From: **Eric Cosman (OITC)**
Date: Thu, Apr 6, 2017 at 5:29 PM
Subject: [NIST] Comments on NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1
To: cyberframework@nist.gov
Cc: Steve Mustard, Michael Marlowe

Please accept the enclosed comments on the latest revision to the NIST Framework.

Regards,

Eric C. Cosman
Principal Consultant
OIT Concepts LLC

[Attachment Copied Below]

April 6, 2017

National Institute of Standards and Technology
U.S. Department of Commerce

Attention: Cybersecurity and Privacy Applications Group

RE: Comments on Revised Framework for Improving Critical Infrastructure Cybersecurity

To whom it may concern;

Thank you for the opportunity to review the January 2017 revision to the NIST Framework for Improving Critical Infrastructure Security.

The Automation Federation continues to support the Cybersecurity Framework initiative and is actively advocating its adoption within organizations that make up the national critical infrastructure.

We offer the attached comments and suggestions in the spirit of this support.

Sincerely;

Eric C. Cosman
Principal Consultant
OIT Concepts, LLC

Steve Mustard
President and CEO
National Automation, Inc.

COMMENTS

It is gratifying to see that after responding to so many comments and questions, it was possible to retain the original structure and content of the original framework. It is very important to maintain a level of continuity as the document continues to evolve.

The following comments pertain to specific sections of the document.

EXECUTIVE SUMMARY

Although the intent is clearly there for use of the Framework by small and medium-sized businesses, it is not clear that such companies have the resources to interpret and apply it.

Are there specific plans for some sort of structure or mechanism for the sharing of "best practices?"

SECTION 1 – INTRODUCTION

What mechanisms are in place to ensure that NIST is fully aware of updates to industrial and international standards as they occur? The ISA99 committee (responsible for the 62443 standards) maintains formal liaison relationships with several external stakeholders.

SECTION 2 – FRAMEWORK BASICS

Implementation Tiers – There appears to still be some confusion about the terms "tier" and "target profile", and how they are related. The inevitable comparison to maturity levels seems to just further confuse the situation.

The term “cyber supply chain” is referenced in this section, but it has not been formally defined prior to this first use. Please consider some sort of introduction to the term, providing this definition.

Risk Management – The management of cybersecurity risk may be a part of a larger risk management program that addresses all types of risk to the company or organization.

The ISA99 committee will soon be releasing the ISA-62443-3-2 standard, which describes a risk assessment methodology that considers both cybersecurity and process safety for industrial automation systems. When this standard is available perhaps it can be referenced by the Framework.

SECTION 3.2: ESTABLISHING OR IMPROVING A CYBERSECURITY PROGRAM

In step 7, the implementation plan should also include provisions for how to sustain improvements after they have been achieved. In the Six Sigma methodology this is known as the Control phase.

SECTION 3.3: COMMUNICATING CYBERSECURITY REQUIREMENTS WITH STAKEHOLDERS

The increased focus on supply chain risk management is also a welcome improvement. It is very important for asset owners to consider all stages of the life cycle when addressing the security of their systems.

Regarding supply chain risk management (SCRM), the document says (on page 17) “A primary objective of cyber SCRM is to identify, assess and mitigate “products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the cyber supply chain.10.” I would suggest that another key issue with SCRM is to ensure that SCRM members have effective cybersecurity management in place, specifically relating to activities outside of products and services. For instance, does the organization train its personnel to respond correctly to phishing attacks, do they perform background checks on employees and their contractors, are policies in place for handling sensitive information, are policies in place for remote working, etc.

The supply chain concepts can become quite complex, particularly on the supplier side. Identifying a single "supplier" may be an oversimplification. Components can be used to assemble products, which can then be combined in an integration process to create solutions.

SECTION 4 – MEASURING AND DEMONSTRATING CYBERSECURITY

Measurement and Metrics – There is considerable interest in the subject of metrics, and both the ISA99 committee and IEC have considered efforts to define measures for compliance to the relevant standards. However, end users need metrics and measures that are simpler and more directly applicable to specific implementations.

RESPONSES TO SPECIFIC QUESTIONS

The draft document posed several specific questions to aid reviewers in preparing their response. The following are replies to those questions.

1. *Are there any topics not addressed in the draft Framework Version 1.1 that could be addressed in the final?*

   The addition of section 4.0 on measurement is a positive addition to the framework. It would be worthwhile to consider extending this to include the use of independent certification tools and methodologies.

2. *How do the changes made in the draft Version 1.1 impact the cybersecurity ecosystem?*

   The additions and changes should serve to broaden adoption and application of the framework.

3. *For those using Version 1.0, would the proposed changes impact your current use of the Framework? If so, how? For those not currently using Version 1.0, does the draft Version 1.1 affect your decision to use the Framework? If so, how?*

   See answer above.

4. *Does this proposed update adequately reflect advances made in the Roadmap areas?*

   Yes, several specific items in the roadmap have been addressed. We encourage continuation of the roadmap approach to defining future areas of opportunity.

5. *Is there a better label than "version 1.1" for this update?*

   "Version" numbers are typically applied to software. Consider the use of editions, rather than versions, since this is more common for recording changes to documents (i.e., first edition, second edition, etc.)

6. *Based on this update, activities in Roadmap areas, and activities in the cybersecurity ecosystem, are there additional areas that should be added to the Roadmap? Are there any areas that should be removed from the Roadmap?*

   We have no specific suggestions at this time.