1201 South 2nd Street
Milwaukee, WI 53204 USA

Rockwell Automation

Reply to Request for Information (RFI) to the Cybersecurity Framework

Executive Summary

Rockwell Automation respectfully submits an independent response to the National Institute of Standards and Technology (NIST) Request for Information (RFI) in order to provide input toward the development of a comprehensive Cybersecurity Framework ("Framework") to reduce cyber risks to the United States of America Critical Infrastructures.

Rockwell Automation, the world's largest company exclusively dedicated to industrial automation, makes its customers more productive and the world more sustainable. Everyday Rockwell Automation helps solve industrial automation challenges and similarly supports the safe, secure and reliable operation of industrial control systems ("ICS") that are owned and operated by private companies and local, State and the Federal government. Through collaboration and cooperation with these entities, Rockwell Automation strives to help enhance and improve the cybersecurity protections available to, and employed within these ICS, especially those systems employed in critical infrastructures on which United States citizens and their Government alike rely.

Through this RFI response process, Rockwell Automation expresses its commitment to continuing to collaborate closely with industry and the US Government to help protect critical infrastructures and key resources (CI/KR). Furthermore, Rockwell Automation desires to actively participate in forthcoming activities related to NIST and other relevant US Government agencies to define and execute a Cybersecurity Framework that fulfills Executive Order 13636 (Executive Order) and Presidential Policy Directive 21 (PPD 21): Critical Infrastructure Security and Resilience both issued 12 February, 2013.

As noted by the Executive Order, the Framework will consist of standards, methodologies, procedures and processes that align policy, business, and technological approaches to address cyber risks. It is recognized by Rockwell Automation that the collective effort to develop and execute this Framework will require successful collaboration among many parties including ICS product, system and service suppliers. Rockwell Automation is pleased to participate in this effort and represent the company's broad ICS perspective in order to help document, scope and refine the approach used in the creation of the Cybersecurity Framework, as per the Executive Order and PPD 21.

April 8, 2013

LISTEN. THINK. SOLVE.

Background on Rockwell Automation

Rockwell Automation, the world's largest company dedicated to industrial automation, makes its customers more productive and the world more sustainable. Throughout the world, our flagship Allen-Bradley® and Rockwell Software® product brands are recognized for innovation and excellence.

In the normal course of business, Rockwell Automation (RA) supplies thousands of public and private customers with a variety Industrial Control System (ICS) products, services and technologies tailored for use in extremely diverse automated industrial applications including: Discrete Control, Motion Control, Safety Control, Process Control, Batch Control, Distributed Control System (DCS) and Supervisory Control and Data Acquisition (SCADA) systems. These industrial control solutions help automate critical infrastructure processes and typically include a range of devices that include Programmable Logic Controllers (PLC); Programmable Automation Controllers (PAC); Human-Machine Interfaces (HMI); Industrial Computers; Software for visualization, monitoring, configuration, data collection and control; AC drives (low voltage and medium voltage); I/O (chassis-based and remote); Safety-rated components and I/O; Motion controllers and servo drives and a variety of other networked and electrically integrated devices and components.

Rockwell Automation's installed base and established market position in both the US and global industrial automation market results in a specific product, system, and services presence in the control systems that comprise all 16 critical infrastructure sectors and key resources (CI/KR) as defined in PPD-21 and formerly, by the Homeland Security Presidential Directive 7 (HSPD-7), National Infrastructure Protection Plan (NIPP), and other federal policies. Rockwell Automation's participation in the Framework development is intended to help ensure adequate and balanced consideration of all 16 sectors and industry types. Furthermore, participation is intended to help facilitate more rapid adoption of the practices that will be defined by the Framework.

Position on Cybersecurity for Critical Infrastructure

Rockwell Automation promotes a position that cybersecurity is a core tenet in the design, operation and ongoing maintenance of legacy and contemporary ICS, especially those systems employed to run critical infrastructure applications.

> NOTE: For the purposes of this response to the RFI, the term "critical infrastructure" will carry the specific meaning given to the term in 42 U.S.C. 5195c(e)— "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

ICS employed in critical infrastructures are increasingly dependent, and in some cases wholly reliant, on network connectivity and information technologies for the reliable transfer of data essential for safe configuration, monitoring and control decisions to be made within the system. Furthermore, the existing and growing interactions among critical infrastructures necessitate very broad consideration of risks, threats and impacts that often extend far beyond any single industrial control system employed within these applications.

