Session – Testing/Risk

Title: **Cybersecurity in the Oil and Gas Industry – What's Here and What's Coming**

Author: **Aarushi Goel,** GoDaddy

Abstract

Cyber-attacks are increasingly targeting the O&G industry by myriad hackers: Trans-national terrorists for political reasons, cyber criminals for extortion by threatening attacks, and hacktivists for anti-energy policies. Because the critical infrastructure is a basis for our economic and national security, the U.S. government is generating new programs (i.e., the NIST Cyber Security Framework) and considering additional regulations. Current regulations are being re-interpreted under cyber security. The existing oil and gas industry is an increasingly technologically complex one. More and more processes are being digitized; data mining and analytical programs are being used more frequently, and sensors are everywhere. This may lead to more efficiency, but it also makes systems more vulnerable to cyber-attacks.

Security attacks in other industries can create disruption and monetary damages to businesses and individuals, but when security attacks compromise oil and gas industry SCADA systems and overtake their industrial control functions, the results can be disastrous — even deadly. If cyber hackers compromise the industrial control network running a pipeline, for example, they could adjust pipeline compressors to increase pressure until a weak point in the pipeline explodes. And all this can be done from anonymous, remote locations via the internet or other similar external communications pathways.

This presentation will justify the need for a cyber security architecture in Oil & Gas industry including the past/possible threats and the catastrophic impacts they may have on the industry. Lastly, this presentation will cover a specialized Oil & Gas NIST framework for effective implementation of security measures in current infrastructure in the form of standards, guidelines, and practices to promote the protection of critical infrastructure.