NIST Cybersecurity Framework

Response to Request for Information

Comment Deadline:	October 10, 2014
Type:	Individual
Sector Scope:	All industrial sectors and critical infrastructure
Technical Scope:	Industrial automation and control systems

Please accept this this response to the Request for Information on the subject Framework for Reducing Cyber Risks to Critical Infrastructure. My responses to the questions posed are based a combination of my role of co-chair of the ISA99 committee on Industrial and Automation Control Systems Security (ISA99) and my personal experience in securing industrial systems in the chemical sector.

Respectfully,

Eric C. Cosman

ISA99 Co-Chair

1 Response to RFI Questions

The following responses represent my *personal* observations and impressions with respect each of the posed questions. Text from the RFI document is shown in *italics.*

1.1 Current Awareness of the Cybersecurity Framework

Recognizing the critical importance of widespread voluntary usage of the Framework in order to achieve the goals of the Executive Order, and that usage initially depends upon awareness, NIST solicits information about awareness of the Framework and its intended uses among organizations.

1. What is the extent of awareness of the Framework among the Nation's critical infrastructure organizations? Six months after the Framework was issued, has it gained the traction needed to be a factor in how organizations manage cyber risks in the Nation's critical infrastructure?

Information about the Framework has been extensively shared and discussed within the ISA99 committee, for the purpose of raising general awareness and determining any implications for the further development of the ISA-62443 series of standards. Our committee consists of over 500 members, representing most major industrial sectors, as well as solutions suppliers, consultants, educators and others with an interest in industrial systems security.

In addition, several sector specific groups and organizations (e.g., The American Chemistry Council) have reviewed the framework and are developing or have developed sector specific guidance dealing with Framework application.

2. *How have organizations learned about the Framework? Outreach from NIST or another government agency, an association, participation in a NIST workshop, news media? Other source?*

The ISA99 committee has included members from NIST almost since the inception of the committee. In addition, several of the leaders of the committee previously participated in related NIST initiatives such as PCSF, as well as government sponsored activities such as PCSRF and its replacement, ICSJWG. The community of people with experience in ICS cybersecurity is still rather small, with the result that most of leaders have worked with each other for several years. This collaboration has extended to the development of the NIST Framework.

ISA99 members have also participated in virtually all of the previous Framework development workshops, under the auspices of the Automation Federation.

Extensive coverage of the Framework in industry press has also led to increased awareness in various sector-specific areas, such as the chemical sector cybersecurity program.

3. *Are critical infrastructure owners and operators working with sector-specific groups, non-profits, and other organizations that support critical infrastructure to receive information and share lessons learned about the Framework?*

The chemical industry has had a cybersecurity program since 2002. This program addresses general cybersecurity issues, as well as those specific to industrial control systems. Consideration of the Framework and its application is currently a major topic of discussion within this group, with a focus on sharing of effective practices.

4. *Is there general awareness that the Framework:*

    a) *is intended for voluntary use?*

In the industry press it appears that there continues to be a misperception that the Framework is "a standard." Despite many attempts to correct this misunderstanding the usage of this term persists. Although standards are typically not mandatory, the use of the term implies a strong push for adoption.

    b) *is intended as a cyber risk management tool for all levels of an organization in assessing risk and how cybersecurity factors into risk assessments?*

This is a matter of awareness and understanding of the nature of the Framework, which generally increases when people actually read the document and try to apply it, as opposed to simply relying on descriptions and other commentary.

    c) *builds on existing cybersecurity frameworks, standards, and guidelines, and other management practices related to cybersecurity?*

This is a matter of awareness and understanding of the nature of the Framework, which generally increases when people actually read the document and try to apply it, as opposed to simply relying on descriptions and other commentary.

5. *What are the greatest challenges and opportunities—for NIST, the Federal government more broadly, and the private sector—to improve awareness of the Framework?*

I believe that awareness and (more important) understanding will increase as the level of adoption and application increases. In other words, rather than simply describing the intended use of the framework we should be describing "real world" applications in the form of case studies.

