NIST Standards Development Process

A Partnership Between Government and Industry

Keith Stouffer
National Institute of Standards and Technology

US Federal Standards and Guidelines

- Measurement standards
  - Length
  - Mass
  - Time
  - Ohm
  - Etc.

- Principle-based and prescriptive standards and guidelines
  - Federal Information Processing Standards (FIPS)
  - Special Publication (SP) 800 Series documents

- NIST does not perform enforcement – Government Accountability Office (GOA) and Inspector Generals (IGs)

Federal Information Standards (FIPS)

- Approved by the Secretary of Commerce
- Compulsory and binding standards for federal agencies non-national security information systems
- Voluntary adoption by federal national security community and private sector
- Examples
  - FIPS 140-2 Security Requirements for Cryptographic Modules
  - FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems

Special Publication (SP) 800 Series Documents

- Special Publications in the 800 series are documents of general interest to the computer security community, established in 1990
- Reports on guidance, research, and outreach efforts in computer security, and collaborative activities with industry, government, and academic organizations
- Documents receive 3 public vetting cycles before being finalized
  - Initial public draft - 90 day review period
  - 2nd public draft - 60 day review period
  - Final public draft - 30 day review period
- Agencies must follow 800 series guidance documents, but 800 series documents generally allow agencies latitude in their application
- Voluntary adoption by private sector – heavily used
- FIPS may mandate specific 800 series documents
  - FIPS 200 mandates NIST SP 800-53 security controls

NIST Approach to Standards Development

- NIST standards only apply to non-national security part of US government (USG)
- NSA standards apply to the national security part of the USG (i.e., classified systems, intelligence-related systems)
- Use of NIST standards is mandatory by government agencies; guidelines require mandatory “consideration”
- Use of NIST standards and guidelines is always voluntary by the commercial sector

NIST Approach to Standards Development

- In order of priority:
  - Adopt or adapt existing voluntary industry standards, if available and acceptable
  - Join voluntary industry standards efforts to develop common government-industry standards; adopt or adapt the completed standard for government use.
  - Use NIST mandated authority and internal resources to develop standards and guidelines for federal agencies

NIST Approach to Standards Development

- Seek heavy commercial sector involvement
- Attempt to develop “dual use” standards
  - Appropriate for use by government & industry
  - Contributions to voluntary standards groups (IEEE, ISO)
- Accept technical contributions from all parties
- Hold open workshops & public briefings
- Have open public comment periods
- Revisions based on public comments
- International coordination & cooperation
  - For example: Japan & India

Why This Approach?

- 90% of critical infrastructure (CI) is owned by the private sector
- All systems within a CI need appropriate, consistent, & comparable protection-should be seamless protection across government & private CI systems
- Government approach is to encourage private sector to strengthen its CI protection
- Private sector is more likely to adopt standards and guidelines if these are developed in an open consensus environment

Why This Approach?

- Product developers are more likely to implement/meet standards if developed in an open consensus environment (e.g., DES, AES, FIPS 140) due to larger market
- Results in larger selection of products for all sectors to chose from
- Results in best possible/stronger standards
  - Wide diversity of technical advice
  - Realistic view of what is technically feasible

Why This Approach?

- Often considered as “best practice” or “due diligence” by private sector
  - “Good enough for government is good enough for us”
  - Promoted through government CI sector liaisons to their CI counterparts
- Better interoperability between government & private sector systems
- Provides general public/citizens with visibility & comfort into how the government is protecting systems that contain personal/private information about them

Consensus-Building Process

NIST Special Publication 800-53

- Employ extensive vetting process for Special Publication 800-53
  - Three full published drafts of document
  - Three public comment periods to obtain feedback from the public and private sectors
- Carefully assess feedback received during the public comment periods; incorporate material into publication, as appropriate
- Provide sufficient time for organizations to become familiar with Special Publication 800-53 before transitioning to FIPS 200

Special Publication 800-53

- Formal and informal comments received from a wide variety of constituencies in the public and private sectors including—
  - Federal, State, and Local Governments
  - Critical Infrastructure Entities (e.g., power companies, telecommunications providers)
  - Fortune 500 Companies
  - Healthcare Providers
  - Financial Industry
  - Consortia (e.g., National Realtors Association)
  - Private citizens