Security compromises and breaches in these ICS can result in direct and indirect consequences that span both the digital and physical space, with impacts from successful intentional or unintentional attacks inflicting damage to a broad range of victims such include: ICS asset owners, operators and associated employees, business operations and business viability; citizens who depend on safe, available and reliable ICS operations; local, state and the national economy; and also national defense.

For these reasons, Rockwell Automation advocates that cybersecurity risks be measured, monitored, mitigated where possible, and also treated as an essential consideration in the development of business continuity, disaster recovery and crisis management plans for all ICS, especially those systems employed within critical infrastructure processes.

Reply to Request for Comment

The responses expressed herein are those perspectives, observations, and points of view of Rockwell Automation gained from globally serving thousands of customers in industrial control system applications that include and extend beyond the 16 critical infrastructure sectors and key resources (CI/KR) defined in PPD-21. These generalizations and specific answers may not necessarily be shared by surveying any single, individual customer or user of Rockwell Automation products, systems and services. Nonetheless, Rockwell Automation has attempted to depict, in the company's experience, what appears most representative, commonplace, or most commonly and widely observed across the collection of CI/KR sectors served by the company.

NIST Engagement with Critical Infrastructure Stakeholders

Rockwell Automation is a strong proponent for standards, guidelines and best practices that can be collectively assembled into a single framework capable of responsibly and measurably helping to reduce cybersecurity risks to critical infrastructures, especially those that employ industrial control product and systems.

It is recognized that the Executive Order 13636 (Executive Order) and Presidential Policy Directive 21 (PPD 21) direct NIST to engage with **critical infrastructure stakeholders**, through a voluntary consensus-based process, to develop the standards, guidelines and best practices that will comprise the Framework. Per the Executive Order and PPD 21, this will include interactive workshops with **industry** and academia, along with other forms of outreach. Furthermore, the Executive Order and PPD 21 call for DHS and Sector Specific Agencies to provide input in this area based on their engagement with **sector stakeholders**.

> Comment: Although not explicitly identified in the Executive Order and PPD 21, it is Rockwell Automation's position that reputable ICS product, service and solution suppliers that hold sizeable installed base and will sustain ongoing support for CI/KR should be considered within this definition of **critical infrastructure stakeholders, industry** and **sector stakeholders**.

As per the NIST Request for Information, Rockwell Automation hereby provides the following responses for consideration by NIST and other relevant US Government agencies in the formation of the Cybersecurity Framework:

1.	What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?	• Inadequate supply of competent, trained personnel in sectors capable of administering security-related ICS designs, installations, device and system configurations, maintenance, ICS security assessments, and the development and successful deployment of risk remediation and incident response plans. • Employee recruiting and retention challenges leading to shortcomings in filling and/or maintaining qualified talent to adequately address risks to ICS. • CI budgetary restrictions that result in greater risk acceptance and trade-offs in the ICS design, component selection, service, support and maintenance practices. • Difficulty identifying and prioritizing risks, threat actors, and the probabilities and potential impacts to a CI's ICS. • Inability to conduct self-assessments and risk remediation as a result of lack of competent internal resources. • Sector-wide underestimation of actual risk and probabilities for both indirect and direct attacks against a sector CI's ICS. • Sector-wide reluctance to introduce change or variables into systems with a measureable history of safe, reliable operation resulting in widespread use of highly antiquated technologies that are exposed to new risks and contemporary threats. • Need to change perspectives on suitable lifespans for CI ICS components. Historical life expectancy was measured in decades, not years. • Lack of planning in systems to sustain downtime in order to adequately service, upgrade and patch ICS equipment (e.g. component upgrades and replacement, patching, etc.) • Inherent risks associated with runtime security in systems that must operate in real time. • Increasing connectivity among ICS systems, machines, I/O, and enterprise networks, resulting in obsolescence of former "air gap" security strategies.
2.	What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?	• CI systems and specifically ICS are not equal across sectors. • Risks and threat actor motives vary widely among sectors. • Some sectors have already established recognized security practices that might be modified in negative ways as result of Framework deployment. • The Framework may only add greater complexity to an already established array of sector-specific governing standards, regulations, governance and certification bodies, consortia. • Sectors operate independently and autonomously, yet a cross-sector standards-based Framework more closely linking sectors together could slow current progress to protect ICS in CIs. • Some sectors have already independently developed different