6. *Given that many organizations and most sectors operate globally or rely on the interconnectedness of the global digital infrastructure, what is the level of awareness internationally of the Framework?*

I believe that in some respects the international awareness may be in fact greater than in the U.S. I have seen several examples of government and industry groups in other countries adopting the same or a similar approach as that used in the Framework to provide very similar guidance that is tuned to their specific situation.

Perhaps the best way to build on this is to promote the Framework and its application through international organizations. This would include standards development organizations (e.g., ISA, IEC), professional societies such as the Automation Federation and IEEE, and industry trade associations, which typically have multi-national or global companies as members.

In the latter example most of the larger multi-national companies are interested in a common approach to ICS cybersecurity throughout their operations, regardless of the country.

7. *If your sector is regulated, do you think your regulator is aware of the Framework, and do you think it has taken any visible actions reflecting such awareness?*

The cybersecurity related regulatory agency for the chemical sector is DHS. It is obvious that they are very aware of the Framework and its intended use.

8. *Is your organization doing any form of outreach or education on cybersecurity risk management (including the Framework)? If so, what kind of outreach and how many entities are you reaching? If not, does your organization plan to do any form of outreach or awareness on the Framework?*

The Automation Federation and ISA have so-sponsored (with NIST) several seminars on the application of the Framework, reaching out to a large number of people and organizations in the process industries.

In the specific case of the chemical sector the American Chemistry Council is currently developing guidance on how to incorporate the Framework into the Responsible Care® security code.

9. *What more can and should be done to raise awareness?*

It is my belief that the level of awareness is not as much of an issue as the level of understanding. (See above comments) Increased understanding will come about as a result of the sharing of case studies and other descriptions of experience in applying the Framework.

If in fact there are still areas where awareness is not at the desired level then methods of increasing it include:

- *Additional information seminars or workshops; preferably not requiring in person participation (i.e., webinars)*
- *Communication via standards development organizations and similar groups*
- *Promotion by sector specific agencies*

1.2 Experiences with the Cybersecurity Framework

NIST is seeking information on the experiences with, including but not limited to early implementation and usage of, the Framework throughout the Nation's critical infrastructure. NIST seeks information from and about organizations that have had direct experience with the Framework. Please provide information related to the following:

1. *Has the Framework helped organizations understand the importance of managing cyber risk?*

Building this understanding has been (and continues to be) a long-term endeavor, specifically as it applies to industrial control systems. Those who design, implement, operate and support these systems already have a well-established and thorough understanding of risk in the broadest sense, since this is a fundamental requirement in successfully controlling what are hazardous and potentially dangerous industrial processes. Our focus has to be on making the connection between cyber risk and process risk by helping people to understand that a different set of threats and vulnerabilities (i.e., cyber) can potentially result in the same consequences with which they are already concerned.

2. *Which sectors and organizations are actively planning to, or already are, using the Framework, and how?*

My personal experience is centered primarily in the chemical sector, and to a slightly lesser extent other process industries such as refining. In these cases I believe that the Framework will play an important role in the relevant cybersecurity related programs.

I have observed a similar emphasis in the Energy sector.

3. *What benefits have been realized by early experiences with the Framework?*

As its name implies, the Framework has provided a useful context for characterizing efforts that may have already been underway. In addition, it provides a valuable means of identifying relevant resources such as standards and recommended practices that describe expectations in specific areas.

4. *What expectations have not been met by the Framework and why? Specifically, what about the Framework is most helpful and why? What is least helpful and why?*

Based on the adoption efforts that I have observed so far the goal of reaching broadly <u>across</u> sectors with common practices based on the framework has not yet been achieved. What I am seeing is that individual sectors are layering additional guidance documents on top of the Framework, explaining what is "special" or unique to their respective environments. This has the approach of creating <u>more</u> guidance material, with the potential to increase confusion.