Significant Comments

- Received over 800 comments on the initial public draft of Special Publication 800-53
- Comments indicated that—
  - ✓ Security controls contained too much implementation detail
  - ✓ Security control baselines (low, moderate, high) included too many controls for a minimum set
  - ✓ There was insufficient flexibility in the security control selection process for organizations to effectively apply the controls in specific operational environments
  - ✓ The “high-water mark” approach required organizations to employ unnecessary security controls

NIST Response

- In response to the initial public comments, NIST re-engineered Special Publication 800-53
- Fundamental changes included—
  - ✓ Streamlining the security control structure and control content to focus on “token-level” requirements
  - ✓ Redesigning the security control enhancement approach to facilitate ease-of-use for organizations requiring additional security controls based on risk assessment
  - ✓ Incorporating scoping guidance to help organizations effectively apply the NIST guidance in specific operational environments
  - ✓ Reducing the number of security controls in the control baselines

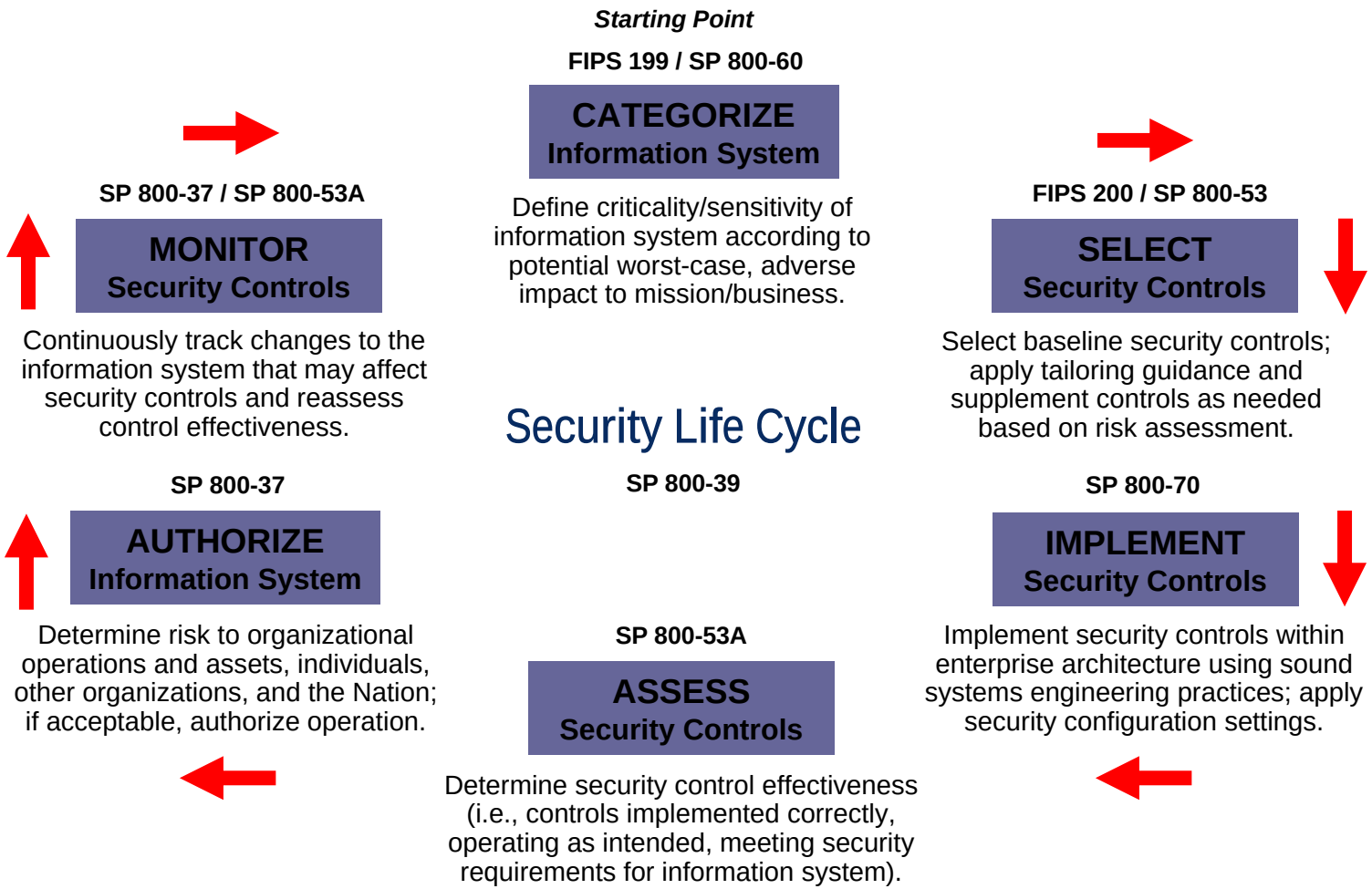
Key Milestones

- NIST Special Publication 800-53
  - Initial Public Draft **(October 2003)**
  - Second Public Draft **(September 2004)**
  - Final Public Draft **(January 2005)**
  - Final Publication **(February 2005)**
- FIPS 200
  - Initial Public Draft **(Projected for May 2005)**
  - Second Public Draft **(Projected for August 2005)**
  - Final Publication **(Projected for December 2005)**

Summary

- Public vetting process proved extremely effective and allowed NIST to build a truly consensus-based security guideline to serve both public and private sector needs
- Extended development cycle and expanded public review periods allowed federal agencies to be better prepare for the transition to FIPS 200, when the security controls become mandatory
- Increasing voluntary acceptance of NIST Special Publication 800-53 by the private sector will help provide greater information security for the nation’s critical infrastructure

NIST Risk Management Framework



Federal ICS Security Standards and Guidelines Strategy

- Add control systems domain expertise to:
  - Already available IT security Risk Management Framework
  - Provide workable, practical solutions for control systems – without causing more harm than the incidents we are working to prevent

- This expertise takes the form of specific cautions, recommendations & requirements for application to control systems - throughout both technologies and programs
  - ICS Augmentation of NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*
  - NIST SP 800-82 *Guide to Industrial Control System (ICS) Security*

NIST ICS Security Project

- Joint MEL/ITL project, in collaboration with federal and industry stakeholders, to develop standards, guidelines and test methods to help secure these critical control systems in harmony with their demanding safety and reliability requirements.

http://csrc.nist.gov/sec-cert/ics

NIST Risk Management Framework

Starting Point

FIPS 199 / SP 800-60

CATEGORIZE
Information System

