Comments on the FERC Staff Preliminary Assessment of the NERC Proposed Mandatory Reliability Standards on Critical Infrastructure Protection issued December 11, 2006 Docket RM06-22-000
February 6, 2007

By

Stuart W. Katzke, Ph.D.
Senior Research Scientist
National Institute of Standards and Technology
100 Bureau Drive; Stop 8930
Gaithersburg, MD 20899
skatzke@nist.gov
(301) 975-4768

And

Keith Stouffer
Senior Mechanical Engineer
National Institute of Standards and Technology
100 Bureau Drive; Stop 8230
Gaithersburg, MD 20899
keith.stouffer@nist.gov
(301) 975-3877

These comments are in response to your solicitation for comments on the *Federal Energy Regulatory Commission (FERC) Staff Preliminary Assessment of the North American Electric Reliability Corporation's (NERC) Proposed Mandatory Reliability Standards on Critical Infrastructure Protection* (hereafter referred to as the "***NERC CIPs***").

We feel you have done an excellent job analyzing the NERC CIPs and their adequacy for protecting components of the U.S. bulk electric system from cyber and other information technology-related attacks (hereafter referred to as "***cyber attacks***"). Our assessment is that the NERC CIPs do not provide levels of protection commensurate with the mandatory minimum federal standards (FIPS) prescribed by NIST (in FIPS 200 and NIST Special Publication 800-53, Revision 1 (hereafter referred to as ***SP 800-53***)) for protecting federal non-national security information and information systems, including industrial control systems (ICS), from cyber attacks. As you know, ICSs are pervasive through the bulk electric system, as well as all other critical infrastructures. Since there are federal agencies that operate and/or have control over the operation of ICSs that support the bulk electric system, these agencies must meet NIST standards and guidelines as well as standards required by FERC for these ICSs. To assist these agencies, NIST is developing an interpretation of SP 800-53 that is specific to ICSs. The ICS interpretation will be available in 2007 for use by federal agencies in demonstrating their (partial) compliance with the Federal Information Security Management Act of 2002 (FISMA).

The ICS interpretation of SP 800-53 will be available for use by the private sector on a voluntary basis.

Our recommendation is for FERC to consider issuing interim cyber security standards for the bulk electric system that:

- Are a derivative of the NERC CIPs (e.g., NERC CIPs; NERC CIPs appropriately modified, enhanced, or strengthened), and
- Would allow for planned transition (say in two to three years) to cyber security standards that are identical to, consistent with or based on SP 800-53 and related NIST standards and guidelines (as interpreted for ICSs). This will be a plan to strengthen the NERC CIPs, rather than a plan to abandon them.

Our recommendation is based on the following reasons:

- The management, operational, and technical controls specified in the NERC CIPs are a proper subset of the moderate baseline control set contained in SP 800-53. As a participant of the Industrial Process Control System Workshop held at NIST April 19-20, 2006, FERC received a copy of a draft report on January 24, 2007, which supports this statement.
- Using SP 800-53 will result in better protection against cyber attacks on bulk electric information systems owned and/or operated by both federal and private sector organizations as SP 800-53 requires the implementation of stronger and more comprehensive sets of controls.
- After the transition to an ICS interpretation of SP 800-53:
    - Federal ICSs within the bulk electric system will only have to comply with one set of standards—the ICS interpretation of SP 800-53.
    - Federal agencies that operate/control both ICSs and other types of information systems will be required to comply with a consistent set of controls for all of their information systems (i.e., SP 800-53 for general information systems & the ICS interpretation of the SP 800-53 for their ICSs).
- Since the NERC CIPs are a proper subset of SP 800-53, implementation of the interim standard would be fully consistent with the planned transition to the ICS interpretation of SP 800-53.
- Since the FERC staff comments address interdependencies between electric and other industrial facilities, SP 800-53 could provide a common basis for security protection for all industries. In fact, organizations in other sectors have expressed an interest in applying NIST 800-53 (e.g.; in the chemical sector)

The background and rationale for the recommendations above are contained in Attachment A.

We appreciate the opportunity to share our views with FERC and will be happy to share interim and final drafts of the ICS interpretation of SP 800-53 with FERC as they are developed. We invite FERC to participate in the development of the ICS interpretation

of SP 800-53 that could be used by both public and private entities in the electric power sector.

ATTACHMENT A

BACKGROUND AND RATIONALE FOR THE RECOMMENDATIONS

BACKGROUND

FISMA required NIST to develop two mandatory Federal Information Processing Standards (FIPS) that apply to all federal information and information systems, including industrial control systems (ICSs). These standards are: (i) FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*; and (ii) FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. FIPS 199 is a standard for determining the security category of an information system. FIPS 199 security categories (low, moderate, and high) are based on the potential impact on an organization should certain events occur which jeopardize the information and information system needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. The organization's impact analysis must also consider the potential impact on other organizations (i.e., dependencies). FIPS 200 is a standard that specifies mandatory minimum security requirements all federal information systems must meet, including ICS.

To support both FIPS 199 and 200, NIST developed Special Publication (SP) 800-53, Revision 1 (hereafter referred to as ***SP 800-53***). SP 800-53 requires federal agencies to implement one of three minimum (baseline) sets of security controls for every information system in the agency based on the systems' security categorization.

