April 5, 2013
Response to Request for Information
Developing a Framework to Improve Critical Infrastructure Cybersecurity
Docket Number 130208119-3119-01

Siemens appreciates this opportunity to make suggestions to the National Institute of Standards and Technology ("NIST") regarding the Cybersecurity Framework that NIST will develop pursuant to Executive Order 13636 ("the Executive Order"). Our company looks forward to participating in NIST's workshops this summer, and to commenting on a draft Cybersecurity Framework this fall.

INTRODUCTION

Siemens is one of a number of competing vendors of computer systems that control and automate machines and infrastructure in the physical world. Industrial control systems deliver indispensible benefits to our society.

The largest categories of industrial control systems are programmable logic controllers ("PLCs") and supervisory control and data acquisition ("SCADA") systems. PLCs and SCADA systems are used in many physical assets – e.g., chemical plants, power plants, and water treatment facilities – that meet the Executive Order's definition of "critical infrastructure."

The propagation of industrial control systems throughout the United States' industrial economy began in the 1970s. At that time, inserting malicious code into a control system would have required physical access to the hardware and some conspicuous tinkering with it. Over the subsequent decades, increased standardization of hardware ports and interconnection of computer systems using telecommunications networks heightened the risk of cyber-sabotage. Appreciation of that risk among decision-makers in the private and public sectors began catching up with the new reality about five years ago, when reports of cyber-attacks started appearing in the mainstream media.

The PLCs and SCADA systems that vendors introduce to the market today incorporate considerably more cybersecurity protection than the models introduced just a few years ago. But industrial control systems are low-maintenance and long-lasting. Older models that were purchased and installed many years ago remain in use in thousands of facilities in the United States, including many facilities that qualify as critical infrastructure.

Vendors of industrial control systems should, as they introduce successive models of their products, address known cybersecurity vulnerabilities while preserving the affordability and ease-of-use that allow the products to play their highly useful role in our industrial economy. For their part, owners of industrial facilities – especially owners of critical assets – should ascertain the models of control systems presently used in their environments, understand the cybersecurity protection available within those systems, and develop a plan to address identified vulnerabilities. In Section I, below, Siemens describes content that the Cybersecurity Framework could include to improve the security profile of the industrial control systems actually in use at many critical-infrastructure assets in the United States.

Many of the most effective defenses against cyber-sabotage do not take the form of software or hardware. Rather, they are best practices to be woven into the routines of managers and workers at the facilities that contain industrial control systems. Fortunately, a number of organizations already have articulated practices that can provide a facility with a reasonable degree of defense against cyber-sabotage. Siemens believes that NIST can perform a valuable service by gathering into the Cybersecurity Framework the most effective and practical methods that are described in those different documents. In Section II, Siemens identifies the existing cybersecurity guidelines that the company finds to be especially suitable for distillation into the Cybersecurity Framework.

Even the best guidelines for preventing successful cyber-sabotage will not protect a facility unless its operators adopt and adhere to the recommended practices. Publishing those best practices in a single, high-profile document like the Cybersecurity Framework, while helpful, will not alone ensure ubiquitous and constant adherence to them. In Section III, Siemens responds to the four specific NIST questions that speak most directly to the goal of universalizing the actual use of cybersecurity best practices throughout the United States' critical infrastructure.

DISCUSSION

I. Content That the Cybersecurity Framework Could Include to Improve the Security Profile of the Industrial Control Systems Actually in Use at Critical Infrastructure

There probably are certain vulnerabilities that all vendors believe should be absent from new industrial control system products introduced from this point forward. Identifying them in the Cybersecurity Framework would likely have the beneficial effect of encouraging decision-makers at enterprises operating critical facilities to ascertain, and take action to reduce, security risks associated with industrial control systems that are currently in use at those facilities. If NIST would like to use any of its upcoming stakeholder workshops to identify the scope of such a consensus among vendors, then Siemens would be pleased to participate in those sessions. In describing any attributes that vendors agree should be absent from new products, the Framework should, we believe, speak in terms of function rather than design (i.e., what a product does rather than how, technologically, the product does it), in order to ensure that the Framework "will not prescribe particular *technological* solutions or specifications."[1]

In instances where a software update reasonably and safely can address a cybersecurity limitation that has been verified in a Siemens industrial control system, Siemens develops the update and makes it available. But many of the industrial control systems still in the installed base have been in service for many years – some of them for decades. A vendor might not know where, specifically, earlier versions of its control systems are still being used. The original vendor of a system still in use somewhere might not even be in business anymore. Siemens recommends that NIST omit from the Cybersecurity Framework any language that could create the misimpression that a vendor can always identify and contact a user of one of its systems or that a software update is always the best solution to a cybersecurity concern.

More broadly, we respectfully request that NIST avoid any content that could create the misimpression that all cybersecurity risks can or should be addressed with changes to industrial control system products. As all of the consensus-based guidelines developed to-date have recognized, the organizational, managerial, and operational practices employed by owners and operators of facilities play an indispensible part in successfully thwarting cyber-sabotage.

