From: "Chaillan, Nicolas (CTR)"
Date: Jan 30, 2017 10:45 AM
Subject: RE: Comments on Cybersecurity Framework v1.1 draft
To: "cyberframework@nist.gov" <cyberframework@nist.gov>
Cc:

One additional comment:

Link www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf added to v1.1 is 404.

Nicolas M. Chaillan
Cyber Security Division
Science & Technology Directorate
Department of Homeland Security

From: Chaillan, Nicolas (CTR)
Sent: Monday, January 30, 2017 10:44 AM
To: 'cyberframework@nist.gov' <cyberframework@nist.gov>
Cc: Douglas Maughan (Douglas.Maughan@HQ.DHS.GOV) <Douglas.Maughan@HQ.DHS.GOV>; Teresa Burt (CTR) (teresa.burt@associates.hq.dhs.gov) <teresa.burt@associates.hq.dhs.gov>; Collins, David (CTR) <david.collins@associates.hq.dhs.gov>; Garwood, Chase <Chase.Garwood@hq.dhs.gov>

Subject: Comments on Cybersecurity Framework v1.1 draft

Hello,

I wanted to provide some (hopefully helpful) feedback on the recent changes on v1.1 and some potential additional changes:

- ID.SC-1 might consider adding “Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders **into a Cyber Supply Chain Risk Management Plan**.

- Isn’t PR.AC-4 now a duplicate or redundant with ID.SC-3?

- I believe we need to address “Data in Use” with a new PR.DS. For example, database data is usually considered in use when the database is running (and not at rest) and its encryption can be critically for classified data (good example with the OPM breach).

- **PR.IP-4:** Backups of information are conducted, maintained, **secured** and tested periodically. Securing the backups are critical (back to PR.DS)

- **PR.IP-6:** Data is destroyed according to policy **and relevant regulations.** Policies sometimes aren’t well updated and checking current regulations is critical as they changed often per state.

- **I see multiple vulnerability management/scans subcategories.** I’m wondering at what point if should be unified and implemented into asset management instead? (PR.IP-12, CM-8). I understand the difference between management and scans but seems redundant anyway.
- **PR.PT-1:** should we add something regarding integrity and monitoring of the logs?

- Isn’t PT-3 redundant with IP-1?

- **DE.CM-1:** The network is **continuously** monitored to detect potential cybersecurity events
- DE.CM-4 is very vague… maybe way too much to be properly implemented?
- RC.CO-2 is almost always impossible to assess. Might want to add “when possible”

Thank you.

Nicolas M. Chaillan
Cyber Security Division
Science & Technology Directorate
Department of Homeland Security