5. *Do organizations in some sectors require some type of sector specific guidance prior to use?*

See the response to the above question. My personal opinion is that while there are no doubt some requirements and constraints that are sector specific, the number of these has been over-estimated. What does vary from sector to sector is the degree of focus or emphasis placed on specific requirements, constraints, expectations and measures. The essential elements of an effective cybersecurity response are largely sector independent.

6. *Have organizations that are using the Framework integrated it with their broader enterprise risk management program?*

I have very few specific cases on which to base my response. However, in the few examples that I have seen people are viewing the Framework as an element of a planned or existing program.

7. *Is the Framework's approach of major components—Core, Profile, and Implementation Tiers—reasonable and helpful?*

Yes, I believe that this is true in general. However I still have some concerns about the Functions that are identified in the Core (Identify, Protect, Detect, Respond and Recover). The choice of the names for these Functions seems to imply a reactive *response, in the sense that there is an implicit assumption that everything has to be based on a response to something that has already happened.*

8. *Section 3.0 of the Framework (''How to Use the Framework'') presents a variety of ways in which organizations can use the Framework.*

   a) *Of these recommended practices, how are organizations initially using the Framework?*

It is hard to answer this question without benchmarking or research, but my personal expectation is that most people will be drawn to section 3.2 (Establishing or Improving a Cybersecurity Program), either because they are indeed establishing a new program, or because they want to compare the approach already used to the one presented.

b) Are organizations using the Framework in other ways that should be highlighted in supporting material or in future versions of the Framework?

This question is probably better addressed to representatives of sector coordinating councils and sector specific agencies.

c) Are organizations leveraging Section 3.5 of the Framework (''Methodology to Protect Privacy and Civil Liberties'') and, if so, what are their initial experiences? If organizations are not leveraging this methodology, why not?

My personal area of focus is on industrial automation and control systems (IACS) cybersecurity, and there is not a lot of emphasis on privacy and civil liberties when dealing with these systems. For example, industrial control systems typically contain little in the way of personally identifiable information beyond basic access credentials.

d) Are organizations changing their cybersecurity governance as a result of the Framework?

I believe that it may still be too soon to make this determination in a general sense, although I suspect that some changes are being contemplated.

e) Are organizations using the Framework to communicate information about their cybersecurity risk management programs—including the effectiveness of those programs—to stakeholders, including boards, investors, auditors, and insurers?

The typical use of the Framework that I have seen is to impress on stakeholders that the need for an effective cybersecurity response is something that has been identified on a national level.

f) Are organizations using the Framework to specifically express cybersecurity requirements to their partners, suppliers, and other third parties?

Yes, I believe that this is starting to happen and will continue and possibly increase. However, I do not expect to see cybersecurity to be a predominant factor in system selection.

9. Which activities by NIST, the Department of Commerce overall (including the Patent and Trademark Office (PTO); National Telecommunications and Information Administration (NTIA); and the Internet Policy Taskforce (IPTF)) or other departments and agencies could be expanded or initiated to promote implementation of the Framework?

More communication and sharing of real-world examples and case studies, with a focus on benefits gained.

10. Have organizations developed practices to assist in use of the Framework?

Yes, typically at the sector level. An obvious example is the guidance material currently circulating for comment from the Department of Energy.

1.3 Roadmap for the Future of the Cybersecurity Framework

NIST published a Roadmap in February 2014 detailing some issues and challenges that should be addressed in order to improve future versions of the Framework. Information is sought to answer the following questions:

1. *Does the Roadmap identify the most important cybersecurity areas to be addressed in the future?*

This (or any) roadmap has to be a "living document" that changes and evolves over time in response to changing circumstances and evolving requirements and expectations. With that caveat in mind I believe that the current version does an adequate job of identifying next steps in the evolution of the Framework.

2. *Are key cybersecurity issues and opportunities missing that should be considered as priorities, and if so, what are they and why do they merit special attention?*

I have no suggestions for additions at this time.

3. *Have there been significant developments—in the United States or elsewhere—in any of these areas since the Roadmap was published that NIST should be aware of and take into account as it works to advance the usefulness of the Framework?*

The state of the international standards (e.g., ISA/IEC 62443, ISO 27000, etc.) continues to improve and evolve. These developments should be monitored carefully to allow the Framework to be updated if and as required.