II. Existing Cybersecurity Guidelines That Are Especially Suitable for Distillation Into the Cybersecurity Framework

We appreciate and support NIST's statement that the Cybersecurity Framework "will incorporate voluntary consensus standards and industry best practices to the fullest extent possible and will be consistent with voluntary international consensus-based standards when such international standards will advance the objectives of the Executive Order."[2] Siemens is familiar with "existing cybersecurity

[1] 78 Fed. Reg. 13024, 13025 (Feb. 26, 2013) (emphasis added).

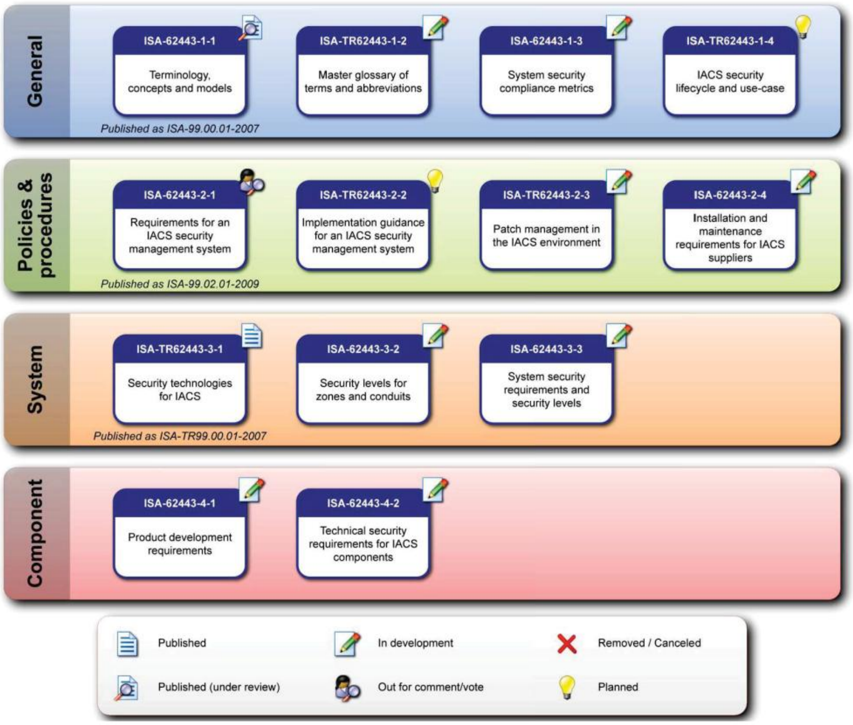
[2] *Id.*

standards, guidelines, frameworks, and best practices that are applicable to increase the security of critical infrastructure sectors and other interested entities."[3] In this section, we respond to seven of NIST's specific questions with information about existing literature that Siemens believes to be especially suitable for encapsulation and emphasis in the Cybersecurity Framework. In Appendix A, please find references to the Siemens Industrial Security website, which augments the responses provided below.

<u>What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?</u>

Siemens has chosen the developing standard IEC 62443 / ISA99 as a leading security standard for the development of automation systems and components. This standard was chosen because it is internationally supported, involves the component supplier, asset owner, and systems integrator in the solution and supports a defense-in-depth approach. It supports a holistic perspective of industrial security.

This standard, when completed, will address many key aspects of industrial security. In the illustrations below, the current status of the standard is depicted along with an overview of the topics covered in the standard. Sections of the standard apply to the key constituents who must be involved in the industrial security solution including the component vendor, systems integrator (addressed in the "System" section), asset owner (addressed in the "Policies and Procedures" section) and general documentation.



General
ISA-62443-1-1 Terminology, concepts and models
ISA-TR62443-1-2 Master glossary of terms and abbreviations
ISA-62443-1-3 System security compliance metrics
ISA-TR62443-1-4 IACS security lifecycle and use-case
Published as ISA-99.00.01-2007

Policies & procedures
ISA-62443-2-1 Requirements for an IACS security management system
ISA-TR62443-2-2 Implementation guidance for an IACS security management system
ISA-TR62443-2-3 Patch management in the IACS environment
ISA-62443-2-4 Installation and maintenance requirements for IACS suppliers
Published as ISA-99.02.01-2009