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

FIPS 200 / SP 800-53

SELECT
Security Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

SP 800-70

IMPLEMENT
Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

SP 800-53A

ASSESS
Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

SP 800-37 / SP 800-53A

MONITOR
Security Controls

Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

SP 800-37

AUTHORIZE
Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

Security Life Cycle

SP 800-39

NIST SP 800-53

- NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*, which was developed for traditional IT systems, contains mandatory information security requirements for all non-national security information and information systems that are owned, operated, or controlled by federal agencies.
- NIST SP 800-53 provides the security controls that need to be applied to secure the system. It does not specify how the controls need to be implemented.
- When organizations attempted to utilize SP 800-53 to protect ICS, difficulties were encountered in implementing SP 800-53 counter-measures because of ICS-unique needs
- Held 2 Workshops (April 2006 and March 2007) with stakeholders to discuss issues and develop ICS material for SP 800-53. 2 drafts were released for public vetting before finalized in December 2007.

NIST SP 800-53 Structure

17 Control Families
171 Controls (Requirements)

- Access Control
- Awareness and Training
- Audit and Accountability
- Certification, Accreditation, and Security Assessments
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental
- Planning
- Personnel Security
- Risk Assessment
- Systems and Services Acquisition
- System and Communications Protection
- System and Information

NIST SP 800-53 Control Example

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

(2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].

LOW Not Selected	**MOD** AU-6 (2)	**HIGH** AU-6 (1) (2)

Changes made to NIST SP 800-53 to address ICS

- Original NIST SP 800-53 controls were not changed
- Additional guidance was added to 65 of 171 controls to address ICS
  - ICS Supplemental Guidance
  - ICS Enhancement Supplemental Guidance
- ICS Supplemental Guidance provides information on how the control applies in ICS environments, or provides information as to why the control may not be applicable in ICS environments.

Example:

SC-13 USE OF CRYPTOGRAPHY

ICS Supplemental Guidance:

ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

Key Take Away

- NIST SP 800-53, Revision 2 is a security standard that addresses both general IT systems as well as ICS. This allows federal agencies, as well as the private sector if desired, to use one document to determine the proper security controls for their IT systems as well as to effectively secure their industrial control systems while addressing their unique requirements.

  http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

- Federal ICS using NIST SP 800-53, Revision 2
  - Bonneville Power Administration (BPA)
  - Southwestern Power Administration (SWPA)
  - Tennessee Valley Authority (TVA)
  - Western Area Power Administration (WAPA)
  - Federal Aviation Administration (FAA)
  - Department of the Interior, Bureau of Reclamation