In addition, the efforts of the various CI sectors to develop and deliver associated guidance documents should also be monitored. These guidance documents provide an important potential source of practical experience.

Annex

The need for standards specific to Industrial Automation and Control Systems

Overview

Industrial automation and control systems designs increasingly use commercial-off-the-shelf (COTS) technology (for example, network protocols and operating systems) that are inexpensive, efficient, and highly automated, and that can be interconnected in heterogeneous environments. These systems are also increasingly interconnected with non-IACS networks for business reasons. These devices, open networking technologies, and increased connectivity present greater opportunities for cyber attacks against control system hardware and software. These multiple weaknesses can lead to serious or even catastrophic health, safety and environmental (HSE), financial and/or reputational consequences in deployed control systems.

The private sector across the industrial automation landscape (including vendors, integrators, asset owners, ISA and the Automation Federation) is greatly concerned about these weaknesses and vulnerabilities and has been working collectively to provide defensible solutions appropriate to both existing and newly built critical infrastructure. For more than a decade, the ISA99 committee has drawn together leading industrial cybersecurity experts to work within the parameters of a largely volunteer structure to develop the comprehensive strategic architecture of the ISA-62443 series of standards, which have now been recognized by industry worldwide through simultaneous adoption by the International Electrotechnical Commission (IEC).

Organizations choosing to deploy general purpose information technology (IT) cybersecurity solutions to address IACS security may unknowingly expose their systems to significant cyber vulnerabilities arising from a lack of understanding of the highly interrelated and complex nature of IACS networks. While some business IT applications and security solutions can be applied in certain IACS operations, they must be applied in an informed and intelligent way to avoid potentially serious inadvertent consequences. This statement is not simply conjecture, but an established conclusion from, for example, NIST Special Publication 800-82 (June 2011) as well as active research into recommended IACS security practices and associated standards by both government and private industry.

Component Types

Industrial automation and control systems are generally composed of two types of components:

- Information processing elements (e.g., Human-Machine Interfaces (HMI's) and Historians) that are based on commodity operating systems such as Windows®. To a large degree, traditional Information Technology (IT) cybersecurity approaches, with appropriate care, can be used to secure these components. Applying these approaches to a deployed system is expensive, however, as it requires substantial retesting and modifications of operational procedures.
- Field measurement and control devices that generally use real time operating systems. The communication at this level is usually implemented using industrial application protocols. Modern versions of these are based on industry standards such as Ethernet and TCP/IP. Securing these field devices requires a major modification of traditional IT cybersecurity policies, technologies, and testing, and in many areas entirely new approaches are necessary.

> Integration of cybersecurity capabilities has begun for the latest generation of field devices, but devices deployed in the field have a lifecycle measured in decades rather than years. Moreover, many industrial protocols have not yet specified security mechanisms.

Even though some of the technologies used in IACS are similar to those used in traditional IT applications, significant differences in characteristics occur due to the fact that logic executing in an IACS environment has a direct affect on the physical world. The approach used to define IACS cybersecurity requirements thus needs to be based on a combination of functional requirements and risk assessment, often requiring an awareness of operational issues as well.

In most cases, a focus on information protection alone is ineffective when considering IACS security. Control systems rarely store or use Personally Identifiable Information. Direct access to the Internet from a control network is often discouraged or prohibited and E-mail usage is also often restricted or even unsupported. Thus, many of the toughest problems facing traditional IT security can often be effectively mitigated by blocking these types of vulnerable applications and protocols, particularly in those parts of a control system deemed 'critical'.

Security Objectives

A critical requirement of IACS security measures is that they must not have the potential to cause impacts to essential services and functions, including emergency procedures. In contrast, IT security measures as often deployed do have this potential. IACS security goals focus on control system availability, plant safety, plant protection, plant operations (even in a degraded mode) and time-critical system response. General IT security goals often do not place the same emphasis on these factors, typically being more concerned with protecting information than physical assets. This difference in emphasis is often referred to as CIA (confidentiality, integrity, and availability) vs. IAC (integrity, availability, confidentiality).