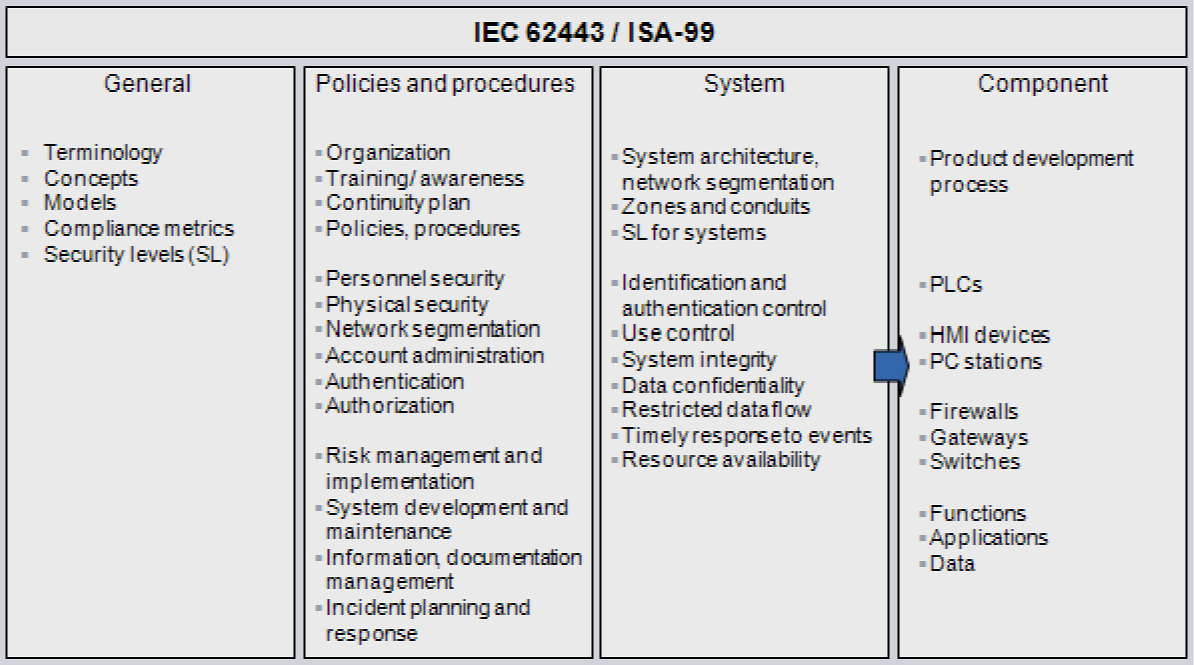
System
ISA-TR62443-3-1 Security technologies for IACS
ISA-62443-3-2 Security levels for zones and conduits
ISA-62443-3-3 System security requirements and security levels
Published as ISA-TR99.00.01-2007

Component
ISA-62443-4-1 Product development requirements
ISA-62443-4-2 Technical security requirements for IACS components

Published
In development
Removed / Canceled
Published (under review)
Out for comment/vote
Planned

[3] *Id.*

Another illustration of the standard provides an overview of the topics covered in the standard.



IEC 62443 / ISA-99

General	Policies and procedures	System	Component
Terminology Concepts Models Compliance metrics Security levels (SL)	Organization Training/ awareness Continuity plan Policies, procedures Personnel security Physical security Network segmentation Account administration Authentication Authorization Risk management and implementation System development and maintenance Information, documentation management Incident planning and response	System architecture, network segmentation Zones and conduits SL for systems Identification and authentication control Use control System integrity Data confidentiality Restricted data flow Timely response to events Resource availability	Product development process PLCs HMI devices PC stations Firewalls Gateways Switches Functions Applications Data

Other standards of focus for Siemens in the area of industrial security include NERC-CIP and WIB M-2784. In addition, Siemens has published operational guidelines and white papers on the subject of industrial security which can be found in Appendix A.

What additional approaches already exist?

Siemens' perspective on industrial control system security has been guided by various standards, guidelines, committees, associations, and government organizations. These include the following:

Technical Committees, Associations, Government Organizations

- NIST Special Publications on cybersecurity
- IEC TC 57 WG15: IEC Technical Committee (TC) 57 is one of the technical committees of the International Electrotechnical Commission (IEC). TC 57 is responsible for development of standards for information exchange for power systems and other related systems including Energy Management Systems, SCADA, distribution automation, and teleprotection. Working Group (WG) 15 is responsible for Data and Communication security.[4]
- SAC TC 124: Chinese National Committee for Industrial Security is the mirror committee of IEC TC 65and is dedicated to promoting IEC International Standards in China.
- DKE: Electrical, Electronic & Information Technologies of DIN and VDE, hosts the German National Committee for Industrial Security.
- VDI: Association of German Engineers.
- VDE: Association of German Electrotechnology.
- NIST: National Institute of Standards and Technology.

[4] Wikipedia, IEC TC 57

- DHS: Department of Homeland Security including US-CERT and ICS-CERT.

Guidelines

- Roadmap to Secure Control Systems in the Energy Sector: Document outlines a plan for improving cyber security within the energy sector.
- Roadmap to Secure Control Systems in the Chemical Sector: Document outlines a plan for improving cyber security within the Chemical Sector.
- BSI / BSI Grundschutz: The BSI is the German Federal Office for Information Security. The BSI Grundschutz is a Guideline on IT Security from the BSI.