		levels of acceptable risk that may be altered by the Framework. • Some sectors have intentionally invested in, adopted and even mandated specific technologies, protocols, hardware, software, design practices, auditing approaches, certifications, etc. that may be altered with a cross-sector Framework. • Most sectors cannot yet characterize and adequately address security risks and threats within their own sectors. A cross-sector Framework may deplete resource availability to address sector-specific risks at the expense of cross-sector progress.
3.	Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?	For Rockwell Automation, ignoring risk is not an option. Once identified, risk is addressed using the following techniques: Risk Mitigation, Risk Transference, Risk Acceptance, and Risk Avoidance. Assessing and addressing risk is also not limited only to the organization. As a leading global supplier of ICS products, systems and services used in industrial applications including CI/KR, Rockwell Automation recognizes our customers similarly face risks. As a result, our organization helps solve industrial automation challenges to facilitate safer, more reliable and more secure operation of systems owned and operated by private companies and local, state and the federal government. A variety of methods are used to communicate and oversee policies and procedures including: technical, non-technical means; organizational structure; separations of duties and responsibilities; reporting; auditing; employee awareness training and competency building. Enterprise Risk Management is integral to company operations and specific, proactive practices are followed to help identify and mitigate risks such as BIA, BCP, DRP and Crisis Management planning. Enterprise Risk Management is addressed by senior management, with oversight from the Board of Directors. Key ERM risks that we have identified include information security, product and service security, and IT availability. We have a Chief Information Security Officer who leads company activities in many of these areas with guidance and oversight from an Information Security Executive Steering Committee of senior executives. Specific to cybersecurity, employees and customers alike are encouraged to remain vigilant for threats and follow methods that can help identify and mitigate risk. Within the organization, information flows freely both upward and downward. Real-time communications among decision makers within the organization is the norm. Directions from senior management are readily cascaded to groups and individuals to execute on protective steps to protect the organization, and when necessary, remediate cyber incidents.
4.	Where do organizations locate their cybersecurity risk	Cybersecurity risk management for ICS in CI often remains undefined until an incident necessitates ad-hoc team to remediate risk. Often IT departments are engaged; however, the lack of IT knowledge of ICS and

	management program/office?	priorities to respect availability and uptime often result in significant inefficiencies and sometimes added risk being introduced during cybersecurity incident response. In our view, cybersecurity and information security risk are much broader than the IT function and need to be separate from IT from a management and oversight perspective. Some progressive organizations have established ICS cybersecurity risk management responsibility under Finance, Legal, as expanded C-level functions via CSO/CISO/CRO functions.
5.	How do organizations define and assess risk generally and cybersecurity risk specifically?	Many organizations process risk, in a general sense, at the Business Enterprise and Operations level using an Enterprise Risk Management approach that often originates with a BIA → BCP process, and includes tabletops and workshops to identify, understand and establish appropriate techniques for managing associated risks and threats. Some proactive organizations expand on the ERM process to include IRP, DRP and Crisis Management Planning. Adoption of ERM and risk assessment, including IR, DRP and Crisis Management planning remain largely limited to only the most progressive organizations with ICS, often to those organizations where regulations have imposed requirements to prepare and perform for compliance reasons. Ignoring risk is largely recognized in industry as unacceptable; however, cybersecurity risks to ICS especially specifically are sometimes characterized differently from safety risks, leading to conflicting opinions for how best to address risk, including differing priorities in the importance, timing and approach for how and when cybersecurity risks to ICS should be managed.
6.	To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?	We have observed that many SEC-reporting companies have not identified cybersecurity risk as a material risk factor, despite SEC guidance that highlights these risks as a disclosure consideration. While we recognize that many companies have legitimate grounds not to include cyber risks in their risk disclosures, we have observed that manufacturing, energy, and CI companies are less likely to acknowledge cybersecurity as a top risk issue, compared to software companies and financial institutions. We are not convinced that cyber risks to ICS (as opposed to enterprise networks) have drawn the attention of the senior executives who rate the likelihood and severity of top enterprise risks. In our experience, organizations that acknowledge cybersecurity risks as legitimate risks to ICS, follow some means to rationalize the technique to manage the risk. Most often, these risks to ICS are evaluated in a manner consistent with IT risk profiles and BIAs for potential disruptive effects to the organization from loss of use, loss of data/IP or downtime