Understanding this fundamental difference in goals between IACS security and IT security is essential to understanding the need for IACS-specific security standards. This is not simply a matter of semantics, but rather these different goals need to be clearly recognized and stated as security objectives regardless of the degree of plant integration intended and/or achieved. A key step in risk assessment, as required by ISA-62443-1-1, Terminology, Concepts and Models, and ISA-62443-2-1, IACS Security Management System – Requirements, is the identification of which services and functions are truly essential for operations (in some facilities, for example, engineering support may be determined to be a non-essential service or function). In some cases, it may be acceptable for a security action to cause temporary loss of a non-essential service or function, unlike an essential service or function that must not be adversely affected. Additionally, timing is critical for certain control and safety functions. Latency introduced by some IT security solutions, for example, can cause unexpected and adverse control system impacts due to timing delays.

IACS security and Existing Standards

As IACS security requirements are codified, there are a number of common constraints that must be met. Earlier sections have already alluded to a number of them. The result should provide a flexible framework that facilitates addressing current and future vulnerabilities in IACS and applying necessary mitigations in a systematic, defensible manner. It is important to understand that the intention of the ISA-62443 series is to build extensions to enterprise security that adapt the requirements for business IT systems and combines them with the unique requirements for strong availability needed by IACS.

As documented in ISA-62443, an essential function is a "function or capability that is required to maintain health, safety, the environment and availability for the equipment under control." As noted earlier, security measures must not adversely affect essential functions of a high availability IACS unless supported by a risk assessment.

NOTE: In support of this vital point, ISA-62443-2-1 provides guidance on the documentation associated with the risk assessment required to support instances where security measures may affect essential functions.

Based on a risk analysis, some facilities may determine that certain types of security measures may halt continuous operations, but must not result in loss of protection that could result in health, safety and environmental (HSE) consequences. Some specific constraints could include:

- Accounts used for essential functions must not be locked out, even temporarily.
- Verifying and recording operator actions to enforce non-repudiation must not add significant delay to system response time.
- For mission critical control systems with inherently high availability requirements, the failure of the certificate authority or other key management mechanisms must not interrupt essential functions.
- Identification and authentication must not prevent the initiation of safety systems. Similarly for authorization enforcement.
- Incorrectly time-stamped audit records must not adversely affect essential functions.
- Essential functions of an IACS must be maintained if zone boundary protection goes into fail-close and/or island mode.
- A denial of service (DoS) event on the control system or safety system network must not prevent the safety system from actuating as designed.

An IACS rarely operates in isolation from the rest of the enterprise, and thus some essential security functions can be expected to be handled by an external resource. Examples of this might be the maintenance of firewalls and intrusion detection systems by corporate organizations. In addition, in some high resource availability applications, compensating countermeasures external to the control system (such as additional physical security measures and/or enhanced personnel background checks) will be needed. In some cases, a legacy control system that cannot be adequately secured with technology might be made more dependent upon compensating countermeasures such as physical access control and 24/7 staffing and supervision. Sensitivity to lockout or loss of control due to security measures is increased, not decreased, for mission critical control systems. Consequently, a risk assessment which includes noting local operational constraints might result in local relaxation of security controls to enable better availability in combination with enhanced surrounding countermeasures.

Additionally, IACS security clearly is consistent with the business IT security concept of "least privilege". The capability to enforce the concept of least privilege is thus a fundamental requirement of IACS security, with granularity of permissions and flexibility of mapping those permissions to roles sufficient to support it. Individual accountability should be available when required, unless it has a detrimental impact on safety.

Finally, some characteristics of IACS – the deterministic nature, the limited number of users, and the usually dedicated purpose of the system – make the use of certain security measures potentially more feasible and affordable in IACS environments than they are in business IT environments. Specifically, security measures applying anomaly detection and the whitelisting concept can be more appropriate in an IACS environment.