While FIPS 199, FIPS 200, and SP 800-53 are intended to apply to the majority of the government's information systems, these standards and guidelines (S&Gs) were developed with the recognition that an interpretation of the SP 800-53 security controls would have to be developed for the federal ICS community for various reasons (e.g., sector-specific laws/regulations/policies, sector-specific technologies, sector-specific application/performance requirements.) As a proof of concept that FIPS 199, FIPS 200, and SP 800-53 can be interpreted and applied to the ICS sector, NIST's Computer Security Division (CSD) and Intelligent Systems Division (ISD) initiated a joint Industrial Control System Security Project in January 2006. The objective of this project is to work cooperatively with federal and private sector stakeholders in the ICS area to craft an interpretation of the SP 800-53 security controls for ICSs. NIST understands that there are standards development efforts that overlap with SP 800-53 and other NIST SPs, such as the NERC CIP, ISA SP99 *Manufacturing and Control Systems Security* standard and the IEC 62443 *Security for Industrial Process Measurement and Control – Network and System Security* standard. In the long term, NIST plans to work within these efforts to create a unified standard for ICS security. A more detailed description of the *Industrial Control System Security Project* is contained in Attachment B.

RATIONALE

The recommendations are based on the following responsibilities, activities, and research:

- NIST's responsibility, as specified by FISMA, OMB, and other sources, for developing information security standards and guidelines for federal government non-national security systems, including ICSs.
- NIST's role and experience in providing technical assistance to DHS in the ICS area.
- NIST's collaborative research activities with DHS, DOE and the DOE labs (e.g., participation in research test beds).
- NIST's ICS internal research activities and test beds including areas such as manufacturing automation and SCADA systems.
- NIST's role as editor of ISA SP99 *Manufacturing and Control Systems Security Standard*, Part 2.
- The results of NIST's April 19-20, 2006 *Industrial process Control System Workshop.*
- Research results that compared the security controls in SP 800-53 to those contained in the NERC CIPs.
- Development of the master catalogue of security controls in SP 800-53 that was derived from many public and private sector sources, including: Common Criteria Part 2, ISO/IEC 17799, COBIT, GAO FISCAM, D/CID 6-3 Requirements, DOD Policy 8500, and BITS functional packages
- NIST's development of an interpretation of SP 800-53 specifically for ICSs. This interpretation will be completed in 2007.
- NIST's development of NIST SP 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*

The responsibilities, activities, and research described above have led to the following conclusions:

- The SP 800-53 control catalogue is a more complete and consistent set of security controls than the source security control sets SP 800-53 was derived from.
- The NERC CIPs are the only other available candidate cyber security control standards for the bulk electric system.
- The management, operational, and technical controls in the NERC CIPs are a subset of the moderate baseline set of controls in SP 800-53.
  - This subset may not be adequate for protecting critical national infrastructure, especially when considering interdependencies of the critical infrastructures.
  - The moderate baseline may not be adequate for all electric energy systems when the impact of regional and national power outages is considered.

- The interpretation of SP 800-53 specifically for ICSs will provide significantly stronger protection for the bulk electric information systems than the NERC CIPs.
- The interpretation of SP 800-53 specifically for ICSs will also be applicable to ICSs in other industry sectors. This, and the fact that they are also mandatory for federal ICSs, will make adoption by ISA and other standards organizations more likely. NIST has committed to exploring convergence of security standards with these standards organizations.
- Federal agencies that have both general information systems and ICSs want to comply with a single set of controls for their information systems and ICSs. The interpretation of SP 800-53 specifically for ICSs allows this possibility.

ATTACHMENT B

COMPUTER SECURITY DIVISION'S AND INTELLIGENT SYSTEMS DIVISION'S *INDUSTRIAL CONTROL SYSTEM (ICS) SECURITY PROJECT*

Key aspects of the *Industrial Control System (ICS) Security Project* include:

- Holding an invited *Industrial Process Control Systems Workshop*, April 19-20, 2006, to bring experts/stakeholders in the ICS community together to address how the government ICS stakeholders can work cooperatively to develop an ICS interpretation of the SP 800- 53 and a minimum baseline set of security controls for their government ICSs. A summary of the workshop can be found at: http://csrc.nist.gov/sec-cert/ics/ICS-Workshop-Meeting-Minutes-FINAL_14Nov06.pdf.

  The results/outcome of this workshop will significantly influence all of the following activities:

- Development of NIST Special Publication 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*
- Development of annotated mappings and gap analyses between SP 800-53 and the NERC CIPs to determine if/how SP 800-53, including the SP 800-53 minimum baseline sets of security controls, would need to be modified or interpreted for ICSs to fully meet the NERC CIPs.
- Development of an ICS interpretation of: a) The security controls contained in the SP 800-53 control catalogue, and b) The minimum baseline sets of security controls defined in SP 800-53 for moderate and high impact ICSs
- Develop the ICS interpretation of the minimum baseline sets of security controls defined in SP 800-53 (mentioned above) so that conformance to the ICS baselines will ensure conformance to the NERC CIPs.
- Continuation of NIST's industry and government outreach efforts and standards development activities.
- Development of a NIST near-term strategy for vetting the ICS interpretation of the SP 800-53, including the minimum baseline sets of security controls, within the government ICS community.
- Assuming convergence within the government community can be achieved. NIST will also develop a long-term strategy to facilitate convergence of government and private sector standards activities.