		associated with loss of data exchange between the ICS and the Enterprise. Few organizations have been observed going to the extent to specifically calculate risk and impact to the business and those dependent on safe, reliable business operations should sustained loss of availability or malicious attack disrupt, damage or destroy a CI's ICS. Still fewer organizations have been observed calculating the value of their intellectual property and know-how as protected by, or incorporated within the ICS system designs.
7.	What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?	• Informal approaches to self-assess risk and determine how to reduce risk to a perceived acceptable level. • Leveraging internal resources, likely from IT, to help evaluate risks to networked ICS; however, recognizing IT departments rarely have built competency to understand unique ICS risks. • Consultants to assist with assessing risks and providing recommendations. • Consultants to apply security controls and make modifications to ICS to improve security posture.
8.	What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?	SEC regulations require SEC-reporting companies to report material cyber risks at a very high level. No such regulation applies to private companies, municipal water utilities, and many government agencies that operate CI. In parallel, a wide range of privacy-driven laws and regulations have arisen that require companies to notify/disclose security breaches, usually when PII (personally identifiable information) has been compromised. Regardless of one's view of the merit of the "breach disclosure" requirements for PII, we believe it would be an enormous mistake to apply a similar perspective to breaches of ICS or other systems involved with CI. When we are breached, we are victims of a crime, not careless stewards of someone else's information. Breach disclosure in this context would usually make matters worse by highlighting vulnerabilities.
9.	What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?	Virtually every asset of a modern enterprise depends on telecommunications and energy. Many assets—and every enterprise—depend on financial services, water and transportation.
10.	What performance goals do organizations adopt to ensure their	Many organizations do correlate performance goals and ability to provide essential services with a high level of availability and reliability. Many progressive ICS asset owners have recognized the effective

	ability to provide essential services while managing cybersecurity risk?	management of cybersecurity risk within an ICS directly relates to higher, more mathematically stable processes and services. Protecting the operational integrity and key information assets of an ICS through the use of system hardening and compensating controls typically results in greater and measureable uptime improvements and greater capability to survive variables that may not necessarily be limited to cyber-attacks from malicious threat actors. Many organizations treat this as part of business continuity planning.
11.	If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?	Rockwell Automation SEC documents include the following: ***[quote included in FORM 10-K]*** ***Failures or security breaches of our products or information technology systems could have an adverse effect on our business.*** *We rely heavily on information technology (IT) both in our products, solutions and services for customers and in our enterprise IT infrastructure in order to achieve our business objectives. Government agencies and security experts have warned about growing risks of hackers, cyber-criminals and other attacks targeting every type of IT system including industrial control systems such as those we sell and service and corporate enterprise IT systems.* *Our portfolio of hardware and software products, solutions and services and our enterprise IT systems may be vulnerable to damage or intrusion from a variety of attacks including computer viruses, worms or other malicious software programs. These attacks have sometimes been successful.* *Despite the precautions we take, an intrusion or infection of software, hardware or a system that we sold or serviced could result in the disruption of our customers' business, loss of proprietary or confidential information, or injuries to people or property. Similarly, an attack on our enterprise IT system could result in theft or disclosure of trade secrets or other intellectual property or a breach of confidential customer or employee information. Any such events could have an adverse impact on revenue, harm our reputation, cause us to incur legal liability and cause us to incur increased costs to address such events and related security concerns.*
12.	What role(s) do or should national/international standards and organizations that	In our experience, many organizations with ICS assets that follow the current approach, whereby firms that operate independently from the standards bodies are accredited and perform as a certifying body for standard compliance, are effective in their conformity assessment. Where possible, provisions that allow organizations with ample and

	develop national/international standards play in critical infrastructure cybersecurity conformity assessment?	competent staff and internal capabilities to self-assess conformity are highly desirable. Regardless of the approach, the Framework definition and execution should strive to reduce conformity assessment burdens and expenses already being imposed on ICS systems asset owners and suppliers by simplifying and streamlining processes and empowering capable organizations everywhere possible. All requirements should be harmonized with global requirements, lest they become a detriment to US competitiveness.