Standards

- ISO/IEC 27000 Series
- ISO/IEC 15408 Series
- IEC TS 62351 Series

Standards (Siemens Focus)

- NERC-CIP: NERC Standards CIP-002-3 through CIP-009-3 provides a cyber security framework for the identification and protection of critical cyber assets to support reliable operation of the bulk electric system.
- WIB Report: M 2784 - X-10, version 2.0: This document specifies requirements and gives recommendations for IT security to be fulfilled by vendors of process control and automation systems to be used in process control domains ("PCDs").
- IEC 62443 / ISA-99 (under development): A multi-part series of standards and technical reports on the subject of industrial automation and control system security.

IEC 62443 / ISA-99 has been chosen by Siemens as a leading standard with respect to Siemens Industry Automation industrial control system products.

Which of these approaches apply across sectors?

Elements of many different standards, guidelines, and best practices can often be applied across sectors. Siemens has chosen IEC 62443 / ISA-99 as a leading standard because it is international in scope, vendor neutral, and incorporates important elements from other standards within our focus including WIB M-2784 and NERC-CIP. It supports a defense-in-depth approach and promotes involvement of all stakeholders including the asset owner, system integrator, and component supplier.

What, if any, modifications could make these approaches more useful?

There are several best practices, standards, controls, and other types of security guidelines that exist today. NIST could provide a valuable service in helping to clarify and promote securing industrial control systems if some of the activities below were considered:

- Review and consolidate existing cybersecurity standards, best practices, and controls into the NIST cybersecurity framework.
- Develop a cross reference between portions of the most widely adopted standards, best practices, and controls and corresponding portions of the Cybersecurity Framework.
- Develop methods to obtain strong support for a baseline level of accepted cybersecurity practice that can be applied by the various stakeholders including the asset owner, system integrator, and both system and component suppliers across all critical infrastructure.
- Establish a list of recommended controls and metrics to allow organizations to monitor and track results.

How do these approaches take into account sector-specific needs?

Establishing a strong, system level, cybersecurity baseline as recommended across all critical infrastructures can be the starting point for any optional, sector-specific enhanced requirements where necessary. Sector industry leaders or sector-specific agencies and coordinating councils can be involved and support NIST in the development of any additional sector specific requirements. Example activities include:

- Determination of whether or not the baseline standard is sufficient for the sector.
- Coordination of the development or adoption of a single sector specific standard that builds upon the baseline.
- Creation of sector specific self audit surveys and tools.
- Support the development independent audit guidelines and tools.

How do these practices relate to existing international standards and practices?

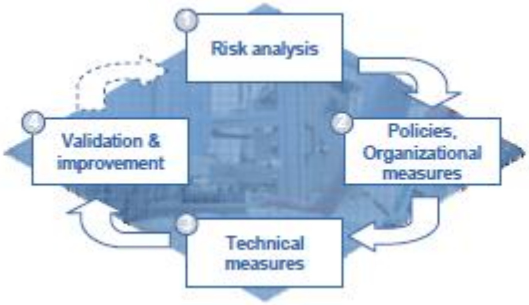
Siemens has three main standards of focus with respect to industrial control product and system related cybersecurity. IEC 62443 / ISA-99 was eventually chosen as the leading standard for Siemens Industry Automation industrial control system products. NIST as part of its request for information solicits feedback on how these practices relate. The following table correlates the practices mentioned by NIST with sections of the three main standards of focus used by Siemens as it relates to product and system related cybersecurity. The table is not meant to be an exhaustive list of references but should serve to show that the three main standards of focus used by Siemens also address many of the NIST Identified Practices

NIST Identified Practices	**Standards (Siemens Focus)**		
	NERC-CIP	**WIB M-2784**	**IEC 62443**
Separation of business from operational systems	**Reference:** CIP 005-5 , Table R1 Electronic Security Perimeter requires segmenting of BES Cyber Systems from other systems of differing trust levels	**Reference:** PA22: Implement the Architecture and associated Base Practices (BP.22.01, BP.22.02) PA32: Implement the Architecture and associated Base Practices (BP.32.01, BP.32.02) WIB's Data Acquisition and Control Architecture in Appendix 3)	**Reference:** IEC 62443-3-3: SR 5.1-Network Segmentation SR 5.2-Zone boundary protection IEC 62443-2-1: Various controls of 11.4 Network access control
Use of encryption and key management	**Reference:** CIP-005-5 Table R2 Interactive Remote Access Management	**Reference:** PA25: Protect Data and associated Base Practices (BP.25.01-05) PA35: Protect Data and associated Base Practices (BP.35.01-05)	**Reference:** IEC 62443-3-3: SR 1.8 – Public key infrastructure (PKI) certificates SR 1.9 – Strength of public key authentication SR 4.3 – Use of cryptography IEC 62443-2-1: 12.3.1 Policy on the use of cryptographic controls 12.3.2 Key management
Identification and authorization of users	**Reference:** CIP-007-5 Table R5 System Access Control	**Reference:** PA07: Secure Account Management and associated Base Practices (BP.07.01-.08)	**Reference:** IEC 62443-3-3: Identification: FR 1 User identification and authentication Authorization: FR 2 Use control IEC 62443-2-1: Most of the controls of 11 Access control
Asset identification and management	**Reference:** CIP-002-5 BES Cyber System	**Reference:** PA06: Implement Patch	**Reference:** IEC 62443-3-3:

