Cybersecurity for Cyber-Physical Systems Workshop
Call for Abstracts

On **April 23 and 24, 2012**, the NIST ITL Computer Security Division will host a two-day workshop to explore cybersecurity needed for cyber-physical systems[1], with a focus on research results and real-world deployment experiences. On the first day, speakers will address CPSs across multiple sectors of industry (e.g., automotive, aviation, healthcare). The second day will focus on cyber security needs of CPSs in the electric Smart Grid.

Extended abstracts should be submitted in IEEE conference format (available at http://www.ieee.org/conferences_events/conferences/publishing/templates.html). The expected length of the abstract is one (1) to two (2) pages. The maximum number of pages that will be considered is four (4). Abstracts should be submitted in either PDF or MS Word format. Extended abstracts will be accepted through **5pm Eastern time January 23, 2012**. Extended abstracts should be sent to cpscybersecurity@nist.gov.

Selected submitters will be chosen, based upon the extended abstracts submitted, to give a presentation at the Workshop. Submitters will be contacted by **February 6th** and notified of their status. Final slides for presentations should be submitted in PDF or PowerPoint format no later than **5pm Eastern time April 9th**.

All extended abstracts and slide sets should be free of copyright protection and proprietary information. Extended abstracts and slide sets from presenters will be published in a NIST Interagency Report as proceedings of the conference. As such, the material will be considered in the public domain. Summary conclusions and other findings will also be used in the updating of NISTIR 7628, *Guidelines for Smart Grid Cyber Security*.

Workshop goals include:

- Examining recent (2 – 3 years) research results and deployment experiences involving CPS in various industries. (e.g., healthcare, manufacturing, automotive, electric Smart Grid, etc.)
- Determining if there are security requirements that are unique to CPS, as opposed to strictly cyber or physical systems.

Submitters are encouraged to address the following issues and questions:

- Include a brief background on your area of CPS. Consider identifying the following:
  - Common threats, or a threat model, specific to a sector CPS;
  - Any known vulnerabilities, including how they are identified;
  - Potential impact(s) if the vulnerability is exploited;
  - Interface(s) between the cyber and the physical mechanisms;
  - Information/connection management mechanisms (internal and external to the system);
  - Protocols used to secure the information while at rest or in transit, including any standards used (sector-specific, or general);
  - Security requirements (management, operational, or technical) that are currently in place.
- What is new in the area of CPS cyber security in the last 2 -3 years in your area / industry?
- What types of security requirements might be needed in your CPS area that are unique to CPSs as opposed to systems that are strictly cyber or physical systems?
- Discuss any strategies for or successes with dealing with legacy equipment when gathering forensic data.
- Are there any privacy implications related to CPSs in your area / industry?
- What effect, if any, did or will malware like Stuxnet have in your particular area of CPSs?
- Any other issues deemed relevant for NIST, this workshop, and its participants.

[1] For the purposes of this workshop, cyber-physical systems (CPS) are smart systems that have cyber technologies – both hardware and software – embedded in them to (1) sense the current state of the system and the surrounding real world context in which the system must perform, and (2) respond to provide optimal performance.