Reply to Use of Frameworks, Standards, Guidelines, and Best Practices

1.	What additional approaches already exist?	• NIST 800-30 Series: Risk Management • NIST 800-40: Creating a Patch and Vulnerability Management Program • NIST 800-53: Recommended Security Controls for Federal Information Systems & Organizations • NIST 800-82: Guide to Industrial Control Systems (ICS) Security • NIST 800-83: Guide to Malware Incident Prevention and Handling • ISA-99/IEC 62443: Network and System Security for Industrial Process Measurement and Control • ISO/IEC 27000-series: Information Security Management System (ISMS) Standards • ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation • NERC-CIP: Reliability Standards for Critical Infrastructure Protection • 21 CFR Part 11: US FDA guidelines on electronic records and electronic signatures • Rockwell Automation Converged Plantwide Ethernet Architecture for Manufacturing (http://www.rockwellautomation.com/products-technologies/network-technology/architectures.page#/tab2) • Highly-tailored ICS consulting solutions from Rockwell Automation Network & Security Services (NSS) consultants.
2.	Which of these approaches apply across sectors?	• NIST 800-30 Series: Risk Management • NIST 800-40: Creating a Patch and Vulnerability Management Program • NIST 800-53: Recommended Security Controls for Federal Information Systems & Organizations • NIST 800-82: Guide to Industrial Control Systems (ICS) Security • NIST 800-83: Guide to Malware Incident Prevention and Handling • ISA/IEC 62443: Network and System Security for Industrial Process Measurement and Control • ISO/IEC 27000-series: Information Security Management System

		(ISMS) Standards • ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation • Rockwell Automation Converged Plantwide Ethernet Architecture for Manufacturing (http://www.rockwellautomation.com/products-technologies/network-technology/architectures.page#/tab2) • Highly-tailored ICS consulting solutions from Rockwell Automation Network & Security Services (NSS) consultants.
3.	Which organizations use these approaches?	It remains unusual for most Industrial Control System (ICS) asset owners to employ practices defined in standards such as listed below to the ICS environment; nonetheless, there are certain regulated industries whose asset owners are mandated to fulfill specific standards or regulations. IT NIST 800-40: Creating a Patch and Vulnerability… IT/G NIST 800-53: Recommended Security Controls for … OT NIST 800-82: Guide to Industrial Control Systems (ICS) Security IT NIST 800-83: Guide to Malware Incident Prevention and… OT ISA/IEC 62443: Network and System Security for Industrial… IT ISO/IEC 27000-series: Information Security Management… IT/G ISO/IEC 15408: Common Criteria for Information Technology… PWR NERC-CIP: Reliability Standards for Critical Infrastructure… PHAR 21 CFR Part 11: US FDA guidelines on electronic… *IT = Information Technology* *G = Government* *OT = Operational Technology* *PWR = Power Generation, Distribution* *PHAR = Pharmaceutical*
4.	What, if any, are the limitations of using such approaches?	The variety and disparity among information security and cybersecurity guidelines result in challenges for CI organizations with ICS to decide and determine which approaches they should follow in order to best address varying and evolving risks. No single approach proves sufficient. Furthermore, overlaps among objectives and approaches to security lead to inefficiencies in the deployment, maintenance and conformance.
5.	What, if any, modifications could make these approaches more useful?	When particular standards, approaches or aspects of an approach are followed, the decision is often the result of biased preference, consulting influence or on occasion overall ignorance of better suited alternatives. Providing clarity surrounding the existing dizzying choices of approaches and their suitability for application to an ICS environment would be helpful.
6.	How do these approaches take into account sector-specific needs?	Of the listed approaches, it is believed that only *NERC-CIP: RELIABILITY STANDARDS FOR CRITICAL INFRASTRUCTURE PROTECTION AND 21 CFR PART 11: US FDA GUIDELINES ON ELECTRONIC RECORDS & ELECTRONIC SIGNATURES* carry any sector-specific mandates. Most approaches are generic and do not account for specific characteristics unique to critical

