Hello,

Please find below my comments on the document.

Best Regards,
Dr. Cédric Lévy-Bencheton

--
Founder
Cetome – IoT Security and Privacy

1. Page 9 – Ecosystem

- Several “IoT-specific” networks are omitted from this definition be they LPWAN (SigFox, LORAwan) or PAN (Zigbee). They can be compromised either through physical proximity or remotely to compromise a system. This is even more true in industrial control systems where several connected devices rely on proprietary radio protocols connected to a base-station that would be connected over IP. Compromising this radio link (due to the lack of authentication and/or encryption) would lead the system to eavesdrop or inject fake data with a potential impact on mission-critical services.

2. Page 9 – Technical domains:
   Please add education and awareness. There should be a training at school to raise awareness at kids and teachers. This is critical in the light of IoT devices targeted to kids (toys and tracking devices). This would go on top of a public-private partnership to raise awareness towards adults.

3. Page 13 - A Vision for the Future of Enterprise Networks
   a) Identify: the remediation is not realistic. It might be easier to find solution to clearly identify and mitigate threats posed by (potentially) vulnerable IoT devices by isolating them on a separate network and monitoring this network (or use a whitelist). There is currently no easy way to identify/authenticate IoT devices (PKI is not a solution). Some solutions are in development but will require acceptance by the industry.
   b) Recover: it is currently difficult to recover a compromised IoT system, in particular when sensors are bricked. I agree with you that the solution would be to have vendors allow configuration export and easy reconfiguration from a trusted host, preferably local. I would suggest to highlight that restoring from the Cloud might be more risky, as it could be one main attack vector.

4. Page 15 – Edge devices
   Edge devices usually do not implement any kind of end-to-end encryption nor authentication (or basic). They also may rely on obsolete or insecure radio communication protocols. This could lead to manipulating a system (which could be more damaging than creating a Botnet). This could be one of the key areas for improvement.

5. Page 17 - Vision for the Future of Edge Devices

End-of-life should provide a way to reset the device to factory settings and delete all data from the device (and potentially the Cloud).

6. Page 23 – goal 1, Action 1.1
   There should be a baseline for IoT security that applies to ALL IoT devices. There should also be complementary sectorial baselines that would add minimum requirements adapted to the domain (e.g. healthcare and railway have different security requirements) .

7. Page 33 – Goal 4, Action 4.2
   The objective is to harmonize these guidelines/frameworks in order to make it easier to choose. This would also limit guidelines negating each other. Indeed, it is easy to do nothing whenever there is no choice, yet it becomes very difficult for non-experts to choose from two or more competing guidelines: they would rather do nothing than redo everything once again if the chosen "standard" is not the right one. Moreover, many guidelines are overlapping and need coordination. Governmental bodies (who are neutral) could lead this harmonization effort.

8. Page 35 – Goal 5, Action 5.1
   Ideally, this would be the role of an IoT-ISAC. This could be supported by the government.

9. Page 36 – Goal 5, Action 5.2
   There are already private and public initiatives on an IoT Trust label at EU and international level. There should be a coordination on which metrics to use and how this label works. For instance, such a label would need to be updated for products that have been sold before a new vulnerability is discovered (think OpenSSL heartbleed). This could be linked to Action 5.1. The Label shall also be clearly an incentive for buyers to select the device with the most adapted security to their concerns.