Invitation to Attend:

NIST Workshop on Applying NIST Special Publication 800-53, Revision 1*: Recommended Security Controls for Federal Information systems,* to Industrial Control Systems. August 16 (1-5 PM) & August 17 (9-Noon), 2007 Marriott Knoxville Hotel Knoxville, TN

The National Institute of Standards & Technology (NIST) will host a workshop for representatives from national and international industrial control system (ICS) communities (e.g., electric, oil, gas, water, manufacturing) to share information, obtain direct inputs, and determine their level of interest in voluntarily adopting and using NIST's ICS augmentation of NIST Special Publication (SP) 800-53, Revision 1. Use of NIST's ICS augmentation of SP 800-53, Revision 1, which is mandatory for federally owned/operated ICS, specifies the minimum information security controls that must be implemented in an ICS based on its security impact categorization. The security impact categorization of an ICS is an indication of the maximum harm that can be done to the organization that owns/operates the ICS, to dependent organizations (i.e., other organizations that depend on the ICS-related services of the organization), and to critical infrastructures should there be a loss of confidentiality, integrity, and/or the availability in an organization's ICS.

NIST feels strongly that ICS information security standards that are adopted and used by private sector critical infrastructures should be at least as strong as those required to protect ICS owned/operated by the U.S. Government. Consequently, NIST is encouraging national and international voluntary ICS standards development organizations to:

- Work towards convergence to a common foundation of information security standards that apply to all ICS communities, and
- To consider the ICS augmentation of SP 800-53, Revision 1 as a candidate for the common foundation.

The meeting will include background information and discussion on:

- NIST's risk management framework (RMF) and NIST's supporting information system security standards and guidelines
- Federal agencies' experiences using NIST's RMF and standards and guidelines (including SP 800-53, Revision 1) in both general information systems and ICS
- NIST's ICS augmentation of SP 800-53, Revision 1
- Federal agencies experiences using NIST's ICS augmentation of SP 800-53, Revision 1

- Discussion on potential voluntary adoption and use of the ICS augmentation of SP 800-53, Revision 1 by the ICS-related voluntary standards community.

While there is no charge to attend the workshop, attendance may be limited by the size of the meeting room (on a first come, first serve basis). NIST will not be providing meals or other refreshment services during the workshop—attendees are expected to cover their own costs in these areas.

If you would be interested in attending, please send email to:

Stu Katzke at: skatzke@nist.gov or Keith Stouffer at: keith.stouffer@nist.gov

The draft workshop agenda is below.

Additional background and information:

Through NIST's assigned responsibility to develop and promulgate security standards for federal information systems, NIST's Information Technology Laboratory (ITL) Computer Security Division (CSD), and NIST's Manufacturing Engineering Laboratory (MEL) Intelligent Systems Division (ISD) partnered to establish an *Industrial Control System Security Project* to improve the information security of public and private sector ICS.

A key goal of this project is the development of information security requirements and baseline security controls for federally owned/operated ICS (including industrial/process controls systems that are operated by contractors on behalf of the federal government) that will significantly improve the information security of these types of systems. An additional desired goal is the voluntary adoption of the same or similar security requirements and baseline security controls by the private-sector ICS community. Adoption of common government and industry requirements and baseline security controls greatly reduce the vulnerability of critical infrastructure systems that are supported by ICS and they raise the security bar on all such systems.

In support of these goals, the NIST ICS Security Project is augmenting SP 800-53, Revision 1 to address ICS. SP 800-53, Revision 1, which was developed for traditional information systems, contains a security control catalogue (Appendix F) and mandatory information security requirements for all non-national security information and information systems that are owned, operated, or controlled by federal agencies (Appendices D and E). While most controls in SP 800-53, Revision 1 Appendix F are applicable to ICS as written, several controls do require ICS-specific augmentation by adding one or more of the following:

(i) ICS Supplemental Guidance
(ii) ICS Enhancements (one or more)
(iii) ICS Enhancement Supplemental Guidance.

When augmenting Appendix F of SP 800-53, Revision 1 to develop Appendix F ICS, the original set of controls, enhancements, and supplemental guidance contained in Appendix F were not changed. ICS Supplemental Guidance provides additional guidance on how to apply a SP 800-53, Revision 1 control in ICS environments. ICS Enhancements are enhancement augmentations to the controls that are required for some ICS. ICS Enhancement Supplemental Guidance provides guidance on how to apply an enhancement in ICS environments.

At this time, Appendices F and I have been released for public comment (public comment period closes August 31, 2007). Modifications to Appendices D and E, the mandatory information security requirements for ICS, are still under development. They will be released for public comment when a mature draft is completed.

DRAFT AGENDA

NIST Workshop on Applying NIST Special Publication 800-53, Revision 1*: Recommended Security Controls for Federal Information systems,* to Industrial Control Systems. August 16 (1-5 PM) & August 17 (9-Noon), 2007 Marriott Knoxville Hotel Knoxville, TN

August 16 (1-5 PM)

1:00 Introduction to NIST's Risk Management Framework (RMF) and related standards and guidelines, including NIST Special Publication (SP) 800-53, Revision 1.
- History, status, public review process
- Primer on the RMF and SP 800-53, Revision 1
- Effort to harmonize with ISO/IEC 27000 series documents

1:30 Federal agencies' experiences in applying the RMF and related standards and guidelines to general information system (i.e., non-ICS environments)

2:00 Federal agencies' experiences in applying the RMF and related standards and guidelines to ICS

2:30 Introduction to NIST's SP 800-82: *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security* and the ICS augmentation of NIST Special Publication (SP) 800-53, Revision 1
- History of SP 800-82 and the ICS augmentation of NIST Special Publication (SP) 800-53, Revision 1
- Process for developing and reviewing ICS-related documents
- Status of the documents

3:00 Federal agencies' experiences in applying the ICS augmentation of NIST Special Publication (SP) 800-53, Revision 1

3:30 Private sector practice and experience with ICS cyber security

4:00 Discussion on ICS standards convergence/harmonization
- Motivation: importance of convergence, diversity is not good
- Stakeholders & communities
- Role of NERC CIPs

Breakout discussions: Whether and how to achieve convergence (Part 1)
Questions to Guide Breakout Groups:
- Do you think that convergence of standards is important?
- Based on prior knowledge and what you heard here, are the NIST RMF and the ICS augmentation of SP 800-53, Revision 1 a good basis for convergence?
- What issues need to be discussed at this workshop?

4:45 Status reports from breakout groups
- Determining next day's agenda (based in part on the status reports)

5:00 Adjourn for day

August 17 (9-Noon), 2007

9:00 Continue breakout discussions: Whether and how to achieve convergence (Part 2)
11:00 Reports on breakout sessions
11:30 Next steps
12:00 Adjourn