		infrastructure ICS, nor specifics that relate to ICS applied in each sector.
7.	When using an existing framework, should there be a related sector-specific standards development process or voluntary program?	Sector-specific standards are essential, both to account for the unique challenges, operating requirements and threat landscape faced by each sector and to ensure that costly requirements are mandated only in those sectors where the cost is warranted by the risk. Consideration should be given to design the Framework at a level high enough so attributes common across sectors are consistently applied across all sectors, while provisions are made for sector-specific issues to be rationalized and addressed via "plug-ins" or "modules" to the Framework. Sectors should retain latitude to expand upon common attributes of the Framework to leverage existing investments and momentum to protect sector CIs. Furthermore, sector-specific new and existing best practices should be continually weighed for applicability to the Framework for adoption or deployment across all sectors.
8.	What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?	Consideration should be given to engage sector-specific agencies and councils after the comprehensive Framework is defined. These agencies and councils can accelerate the development of relevant sector-specific "modules" or "plug-ins" to the Framework to ensure the goals of both the sector and overarching Framework are fulfilled. Furthermore, these agencies and councils can help facilitate information exchanges among sectors to help with sharing of best practices and relevant information, especially for those sectors with known interdependencies.
9.	What other outreach efforts would be helpful?	Consideration should be given to broad and consistent promotion and communication to sector stakeholders about the progress being made to develop and deploy the Framework, as well as progress by each of the specific sectors to participate and adapt to the defined practices. Efforts also should be made to ensure the Framework evolves over time and remains flexible to change with emerging threats, technologies and as new best practices emerge.

Reply to Specific Industry Practices

1. Are these practices widely used throughout critical infrastructure and industry?

Practices	*Widely Observed?*	*Comments*
SEPARATION OF BUSINESS FROM OPERATIONAL SYSTEMS	Yes	Typically firewalls; Growing use of DMZ and segmentation.
USE OF ENCRYPTION AND KEY MANAGEMENT	No	
IDENTIFICATION AND AUTHORIZATION OF USERS ACCESSING SYSTEMS	Yes	Varying degrees of granularity, ranging from all with physical access to ICS, to users restricted to specific tasks.

ASSET IDENTIFICATION AND MANAGEMENT	Yes	
MONITORING AND INCIDENT DETECTION TOOLS AND CAPABILITIES	Yes	Often physical security and building automation security systems; in ICS, safety systems are employed for access control; ongoing slow growth of IDS/IPS in ICS infrastructure; PC endpoint security largely commonplace; Product updates and product patch management practices are irregular, thereby diminishing the effectiveness of monitoring tools and also potentially resulting in greater exposure for the ICS to security risks.
INCIDENT HANDLING POLICIES AND PROCEDURES	No	*No* for cybersecurity IR for ICS; however, typically *Yes* for Safety IR for ICS.
MISSION/SYSTEM RESILIENCY PRACTICES	Yes	High Availability (HA) and Redundancy typically engineered into critical systems; failure/fault-modes configured; Safety Instrumented Systems (SIS) employed and typically include mechanical safety mechanisms where possible and practical.
SECURITY ENGINEERING PRACTICES	No	Security architected into the ICS of the CI prior to or during initial deployment remains rare due to most CIs being existing systems that have evolved over time and been only partially upgraded; Bolt-on security in CI ICS remains most commonplace, leading to incomplete defense in depth practices that often deliver little more than perimeter controls attempting to protect against external threat actors; Even many contemporary ICS that proactively include security considerations in the system design can devolve to less secure states as a result of personnel changes, and needs to streamline or accelerate support, service and maintenance to the system and its components.
PRIVACY AND CIVIL LIBERTIES PROTECTION	See comments	Intellectual Property (IP protection): Yes Civil liberties protection: Security issues in ICS revolve around information about processes, not people.

