Subject: Opposition to Supporting Recommendation 3.7 on the SRMAs and "voluntary" performance metrics

Date: Monday, September 25, 2023 at 12:17:01 PM Pacific Daylight Time

From: Mike Bergman

To: Benson Chan, Dan Caprio

CC: Ann Mehra, ashehabi@lbl.gov, datadiva@debbiereynoldsconsulting.com, debra.lam@innovate.gatech.edu, Kevin.Kornegay@morgan.edu, maria.rerecich@consumer.org, nick.e@cropx.com, Nicole.Coughlin@carync.gov, pete@dotsandbridges.com, ranveer@microsoft.com, robby.moss@gmail.com, Steve.Griffith@Nema.org, tomkat@archon-ds.com, Barbara Bell Cuthill (barbara.cuthill@nist.gov), Jeffrey Brewer, greg.witte@hii-tsd.com

Benson and Dan,

Regarding this proposed Supporting Recommendation:

> **Supporting Recommendation 3.7**: The Sector Risk Management Agencies (SRMAs) should collaborate with sector partners and develop IoT performance metrics intended to strengthen critical infrastructure security and resilience.
> The expansive development and adoption of IoT assets and systems should map to IoT performance metrics intended to strengthen critical infrastructure security and resilience. Agency Chief Technology Officers and other officers and associated program offices could serve as the nexus for convening peer stakeholders. Performance metrics will need to be defined in conjunction with owners/operators of critical infrastructure assets/systems (both Information Technology (IT) and Operations Technology (OT)). The Board also recommends that the SCO in each agency will participate in a Community of Practice, like the Federal Chief Information Officer (CIO) Council format, which, in turn, will serve to convene officers across all agencies.

I oppose including this Recommendation in the IoTAB report. The SRMA for the IT and Communications sectors is CISA. That agency's history of "performance goals" in cybersecurity over the past year has left industry leery of such efforts, for reasons outlined below. We have experience; CISA initially drafted Critical Infrastructure performance goals that were without real-world input and that were disconnected from relevant NIST work. Lack of industry or NIST SME input was mitigated after a significant pushback from industry, but CISA then developed Secure By Design in a similar non-transparent way. So having a SRMA develop "voluntary" performance metrics is of concern. Here is additional information.

1. **CONFLICTING AGENCIES:** The process that is currently working has NIST developing outcome-based frameworks, not performance goals or metrics. For another agency to set voluntary performance goals means setting up a competing project.
2. **OUTCOMES NOT METRICS:** When metrics are established by fiat—by agencies, by the Hill—the results are often unrealistic and unworkable. For example, a typical "performance goal" we saw in Critical Incident Reporting over the past two years was, *"report all cybersecurity incidents within 72 hours"*. There are multiple reasons such a goal weakens industry's ability to respond to such incidents, such as the word "all" (an ISP may have 1000 minor incidents per day!), or the fact that confidentiality may be requested by DoJ or DoD officials as they seek the perpetrators, and more. Outcomes, which are one step removed from metrics, can be understood appropriately by different sectors with different requirements. Outcomes, rather than metrics, should be the focus.
3. **NOT VOLUNTARY:** The existing (critical infrastructure) "voluntary" performance goals have already found their way into draft legislation as mandates. It is ingenuous to believe that new metrics modeled on this approach would be "voluntary" for very long.
4. **REDUNDANT WITH THE CYBER TRUST MARK:** The NIST-managed multi-stakeholder process that

has led to the U.S. Cyber Trust Mark is already moving the consumer technology world. It is being cloned for other sectors. New metrics that are developed disjoint from this process is the wrong approach.

The idea of the SRMAs developing performance metrics is not salvageable with new wording. For this reason, and the above reasons, I propose deleting this draft recommendation from the draft IoTAB report.

Best Regards,

Mike Bergman
Vice President, Technology & Standards
Consumer Technology Association, producer of CES®
m: +1(609) 865-4402
@mbergman42
CTA.tech | CES.tech