

Remarks for Christopher Painter
Coordinator for Cyber Issues, U.S. Department of State
at
**“Promoting Inclusive Growth in the Digital Economy: The OECD Evidence
and Practice Base”**
U.S. Council for International Business Foundation/OECD/BIAC
March 10, 2015

Draft

- Thank you, Joe [Alhadeff], for your kind introduction. It’s a pleasure to be here today. I want to begin by thanking the United States Council for International Business (USCIB), the Organization for Economic Cooperation and Development (OECD), and the Business and Industry Advisory Committee (BIAC) to the OECD for holding this conference again this year. My office has been fortunate to work with you all for the last few years, and I am happy to join this discussion today.

- As the OECD gears up for its next Ministerial on the Digital Economy in 2016, it is a great time to reflect on the contributions that the OECD has made to the global conversation, and to prepare for its continued efforts. I have always felt strongly that the OECD can provide great value in providing evidence-based work on the contributions of the digital economy and, crucially, an open Internet, to economic growth and social prosperity.

And, it's clear I'm not alone as the membership and stakeholders have embraced the idea of "inclusive growth" as the theme for the Ministerial.

- As far as contributions to date, the OECD's work on the Internet Policy Making Principles, the security guidelines, the privacy guidelines, critical infrastructure protection and Computer Security Incident Response Team or CSIRT activity, and big data, among other efforts, have all made worthy contributions to the global discussions in these areas. Notably, the OECD's presence in various forums to discuss these complex issues, such as the Internet Governance Forum, the United Nations Educational, Scientific and Cultural Organization (UNESCO), NETmundial – the Global Multistakeholder Meeting on the Future of Internet Governance, the Organization of American States (OAS), and the Asia-Pacific Economic Cooperation Telecommunications and Information Working Group (APECTel), among others, I'm sure has been exceedingly helpful in furthering those discussions and providing content to them.
- My office has been particularly engaged in the current efforts to revise the security guidelines, and I commend the Secretariat for your deliberative process to arrive at what we believe is close to being finalized for the upcoming meeting in June. It has been a daunting task to translate the

guidelines as they were – a very important contribution to the discussion about network security, user awareness, and democratic values – to something even more profound on the impact of digital security risk management for economic and social prosperity.

- As we have engaged in the deliberations, we have noted that the work on the guidelines revision also tracks nicely with what the U.S. government is addressing in other ways. For example, the work our colleagues at the National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS) have done on the Cybersecurity Framework and its collaborative approach to the compilation and adoption of standards and best practices, not only for us in the United States but also with our partners globally. In addition, I’ve most recently returned from UNESCO’s “CONNECTing the Dots” conference in Paris where the multistakeholder community there was assessing how to address the confluence of security, privacy, human rights, access, and freedom of expression – aspects which the revised guidelines also embrace in important ways – while maintaining focus on how all stakeholders should assess and address their risk.
- Both industry participation as well as the other stakeholder groups’ engagement have been vital in bringing all the perspectives to the table. The

message to all stakeholders is a key component of the draft revision, so is, in our view the recommendation for a national strategy to address digital security risk. We have found over the years that a coordinated and consultative approach to our own national strategy development has been imperative to making it useful and actionable. In our bilateral, regional, and international engagements with partners, we always stress the need for a national strategy – one that reflects engagement with the private sector, civil society, and the technical community. We note that more and more countries are developing their strategies, and this recommendation, we attest, will help encourage even more to do so, and not just members of the OECD.

- We look forward to having that new iteration to add to the body of work for the 2016 Ministerial, certainly, but also to add to the body of work on Internet-related issues in many of these venues.
- In our remarks last year, we noted that 2014 and indeed 2015 represented busy years on Internet-related issues, and we are very much still in the midst of that flurry now: we completed a successful International Telecommunication Union (ITU) Plenipotentiary Conference last November; we are mid-stream on positive movement for Internet Assigned Numbers Authority or IANA transition and Internet Corporation for

Assigned Names and Numbers or ICANN accountability, continuing improvements to the IGF, preparations for important UN General Assembly meetings, including the conclusion of the ten-year review of the World Summit on the Information Society in a way that is contemplative rather than controversial and focuses on development and continued practical implementation of the WSIS outcomes – including continuing the mandate for the IGF.

- My office recently celebrated its fourth anniversary, and our cyber diplomacy efforts are very much reflected in the work of the OECD and related work streams elsewhere. Continuing to build an understanding of the economic benefits of the open, interoperable, secure, and reliable Internet, building a body of literature around it, and reinforcing connections to other work on trust and confidence are additional critical roles we would like to see the OECD undertake. We also encourage your continued engagement in other processes and events to help maintain traction in the global cyber dialogue. And we look forward to working with all of you in the stakeholder community to do that.
- Thank you. I look forward to your questions.