	Categorization CIP-007-5, Table R2 Security Patch Management	Management PA16/26: Manage the Deployment PA21: Support Backup/Restore All of the above PAs have associated Base Practices	SR 7.8 – Control system component inventory IEC 62443-2-1: All controls of 7 Asset management
Monitoring and incident detection tools and capabilities	**Reference:** CIP-007-5 Table R4 Security Event Monitoring	**Reference:** PA09: Increase Network Visibility and associated Base Practices (BP.09.01-02) PA10: Standardize Historian Interfaces and associated Base Practices (BP.10.03)	**Reference:** IEC 62443-3-3: SR 2.8 – Auditable events SR 2.9 – Audit storage capacity SR 2.10 – Response to audit processing failures SR 6.1 – Audit log accessibility SR 6.2 – Continuous monitoring IEC 62443-2-1: Multiple controls of 10.10 Monitoring and 13 Cyber security incident management
Mission/system resiliency practices;	**Reference:** CIP 009-5 - Recovery Plans for Critical Cyber Assets R1. Recovery Plans R2. Implementation and Testing R3. Review, Update and Communication	**Reference:** PA09: Increased Network Visibility and associated Base Practices (BP.09.02) PA17: Harden the System and associated Base Practices (BP.17.01-02)	**Reference:** IEC 62443-3-3: SR 7.1 – Denial of service protection SR 7.5 – Emergency power IEC 62443-2-1: Controls of 14 Business continuity management
Security engineering practices	Security Engineering practices are distributed throughout the Version 5 CIP Cybersecurity Standards	**Reference:** Chapter 3, Sections 3.1, 3.2 define 35 Process Areas (PA) containing practices that define security engineering	**Reference:** IEC 62443-2-4: Installation and maintenance requirements for IACS suppliers IEC 62443-3-2: Security levels for zones and conduits
Incident handling policies and procedures	**Reference:** CIP-008-5 Incident Reporting and Response Planning	**Reference:** PA01: Prepare and Inform Personnel PA02: Designate a Security Contact PA03: Specify Base Practices Including all associated Base Practices	**Reference:** IEC 62443-2-1: Various controls of 13 Cyber security incident management 14 Business continuity management
Privacy and civil liberties protection	**None Identified**	**None Identified**	**None Identified**

Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

All of the practices listed by NIST are important to the protection of critical infrastructure. For the most part, the listed practices represent an especially critical subset of the larger set of highly-advisable best practices that can be found in several of the documents referenced in these comments. As mentioned later in this response, Siemens believes that improving the cybersecurity of operations is a continuous process. This process involves four major phases as shown in the figure below:



Rather than propose which of the practices listed by NIST are the most critical (they are all important), we thought it would be helpful for us to sort those listed practices into the appropriate phases that appear in the process illustration above. As indicated in the table below, we believe that each of the practices listed by NIST falls into one or the other of two of the phases. Details of the security management process illustrated above can be found in the Operational Guidelines presentation referenced in Appendix A.

Policies, Organizational Measures	Technical Measures
• *Employee training and awareness of cybersecurity*	• Monitoring and incident detection tools and capabilities
• Incident handling policies and procedures	• Identification and authorization of users
• Asset identification and management	• Appropriate use of encryption and key management *(where protocol supports)*
• Ongoing security engineering practices	• *Network Segmentation including separation of business from operational systems*
• Mission / system resiliency practices	

Note 1: Italicized text contained in the list above was added to the original NIST proposed practices.
Note 2: Policies, Organizational Measures and Technical Measures work together to improve cybersecurity. In many instances both are required to effectively implement the measure

Privacy and civil liberties protection are very important. It should be possible to protect critical infrastructure while also respecting those important principles.

III. Universalizing the Actual Use of Cybersecurity Best Practices Throughout the United States' Critical Infrastructure

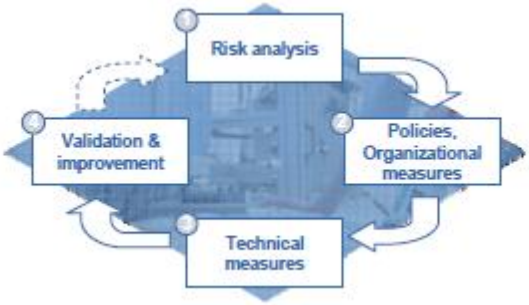
<u>What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?</u>

There are many challenges to improving cybersecurity practices across critical infrastructure. Within the United States, Siemens views the following as important challenges for consideration:

- Security Management Process
  - Security Management is a continuous process requiring sustained effort to deploy, manage, and maintain. It should be a major component of any industrial security concept. It begins with a risk analysis; encompasses policies, organizational measures, and training; deploys technical measures; and requires validation and improvement.

