**Workshop on Cybersecurity Incentives (WoCI)**





***Workshop on Cybersecurity Incentives (WoCI)***

[**George Mason University**](http://www.gmu.edu/)**, Fairfax, VA**

**Mason Inn**

**June 16, 2011**

**Co-Chairs**

Daniel E. Arista, SRC (fka: Syracuse Research Corporation)

Timothy P. Clancy, J.D., George Mason University

**Objectives**

* Promote the prioritization of security in risk management decision making
* Improve the understanding institutional designs which create incentives for security
* Explore implementable cybersecurity governance mechanisms at the enterprise and national levels

**Background**

Improved risk management is central to improving cybersecurity at all levels. Managing risk involves making trade-off decisions or choices between 'valuables'. When resources are limited, trade-offs will call for a prioritization of objectives. In every organization, public and private, security must compete for priority with other operational objectives and imperatives. In the competition for scarce resources, security often loses out to more pressing or short-term needs. The reasons are varied including issues of individual and organizational risk perception and tolerance as well as misaligned or lack of incentives for security. Any serious attempt at resolving this issue immediately exposes the stark inadequacy of quantitative methods to measure risk as well as the scarcity of clear and functional processes to adjudicate what is reasonable risk taking in cyberspace. Tackling these issues requires an examination of the complexity of economic markets, social institutions, and technological infrastructure. Designing a politically and technologically feasible model that coordinates these elements into an acceptable balance is ultimately the challenge at hand.

**About the Workshop**

The Workshop on Cybersecurity Incentives (WoCI) will discuss the history, present, and future of societal mechanisms and institutional designs that leverage incentives to bring an acceptable balance between security and other priorities in cyberspace. The agenda will focus on illustrating cyberspace as an ecosystem of actors and discuss their roles and responsibilities, and the dynamics of their interaction and interconnectivity. Scholarship in law, economics and other fields within the behavioral sciences inform stakeholders about how markets, incentives and legal rules affect each other and shed light on determinations of liability and responsibility. This is considered essential to achieving efficient accountability and a sound public-private order in cyberspace. Considerations of what is technologically possible and feasible will be included. Ongoing debate and research in this area will be presented in practical terms allowing for participants to immediately realize implementable options for governing cybersecurity at the enterprise and national levels. The workshop will be composed of presentations and panel discussions covering the legal, economic, and technological facets of the topics presented.