From: David Kuipers
Sent: Tuesday, March 14, 2017 12:54 AM
To: cyberframework
Subject: Comments on Draft V. 1.1 of Cybersecurity Framework

To Whom it May Concern,
I'm not sure if you need my credentials in this process:
I work as a Cybersecurity Assessor for the DHS ICS-CERT Assessment program at the Idaho National Laboratory and have 40 years experience encompassing ICS operations (nuclear), ICS design (nuclear, electrical, water), and ICS CI/KR Cybersecurity. I was program manager for the DOE-OE NSTB/CEDS R&D program at INL for 7 years.

In reviewing the draft v. 1.1 of the framework, I noted the absence of cyber or related security cross-organizational tabletop exercises to test detection, response, cross-organizational understanding, procedural validation, communications plans and backup contact awareness, inter-dependency discussion and provide lessons learned feedback to improve the process, plans and procedures.

Note: this is considered as Moderate and High in priority and baseline allocation in IR-3 Incident Response Testing in NIST-800-53r4 and that only referencing coordination with related plans, however in evaluating the considerable value that the process brings to operational technology organizations and their integration into the overall business or information technology organizations, I feel it is essential in all organizations to leverage to improve communications and broaden organizational cybersecurity awareness and collaboration. I have recommended this to many entities to support better OT organization involvement in the business incident response planning.

Sincerely,

David Kuipers, CISSP