    A software configuration management process that supports regular updates is perhaps one of the most important aspects of the security management process. An update must be received from the vendor, tested in the customer's environment, the application recertified if required, and the industrial control system software updated. This process, though difficult and time consuming, is an essential component in protecting industrial control systems from attack. A close collaboration with the asset owner's IT department and the supplier of the industrial control system can make the process easier.

    A long-term commitment is associated with the implementation of a security management process. A significant challenge for many companies is the justification of the investment. It is important to realize that a sustained investment in the security management process is necessary to achieve the best long-term results.



- Behavioral habits are the weakest link
  - Part of the Policies and Organizational measures that should be clearly highlighted is security awareness training for all employees. The best cyber security defense can be quickly compromised by a user opening an EMAIL attachment or link as part of a general phishing campaign. Even more difficult to protect against is when the EMAIL is targeted at the organization or selected employees in a spear phishing campaign. Both types of attacks can be very successful at bypassing the cybersecurity defenses and potentially infecting an unprotected user's PC, providing a starting point for further reconnaissance and possible attack. Educating employees on the methods used by attackers and changing employee behavior when it comes to cybersecurity is accomplished through security awareness training.

- Convincing stakeholders that there is no single silver bullet
  - As more and more companies become aware of the risks of a cyber-attack, there is a natural tendency to look for one approach, a single best answer, a solution that can be configured once and never has to be considered again. New attack methods are constantly being developed. What protects systems today might be defeated tomorrow. Implementing a sustained, robust security management program is a key component to reduce the risk of a successful attack and limit the damage if one should occur. However, there is no silver bullet, no one solution fits all. The industry (as a whole), including the asset owners, system integrators, component suppliers, researchers, government agencies, etc., need to continue to monitor , invest, and update security solutions, using a standards and best practice approach, as the security situation evolves.

Other feedback from Siemens customers regarding challenges to improve cybersecurity practices include:

- Lack of Expertise in Secure Industrial Control Systems (ICS)
  - Securing an industrial control system, along with monitoring and maintaining that security requires special skills that are not readily available to some asset owners. Properly securing an ICS requires expertise in IT, operations, and controls. In some cases, IT support is provided by a third party. In other cases, control system support is provided by a systems integrator. It is very difficult to find all three skills in a single person. Bringing the skill sets from these various parties together can also be difficult and expensive. However, the best solutions are developed when the proper resources are brought to bear. Siemens provides both technical papers describing how to secure the ICS and security services to assist the asset owner. More information can be found in Appendix A.

- Decision Making / Accountability for Cybersecurity is Overly Confined to Corporate IT
  - In some operation environments, the responsibility for cybersecurity lies with Corporate IT. That can be a problem if the IT department attempts to manage the security of industrial control systems in the same manner as office IT equipment. In the event that Corporate IT is responsible for industrial control system security, a good practice is to form a partnership with operations and controls engineers in order to understand the requirements of operations and the constraints of the industrial control system. Working together, all constituents' concerns can be evaluated and the best possible solution to secure the industrial control system selected. Siemens provides extensive resources to assist in this area. More information can be found in Appendix A.

- Companies Accept Substantial Risk due to the Financial Investment Required to Mitigate Cybersecurity Risk
  - A systematic process should be followed to evaluate risk. Such a process leads to a business decision regarding the available choices concerning risk. These include:
    - Accepting the risk.
    - Mitigating, reducing, or eliminating the risk.
    - Transferring the risk (e.g., insurance)

    Siemens recommends a thorough review of the available options to mitigate the risk be conducted before deciding to accept the risk. Although accepting the risk can sometimes be a valid choice, in some instances business decisions are made to accept a risk that could otherwise be economically mitigated if the risk assessment team had current knowledge of the methods and techniques to secure the system. A good practice is to involve the industrial control system supplier in the risk assessment process where possible to ensure the latest practices to secure the system are available for consideration. Siemens can provide security services to assist the asset owner in this important process. More information can be found in Appendix A.

What other outreach efforts would be helpful?

Additional outreach efforts would be helpful in driving cybersecurity improvement across the critical infrastructure. These efforts could include:

- Highlight success stories without identifying the specific customers involved; perhaps by communicating success stories at the sector level.
- Voluntary reporting of metrics on the progress of the sectors.
- Conduct Local / Regional cybersecurity assessment seminars.
- Sponsor / support / provide cybersecurity awareness training for company executives and employees

Are these practices widely used throughout critical infrastructure and industry?

NIST, as part of its request for information, has proposed certain practices and solicits feedback on their use. The use of these practices vary with the critical infrastructure and industry involved. Based upon our observations across industries, an approximate categorization of the practices according to use is provided below:

Most Widely Adopted Practices

- Separation of business (office IT) from operational systems.
- Identification and authorization of users accessing systems.