2.	How do these practices relate to existing international standards and practices?	The referenced practices remain largely unaddressed by existing international standards. Some progressive organizations with ICS look toward, and attempt to adapt techniques and practices commonly employed by IT; however, most organizations create their own practices due to an absence of defined practices tailored to ICS. Even existing ICS-focused cybersecurity standards lack guidance on a majority of these referenced standards.
3.	Which of these practices do commenters see as being the most critical	Of the referenced practices, Authorization/access, Asset ID, and Monitoring are deemed most important to ICS asset owners in CI. Many organizations are challenged with asset identification, including

	for the secure operation of critical infrastructure?	mobile assets, user authorization/access controls, monitoring and logging and incident handling procedures. Many organizations with ICS assets do not know what, nor how many assets are employed in their systems. Few have visibility to how and when assets connect/disconnect from the ICS. Monitoring of such events in an ICS remains largely nonexistent. Intrusion detection and protections are largely absent in most ICS. Although separations and perimeter controls may be part of a design, assessments often highlight improper configurations or rogue communication routes into the ICS that bypass security controls. The root cause for many of these challenges stems from shortcomings in secure engineering practices during the design, installation and maintenance lifecycle aspects of the ICS.
4.	Are some of these practices not applicable for business or mission needs within particular sectors?	Yes. Every sector has unique needs and not all practices apply across the board. However, some concepts and principles apply to most or all sectors.
5.	Which of these practices pose the most significant implementation challenge?	From Rockwell Automation's point of view, Encryption and Key Management for an ICS environment in CIs pose the most significant technical implementation challenges.
6.	How are standards or guidelines utilized by organizations in the implementation of these practices?	Standards and guidelines are typically only used at a very high level, unless specific performance criteria are mandated for compliance. Often, organizational personnel tailor existing standards and guidelines to fit specific application, regulations, business and cultural needs. Standards and guidelines are rarely applied in their entirety, with a mix of approaches often applied at different timeframes, by different personnel with different motivations behind the application of the standards and guidelines.
7.	Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?	Most organizations do not. Many IT standards are deployed on an ad-hoc basis driven by specific business conditions that warrant focused investment at a given time. Rarely are organizations observed as following methodical deployments of security approaches whereby business resources are allocated to develop and deploy practices in a comprehensive and proactive manner. The same challenges, only amplified, are seen to apply to organizations with ICS assets.
8.	Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?	Organizations do not typically develop, maintain and exercise formal cybersecurity Incident Response plans for ICS in the CI/KR space. Any necessary escalation process would typically be handled ad-hoc, evaluated on a case-by-case basis and initiated during an actual cyber event.
9.	What risks to privacy and civil liberties do commenters perceive	None.

	in the application of these practices?	
10.	What are the international implications of this Framework on your global business or in policymaking in other countries?	Where sector critical infrastructure processes may cross adjacent country borders (e.g. power, water, etc.), there are potential compliance implications for a CI asset owner expected to conform to the Framework since contradictory requirements outside of the US may influence the cybersecurity practices applied to the CI. Mandated use of specific encryption application or technologies can introduce import/export limitations or complexity if certain technologies are mandated for use by the Framework without flexibility for the sectors to override or take exceptions to such mandates. All US requirements should be harmonized with global requirements and standards.
11.	How should any risks to privacy and civil liberties be managed?	Inapplicable.
12.	In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?	Programs and methods that facilitate clearer and greater levels of relevant information sharing among stakeholders both within and across sectors should be deployed.

In addition to these above responses, please refer to the accompanying document titled, Securing SCADA and Industrial Control Systems. This publication highlights Rockwell Automation's position on the importance of enhancing the security of Securing Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) and also the linkage between security and safety within these systems.

Any desire by NIST and other relevant US Government agencies for further clarification with respect to Rockwell Automation's answers to these provided to questions can be requested at any time.

Respectfully submitted,

Sujeet Chand
Senior VP and Chief Technology Officer
Rockwell Automation, Inc.

James B. Motes
VP and Chief Information Security Officer
Rockwell Automation, Inc.

For follow up or further information:

Doug Wylie, CISSP
Director, Product Security Risk Management
Rockwell Automation, Inc.
drwylie@ra.rockwell.com
Tel:(440) 646-3728

LISTEN. THINK. SOLVE.