique to the United States but are relevant and should be of concern to the international community as a whole.

- These issues are being addressed in a wide variety of venues, including technical standards groups and other multistakeholder organizations looking at how to strengthen the security of the Internet's architecture. We proceed from the perspective that the Internet and its associated networks are neither owned nor controlled by States. Rather than trying to regulate or control it, we view the role of states as one of many stewards - that is, caretakers, who work with all other stakeholders to ensure that this resource is available to all to reap positive benefits and rewards. This inclusive concept forms the basis for the multi stakeholder process and reflects the reality of how the Internet functions today.

- As one of these stewards, States must recognize our role(s) and focus our work on potential "value-add" contributions. In that respect, we recognize that States do have a well-established and important role to play with regard to facilitating transnational cooperation – including law enforcement cooperation – and seeking to prevent conflict and promote international stability. This role extends to the security of networked information systems.

- The challenge that we face as policy makers and practitioners is how to aggressively investigate, disrupt, and deter malicious activity online, including criminal and terrorist activity, while preserving the characteristics of the Internet that make it so vital to modern society.

- Our region has been leading the charge in navigating challenges in cyberspace since 2002. That was when we first came together as OAS member states to acknowledge that the benefits of information technology won't be fully realized if the security and reliability of these systems are threatened. We agreed that we must find ways to ensure security and stability in cyberspace while protecting

fundamental freedoms, creating opportunities for innovation, and promoting economic growth around the world.

- We concluded that no matter what steps individual states might take, national efforts, while necessary, are not themselves sufficient. Transnational cooperation is essential to our success on all fronts.

- That is why the United States has continued to support the OAS through CICTE, REMJA, and CITEL in building national cybersecurity strategies, developing new and stronger Computer Emergency Response Teams (CERTS), educating the public about cybersecurity and staying safe online, and training technicians, law enforcement, and policy makers about cybersecurity best practices specific to their fields of work. We were pleased to support OAS in hosting its first cyber security meeting in January 2004 in Buenos Aires, an initiative which led to development of a hemispheric strategy that has established OAS leadership in this emerging field.

- And I am proud to note the progress we have made in implementing that strategy, adapting to and confronting challenges in cyberspace—both longstanding and new, by relying heavily on the strength of our federal, state, local, and international partnerships. We have shown that there is immense value in working cooperatively with one another and other key stakeholders to protect our networks, share best practices, and communicate regarding threats, investigations and prosecutions.

- I would note that the themes of our discussion this year are indicative of that progress. In addition to expressing our continued support for the OAS's ongoing work on cybercrime and cybersecurity, I would like to take a few minutes today to encourage us to build on our past success. In particular, our work to address the numerous everyday challenges cyberspace presents could be augmented by new efforts to address the specific cyber challenges that could rise to the level of a national security concern.

- As cyber capabilities become more sophisticated, this concern is a growing possibility. Many states are developing military cyberspace capabilities—a prospect that is increasingly viewed as threatening both our national security and international security. In addition, key aspects of cyber tools—such as the difficulty of attributing an attack to its perpetrators or sponsors, and the dual-use

nature of the technology—are seen by many as inherently destabilizing.

- To address this concern, the United States has developed and is promoting a strategic framework of international cyber stability, designed to achieve and maintain a peaceful cyberspace environment where all states are able to fully realize its benefits, where there are advantages to cooperate against common threats and avoid conflict, and where there is little incentive for states to engage in disruptive behavior or to attack one another.

- There are three key elements to this framework: global affirmation of the applicability of international law to state behavior in cyberspace; the development of international consensus on additional norms and principles of responsible state behavior in cyberspace that apply during peacetime; and the development and implementation of practical confidence building measures that can help ensure stability in cyberspace during times of crisis.

- In recent years, we have had great success in building international consensus as states coalesce around this framework. As the 2016 CICTE Declaration notes, the 2013 and 2015 reports of the UN Group of Governmental Experts (GGE) indicated consensus that international law applies to state conduct in cyberspace, affirmed the applicability of international law and laid out norms of responsible state behavior in cyberspace.

- The relatively swift affirmation of these concepts by states is notable and likely driven by an increased understanding among leaders and senior policymakers of the challenges and opportunities cyberspace presents to national security and foreign policy.

- One component of this framework – the development of regional cyber confidence building measures – was also highlighted in this year's CICTE Declaration as a new potential area for practical regional work. We are pleased to see member states considering how CICTE can play a role in the development of such measures. CBMs have been used by the international community for decades to build confidence, reduce risk and increase transparency in other areas of transnational concern. Given the nature of cyberspace, CBMs can play a valuable role in building some confidence that normal operating behavior by states is somewhat predictable. Otherwise, activity in cyberspace could cause unintended reactions, miscalculation or misattribution - thus increasing risk of unintended conflict.

- The Organization for Security and Cooperation in Europe (OSCE) and ASEAN Regional Forum (ARF) have both been working on regional cyber CBMs and we have found the discussion very productive in those venues. In both venues, we are now at the stage of implementing specific regional cyber CBMs.

- It is our view that, taken together, peacetime norms of voluntary self-restraint and cooperation, coupled with existing international law and our work to pursue CBMs in cyberspace, will go a long way to achieving a more secure and stable cyberspace for everyone. If all states have an incentive to enjoy the benefits of cyberspace and little incentive to disrupt it, cyberspace can continue to be an engine for economic and social growth around the globe.

- Of course, affirmation of the applicability of international law and the development of additional, non-binding norms of responsible state behavior alone are not a silver bullet for all of the issues we face in cyberspace. We must also continue to address non-state threats and actors by developing better network security, cyber incident response capabilities, and enhancing international cooperation against cybercrime.

- We are doing that through, among other things, our capacity building efforts, including in building better cybersecurity and cybercrime capabilities and strengthening cooperation between and among technical computer response teams and law enforcement to deal with shared threats.

- I look forward to working with all of you to ensure that our region, working together and through the OAS, be it CICTE, REMJA, or CITEL, can continue to be a cohesive and progressive group.