Adopted Practices

- Use of encryption and key management (where protocol supports).
- Asset identification
  - Although asset identification is adopted, the management of these assets, in particular with respect to keeping the software up to date with current releases and updates, seems to be a minimally adopted practice.
- Incident handling policies and procedures.
- Privacy and civil liberties protection.

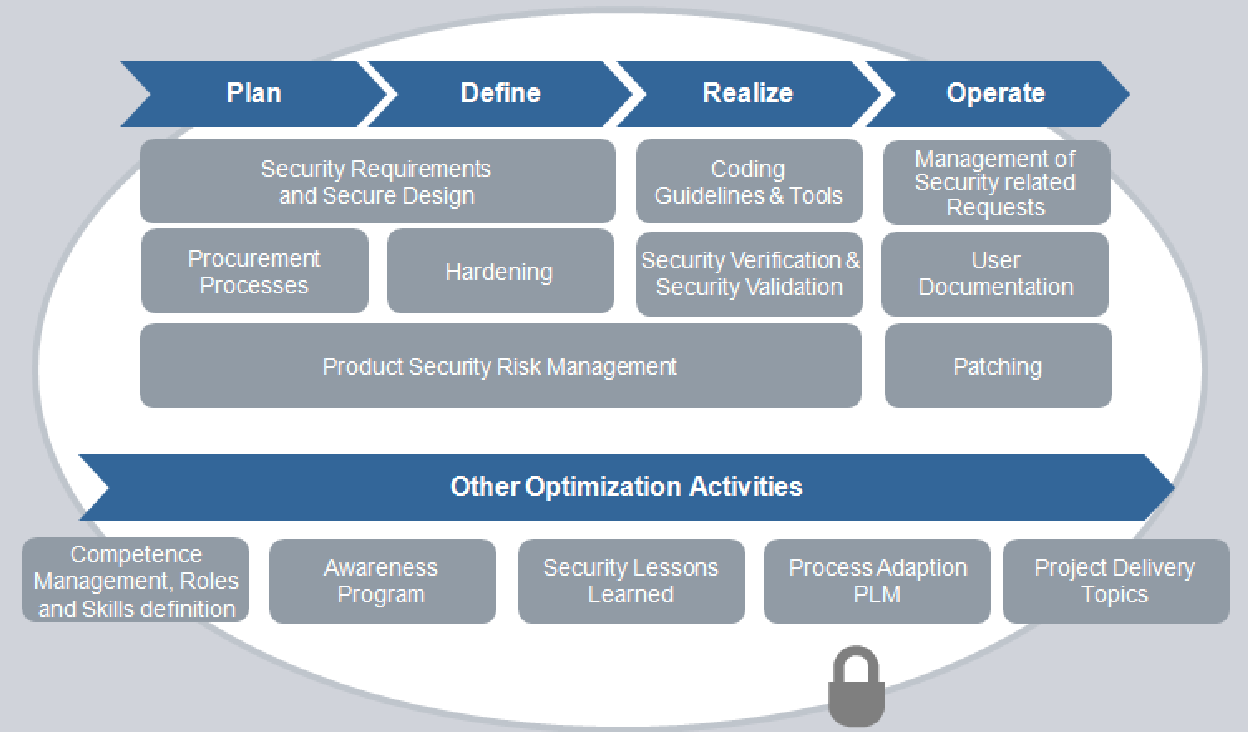
Minimally Adopted Practices

- Asset management
  - Although asset identification is adopted, the management of these assets, in particular with respect to keeping the software up to date with current releases and updates, seems to be a minimally adopted practice.
- Monitoring and incident detection tools and capabilities.
- Mission/system resiliency practices.
- Security engineering practices.

Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

Siemens actively supports the development of industry standards with broad participation in various committees. With respect to security standards that relate to our industrial control system products, this activity is coordinated by our Corporate Technology group. For example, Siemens is actively involved in the working groups associated with the development of ISA99 / IEC 62443.

In addition, Siemens has continued to invest in the development of internal policies, procedures, and best practices to support the secure development of industrial control systems. Many of those processes are derived from industry standards or specifically developed to support them. As a result of our Industrial Security Process Improvement (ISPI) program, applicable practices that improve product security are now contained within the Siemens Industry Automation development lifecycle:


Plan
Define
Realize
Operate
Security Requirements and Secure Design
Coding Guidelines & Tools
Management of Security related Requests
Procurement Processes
Hardening
Security Verification & Security Validation
User Documentation
Product Security Risk Management
Patching
Other Optimization Activities
Competence Management, Roles and Skills definition
Awareness Program
Security Lessons Learned
Process Adaption PLM
Project Delivery Topics

Another recent example was the development and publication of Siemens vulnerability handling disclosure policy. It is based upon a best practice recommendation from the Department of Homeland Security-sponsored Industrial Control System Joint Working Group (ICS-JWG) publication, entitled "Common Industrial Control System Vulnerability Disclosure Framework." A link to the Siemens policy can be found in Appendix A.