NIST SP 800-53 Security Baselines

- LOW Baseline - Selection of a subset of security controls from the master catalog consisting of ***basic*** level controls
- MOD Baseline - Builds on LOW baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***
- HIGH Baseline - Builds on MOD baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***

- ***How do we categorize ICS?***

Low Impact System

Possible ICS Impact Level Definitions

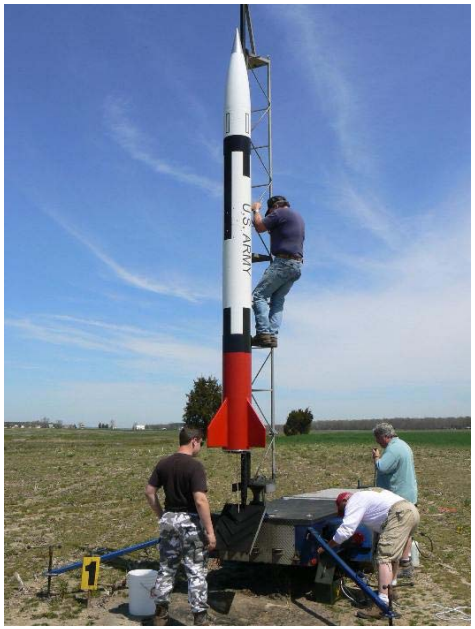
- **Low Impact**
  - **Product Controlled:** Non hazardous materials or products, Non-ingested consumer products
  - **Industry Examples:** Plastic Injection Molding, Warehouse Applications
  - **Security Concerns:** Protecting people, Capital investment, Ensuring uptime

Moderate Impact Systems

Possible ICS Impact Level Definitions

- **Moderate Impact**
  - **Product Controlled:** Some hazardous products and/or steps during production, High amount of proprietary information
  - **Industry Examples:** Automotive Metal Industries, Pulp & Paper, Semi-conductors
  - **Security Concerns:** Protecting people, Trade secrets, Capital investment, Ensuring uptime

High Impact System



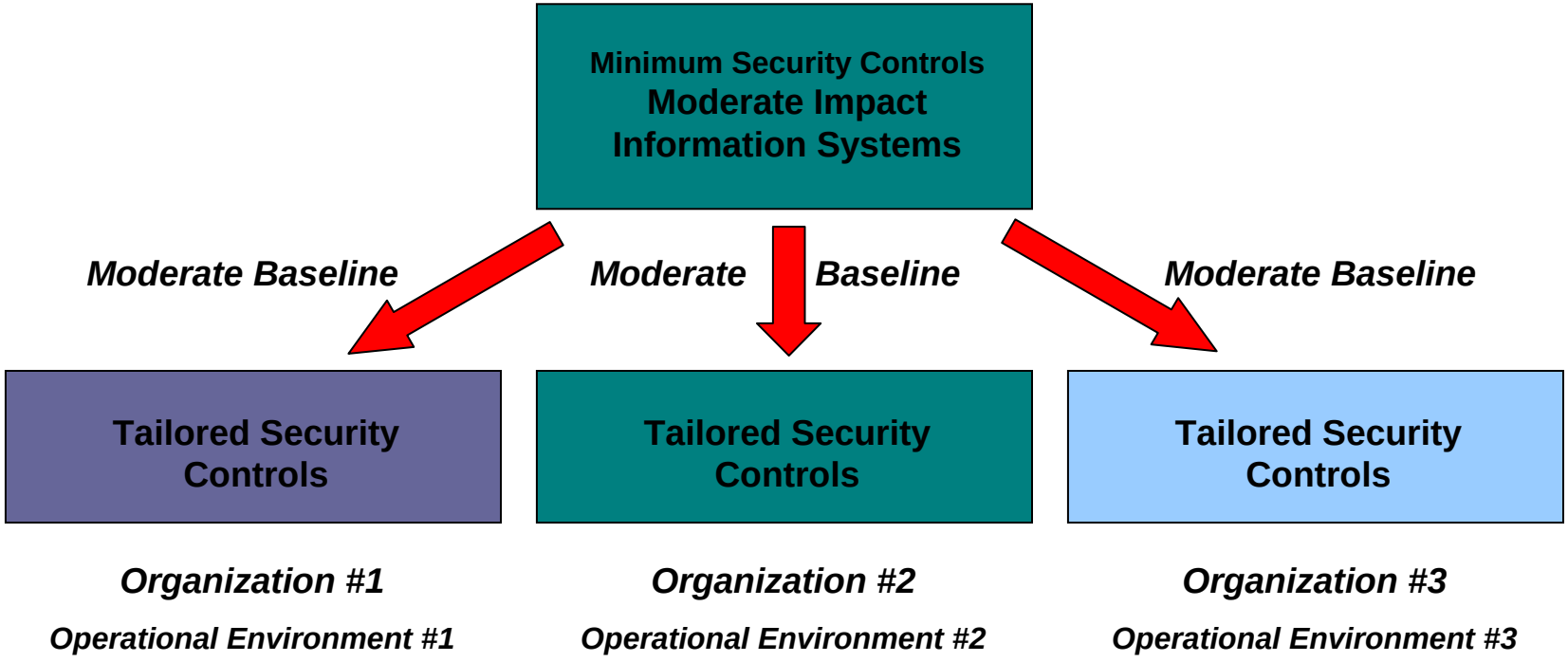
High Impact System !!!

