Comments on: DEPARTMENT OF COMMERCE National Telecommunications and Information Administration [Docket No. 150312253–5253–01] RIN 0660–XC018 Stakeholder Engagement on Cybersecurity in the Digital Ecosystem

Overall the list of cybersecurity issues presented is strong and represents many of the demonstrably hard problems we all face. At the Center for Internet Security, we strongly endorse, and act upon every day, the basic principles put forth by the IPTF request for comment: "*broad consensus, coordinated action, and the development of best practices*…". As an institution, we have significant experience in such approaches that cut across the entire SLTT Community, industry and government, international standards, etc. in issues ranging from fundamental technology to operational practice.

We would only add that the **development** of best practices is rarely the issue. Practices usually fail to achieve their potential due to a lack of: creation and sustainment of ongoing operational communities-of-practice to carry on such practices; the community-building needed to identify and remove barriers in common; and organization of the entire eco-system of participants, e.g., technologists, vendors, practitioners, policy-makers, educators, workforce organizers, and "enforcers" (auditors, Inspectors General, etc.). Therefore it would be useful to include as stakeholders any institutions which have a track record of taking practices and turning them into ongoing operational organizations or process, to complement stakeholders with a direct stake in the problem. For example, the Center for Internet Security established and operates an ongoing volunteer-staffed process to create and sustain the Critical Security Controls, a set of best practices driven by threat data, adopted voluntarily by countless institutions, and widely supported by Vendors. This illustrates the kind of sustained community-building activity needed to "Make Best Practice Common Practice".

Concerning the process, we suggest focusing initially on problems that have a relatively small number of key stakeholders, and where the technical issues are reasonably well understood. Excellent candidates are found in the Network and Infrastructure Security section of the RFP. All have a relatively small stakeholder community, and many technical ideas are already well established.

Concerning the topics, we think the initial list contains more than enough good starting projects, although one area not addressed is the national cybersecurity workforce issue.

Tony Sager
Senior Vice President, Chief Evangelist
Center for Internet Security
tony.sager@cisecurity.org
(www.cisecurity.org)