From: Patrick Coyle
Sent: Saturday, December 09, 2017 2:45 PM
To: cyberframework <cyberframework@nist.gov>
Subject: CSF Revision Comments

The attached comments were originally published in the Chemical Facility Security News blog on December 9th, 2017.

[*Attachment Copied Below*]

NIST Publishes 2nd Draft for CSF 1.1 for Comment

This week the National Institute of Standards and Technology (NIST) published their second draft of version 1.1 of the Cybersecurity Framework (CSF) and a fact sheet that broadly outlines the changes made to the CSF.

The fact sheet makes the point that the revised CSF is applicable to information technology, operational technology, cyber-physical systems, and internet of things. Since the original CSF core already provided references to ISA 62443-2-1:2009 and ISA 62443-3-3:2013 that are found in this revision it does not seem that the new version changes much with respect to OT/IOT security.

OT/IOT Changes

In fact, if you look at the list of changes made to the CSF (starting at page 50) there are only four references to OT/IOT changes:

> • Section 1.0 (pg 7): ‘Framework Introduction’ was updated to reflect security implications of a broadening use of technology (e.g. ICS/CPS/IoT) and to more clearly define Framework uses;
> • Appendix C (pg 53): ‘Acronyms’ - was modified to include CPS - Cyber-Physical Systems;
> • Appendix C (pg 53): ‘Acronyms’ – was modified to include IoT - Internet of things;
> • Appendix C (pg 53): ‘Acronyms’ - was modified to include OT - Operational Technology

The introduction section discussion referenced above addresses OT/IOT security issues this way:

> “The critical infrastructure community includes public and private owners and operators, and other entities with a role in securing the Nation’s infrastructure. Members of each critical infrastructure sector perform functions that are supported by the broad category of technology, including information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), and connected devices more generally, including the Internet of Things (IoT). This reliance on technology, communication, and interconnectivity has changed and expanded the potential vulnerabilities and increased potential risk to operations. For example, as technology and the data it produces and processes is increasingly used to deliver critical services and support business decisions, the potential impacts of a cybersecurity incident on an organization, the health and safety of individuals, the environment, communities, and the broader economy and society should be considered.”

Unfortunately, the terms ‘CPS’ and IoT are not used in the revised CSF Core. In short, the CSF does not specifically address the specific cyber-physical consequences of security breaches in OT/IoT systems.

Suggested OT/IOT Changes

Unfortunately, this revision to the CSF still does not adequately address the potential cyber-physical consequences of a cybersecurity incident. At a minimum, the core should have an additional subcategory under Risk Assessment:

> ID.RA-X: Worst-case cyber-physical events need to be identified that effect either on-site operations and/or the off-site community.

This would then lead to requiring an additional Risk Management Strategy subcategory:

> ID.RM-X: Appropriate emergency response agencies are notified of potential off-site community effects of cyberphysical incidents.

The on-site effects on operations would be addressed by the current IR.RM-4. To clarify that addition, I would reword the subcategory title to read: “Potential business impacts (including on-site and off-site effects of cyber-physical incidents) and likelihoods are identified.”

Broadening Information Security Focus

While the verbiage in the introduction to the CSF would indicate that NIST intends to broaden the focus of CSF to include OT/IoT security, there are still a number of references to ‘information security’ in the CSF core that really should be revised to indicate that broadened focus. For example ID.GV-1 still refers to ‘information security’ when the intent should reflect a broader ‘cybersecurity’; the words should be changed to reflect this. Similar wording changes need to be made to ID.GV-2, ID.SC-3, PR.AT, and PR.AT-5,

Public Input

NIST is asking for public input on this second draft for CSF 1.1. Comments need to be submitted by January 19th, 2018. Comments can be submitted by email to cyberframework@nist.gov.

http://chemical-facility-security-news.blogspot.com/2017/12/nist-publishes-2nd-draft-for-csf-11-for.html 12-09-17