Possible ICS Impact Level Definitions

- **High Impact**
  - **Product Controlled:** Critical Infrastructure, Hazardous Materials, Ingested Products
  - **Industry Examples:** Utilities, PetroChemical, Food & Beverage, Pharmaceutical
  - **Security Concerns:** Protecting human life, Ensuring basic social services, Protecting environment

Tailoring Security Controls

Scoping, Parameterization, and Compensating Controls



Cost effective, risk-based approach to achieving information security…

NIST SP 800-82

- Guide to Industrial Control Systems Security
  - Provide guidance for establishing secure ICS, including implementation guidance for SP 800-53 controls
- Content
  - Overview of ICS
  - ICS Characteristics, Threats and Vulnerabilities
  - ICS Security Program Development and Deployment
  - Network Architecture
  - ICS Security Controls
  - Appendixes
    - Current Activities in Industrial Control Systems Security
    - Emerging Security Capabilities
    - ICS in the FISMA Paradigm

NIST SP 800-82

- Initial public draft released September 2006 - public comment period through December 2006
- Second public draft released September 2007 - public comment period through November 2007
- Final public draft released September 2008 – public comment period through November 2008
- Downloaded over 500,000 times since initial release
- Current document available at:
  - http://csrc.nist.gov/publications/drafts.html

Private Sector ICS Security Standards

- Where the rubber hits the road!
- 90+% of ICS are owned by the private sector
- Standards for the ICS industry, if widely implemented, will raise the level of control systems security
- Greatest chance for industry acceptance and adoption is to have security requirements published in cross industry standards
  - **ISA99 *Industrial Automation and Control System Security* standard**
  - **IEC 62443 *Security for Industrial Process Measurement and Control – Network and System Security* standard**

ISA99

- Co-Chairs: Bryan Singer, Eric Cosman
- Developing an ANSI Standard for Industrial Automation and Control System Security
  - Part 1 – Models and Terminology
  - Part 2 – Establishing an Industrial Automation and Control Systems Program

    Part 3 – Operating an Industrial Automation and Control Systems Program
  - Part 4 – Technical Security Requirements for Industrial Automation and Control Systems

  - NIST SP800-53, Rev 2 have been provided to ISA99 as references to consider in the development of the standard

http://www.isa.org/MSTemplate.cfm?MicrosoftID=988&CommitteeID=6821

IEC 62443

- Convenor: Tom Phinney (US)
- Scope: Establish requirements for securing access to industrial process measurement and control networks and devices on those networks
- IEC 62443 *Security for industrial process measurement and control – Network and system security* standard
  - 62443-1, *Framework and threat-risk analysis*
  - 62443-2, *Security assurance: principles, policy and practice*
  - 62443-3, *Sets of security requirements for security elements in typical scenarios*

  - NIST SP800-53, Rev 2 have been provided to IEC TC65/WG10 as references to consider in the development of the standard

http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=e&wwwprog=dirwg.p&progdb=db1&ctnum=2931

NIST ICS Security Project Contact Information

Project Leaders

Keith Stouffer
(301) 975-3877
keith.stouffer@nist.gov

Dr. Stu Katzke
(301) 975-4768
skatzke@nist.gov

sec-ics@nist.gov

Web Pages

Federal Information Security Management Act (FISMA) Implementation Project

http://csrc.nist.gov/sec-cert

NIST ICS Security Project

http://csrc.nist.gov/sec-cert/ics