Finally, Siemens also invests in third-party certifications of its control components. For example, Siemens has recently achieved Achilles® Communication Certification offered by Wurldtech for several industrial control system components. Achilles® Level 2 Certification is an indicator that the component has achieved a high level of communications robustness. A link to Siemens components that have achieved Achilles® Level 2 Certification can be found in Appendix A.

CONCLUSION

The foregoing comments have touched upon three significant elements of the cybersecurity *status quo*. The first is the presence of cybersecurity vulnerabilities in older industrial control systems still being used at many industrial facilities, including many critical-infrastructure assets. The second is the body of effective and practical cybersecurity guidelines already available to owners and operators of industrial facilities. The third element is the current rate of actual use of those existing guidelines by the owners and operators of critical infrastructure. Siemens believes that, with respect to each of those three elements, there is constructive content that NIST could include in the Cybersecurity Framework to advance the goals of the Executive Order. Siemens stands ready to work with other stakeholders and NIST, over the next several months, to craft that content. We intend this document to serve as a helpful start.

APPENDIX A

Siemens Industrial Security

Siemens provides an Industrial Security Website to assist customers in the process of securing Industrial Control Systems. The website provides access to a wide variety of guidelines, best practices, product advisories and services of which a subset are highlighted below

Siemens Industrial Security Website:
http://www.industry.siemens.com/topics/global/en/industrial-security/pages/default.aspx

---

Siemens provides current documents and white papers on the topics of industrial security. A subset of this information is provided below:

Industrial Security > Support > White Papers:
http://www.industry.siemens.com/topics/global/en/industrial-security/support/Pages/white-papers.aspx

> Operational Guidelines: Provides proposals and recommendations for technical and organizational measures for secure operation of plant and machinery.
> http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_en.pdf
>
> Security whitepaper PC-based: Discusses security for PC-based Automation Systems with Windows Embedded Operating Systems
> http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&lang=en&objid=55390879&caller=view
>
> SIMATIC PCS 7 / WinCC Security concept: Provides a concept for securing SIMATIC Process Control System PCS 7 and WinCC (Basic)
> http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&lang=en&objid=60119725&caller=view

Other excellent articles, including those developed by ARC, along with interviews with senior Siemens management pertaining to security, are also available.

Siemens provides services to support the systems integrator or asset owner in the process of securing an Industrial Control System. Siemens' approach integrates security mechanisms with a comprehensive understanding of automation, providing support in implementing the necessary measures to secure the industrial control system. Siemens' Industrial Security Services range from risk assessment, to implementation of suitable measures, to proactive threat management with the following goals:

- Protection of the availability of production processes with an individual security architecture
- Protection of intellectual property
- Integrity of the data and data streams

For this purpose, Siemens offers professional consulting, assessments and service contracts that are based on our packaged solution modules and are individually adapted to customer needs.

Information regarding the various services available from Siemens can be found on the Siemens Industrial Security Website by selecting the "services" tab. A subset of this information is provided below:

Industrial Security > Services (select "Services" tab)

Services Overview: http://www.industry.siemens.com/topics/global/en/industrial-security/services/Pages/Default.aspx

Integrated Packages: http://www.industry.siemens.com/topics/global/en/industrial-security/services/Pages/packages.aspx

Assessments: http://www.industry.siemens.com/topics/global/en/industrial-security/services/Pages/assessments.aspx

Service & Maintenance: http://www.industry.siemens.com/topics/global/en/industrial-security/services/Pages/maintenance.aspx

Brochure: "Security all around – Industrial security for your plant at all levels"
https://c4b.gss.siemens.com/resources/images/articles/e20001-a1140-p200-x-7600.pdf

Brochure: "Network Security"
http://www.automation.siemens.com/salesmaterial-as/brochure/en/brochure_network-security_en.pdf

Siemens CERT: http://www.siemens.com/corporate-technology/en/research-technologies/technology-areas/it-security/cert.htm

ProductCERT Security Advisories: http://www.siemens.com/corporate-technology/en/research-technologies/technology-areas/it-security/cert-security-advisories.htm

Siemens Vulnerability Handling Disclosure Policy: http://www.siemens.com/corporate-technology/en/research-technologies/technology-areas/it-security/vulnerability-handling.htm

A substantial amount of additional information is available on the Services portion of the Industrial Security website including our security concept, products, support, and news/alerts. We encourage interested readers to browse the site and learn more about Siemens Industrial Security.

Wurldtech Achilles® Communications: Wurldtech's Achilles® Communications Certification provides an industry leading benchmark for the secure development of the applications, devices and systems found in critical infrastructure. Several Siemens industrial controls components have achieved Achilles® Level 2 Certification. A link to the list is provided below:

http://www.wurldtech.com/product_services/certify_educate/achilles_communication_certification/