Appendix B

Standards Organizations

INFORMATION IN THIS CHAPTER

- North American Reliability Corporation (NERC)
- The United States Nuclear Regulatory Commission (NRC)
- United States Department of Homeland Security
- International Society of Automation (ISA)
- International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)

While a limited selection of regulatory standards and compliance controls have been discussed in Chapter 13, there are many additional controls that are either mandated or recommended by NERC, NRC, DHS, ISA, and the ISO/IEC. The following organizations provide useful resources, including access to the most recent versions of compliance standards documents.

NORTH AMERICAN RELIABILITY CORPORATION (NERC)

The North American Reliability Corporation is tasked by the Federal Energy Regulatory Commission (FERC) to ensure the reliability of the bulk power system in North America. NERC enforces several reliability standards, including the reliability standard for Critical Infrastructure Protection (NERC CIP). In addition to these standards, NERC publishes information, assessments, and trends concerning bulk power reliability, including research of reliability events as they occur.

The NERC CIP standards are comprised of nine standards documents, all of which are available from NERC's website at: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

THE UNITED STATES NUCLEAR REGULATORY COMMISSION (NRC)

The United States Nuclear Regulatory Commission is responsible for the safe use of radioactive materials, including nuclear power generation and medical applications of radiation. The NRC publishes standards and guidelines for Information Security, as well as general information and resources about nuclear materials and products, nuclear waste materials, and other concerns.

NRC TITLE 10 CFR 73.54

NRC Title 10 of the Code of Federal Regulations, Part 73.54 regulates the "Protection of digital computer and communication systems and networks" used in member Nuclear Facilities. More information on CFR 73.54 is available from NRC's website at: http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html.

NRC RG 5.71

The United States Nuclear Regulatory Commission's Regulatory Guide 5.71 offers guidance on how to protect digital computer and communication systems and networks. RG 5.71 is not a regulatory standard but rather a guidance on how to comply with the standard, which is Title 10 of the Code of Federal Regulations, Part 73.54. Information on RG 5.71 is available from NRC's website at: http://pbadupws.nrc.gov/docs/ML0903/ML090340159.pdf.

UNITED STATES DEPARTMENT OF HOMELAND SECURITY

The Department of Homeland Security's mission is to protect the United States from a variety of threats including (but not limited to) counter-terrorism and cyber security. One area where cyber security concerns and anti-terrorism overlap is in the protection of chemical facilities, which are regulated under the Chemical Facilities Anti-Terrorism Standards (CFATS). CFATS includes a wide range of security controls, which can be measured against a set of Risk-Based Performance Standards (RBPSs).

CHEMICAL FACILITIES ANTI-TERRORISM STANDARD (CFATS)

The Chemical Facility Anti-Terrorism Standards (CFATS) are published by the United States Department of Homeland Security, and they encompass many areas of chemical manufacturing, distribution, and use including cyber security concerns. More information on CFATS can be found on the DHS's website at: http://www.dhs.gov/risk-chemical-facility-anti-terrorism-standards-cfats.

CFATS RISK-BASED PERFORMANCE STANDARDS (RBPS)

The United States Department of Homeland Security also publishes recommendations in the form of Risk-Based Performance Standards for CFATS. These RBPS standards provide guidance for the compliance to the Chemical Facility Anti-Terrorism Standards. More information on the CFATS RBPS can be found on the DHS's website at: http://www.dhs.gov/xlibrary/assets/chemsec_cfats_riskbased_performance_standards.pdf.

INTERNATIONAL SOCIETY OF AUTOMATION (ISA)

The International Society of Automation (ISA) and the American National Standards Institute (ANSI) have developed a suite a standards addressing cyber security for ICS originally under the embrella of ISA-99, but renamed to ISA-62443. This naming change was the result of ISA's alignment with the global International Electrotechnical Commission (IEC) and the adoptation of the global IEC-62443 standards. The suite contains at the time of publishing of this book 13 standards.

Additional information on ISA-99/IEC-62443, including access to "draft" versions of standards that are currently in development, can be found at: http://isa99.isa.org/.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) AND INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC)

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) produced the ISO/IEC 27002 standard for "Information technology — Security techniques — Code of practice for information security management." While ISO/IEC 27002 does not apply exclusively to SCADA or industrial process control networks, it provides a useful basis for implementing security in industrial networks, and is also heavily referenced by a variety of international standards and guidelines.

More information on the ISO/IEC 27002 can be found on the ISO website at: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54533.

ISO also released in 2013 technical report TR27019 that provides guidance principles based on 27002 applied to ICS used in the energy sector, extending the 27000 series to include ICS as well as traditional IT information systems.

More information on the ISO/IEC TR27019 can be found on the ISO website at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43759.