The following comments are the result of a cooperative review of the IoT Trust Framework document done by Wesley George, Chris Roosenraad, and Robert Seastrom, all of Time Warner Cable, 13820 Sunrise Valley Drive, Herndon, VA 20171. These comments reflect the opinions of the individuals listed here, and do not represent an official Time Warner Cable position on this document. Questions and comments on specific items can be emailed to wesley.george@twcable.com

Feedback on specific items in the proposed minimum requirements:

#1,2 – Changes to these policies should be highlighted prominently, and previous versions of the policies should remain publicly available for comparison

#3 – disclosure should include a discussion of whether the manufacturer makes reasonable effort to anonymize this data before storing, analyzing or sharing it, or why this is not possible. It may be appropriate to cite (or develop, we are unaware of any existing ones) specific best practices for anonymization of PII in such a way as to render it as useless as possible for correlation to specific individuals, while maintaining the ability to draw aggregated conclusions from it.

#4 – include a recommendation to explicitly publish the names and contact info for third parties with whom this information is being shared, as well as pointers to those third parties' privacy, security, and data retention policies if applicable to the data being shared. In addition to nature and scope of data shared, manufacturers should disclose their purpose in sharing the data. Similarly to #1,2 above, there should be a method to highlight changes and display history so that as third party partners change, the information stays current and publicly available. There is a large difference between sharing data with third parties for marketing purposes and sharing data with third parties for them to provide an integral part of the service being offered. This is too ambiguous as currently written because it does not make that distinction. This item should probably also discuss legal liability, as "responsibility…to manage their third party service providers" is too ambiguous. Should it be contractual, with penalties if the terms are violated? Does liability transfer if a third party violates terms, or does this imply that liability remains with the manufacturer? The only way to make most companies take security and privacy seriously is if they believe that they have some legal liability to protect against.

#5 – discuss specifics around which information is retained and why. Different types of information have differing levels of sensitivity and different uses, and thus customers may have differing expectations on the duration of retention, effort made to protect and anonymize the data, etc.

#7 – I recommend removing the "would not apply to direct wired connections" exception. While there are many situations where the assumption can be made that a wired connection is more secure than a wireless one, there is wide variability in networking such that a wired connection may well use one or more insecure

wireless elements after it has left the device before it gets to its end destination, and assuming that just because the device only has wired connectivity this obviates the need for proper encryption of data is not something manufacturers should get in the habit of doing. Alternatively, the language could be clarified to reflect the fact that the wired connection being referred to is not a networking connection, but something that connects the device to another more capable device where encryption would be implemented, e.g. USB, but even in this case, the document is recommending elsewhere that any data stored on the device should be encrypted, so it makes little sense to decrypt it before sending it across a USB cable in order to re-encrypt it.

#9, 10 – While the terms are often used interchangeably, SSL refers to a specific technology, which is generally deprecated in favor of TLS, so the language should be updated accordingly. https://tools.ietf.org/html/rfc7568
Additionally, there is a lot of overlap in the recommendations between these two items, with the main distinction being user site vs cloud. These should probably be merged into a single requirement for pervasive transport layer encryption, with appropriately time-scoped periodic reviews to make sure that they still "score a minimum of 90% using industry benchmark testing tools" (like other points, semi-annually seems good).

#11 – some sort of recommendation as to what the minimum acceptable level of penetration testing can be, along with a reference to a best practice penetration test for different classes of devices and services might be helpful here. A bug bounty program (see discussion below on responsible disclosure) would be a useful augment to penetration testing.

#12 – there needs to be specific language that security and privacy updates should be provided for the expected lifetime of the device, not simply until its warranty period lapses or until the device is discontinued (no longer sold) by the manufacturer. This is briefly discussed in #21, but that discusses the need to tell customers what the policy is, rather than making a recommendation on what the support policy should be.

#13 – if there are third parties involved as in #4, that plan should include all relevant third parties.

Additional recommendations section:
#1 – Recommend that this is binding on successors, heirs, and assignees.
#7 – While IPv6 is well beyond the “evolving” standards category now, it may be appropriate to specifically mention it, as IPv6 comes with unique challenges to security and privacy that must be considered in this framework.

General comments not on specific recommendations –

Lawful intercept/LEA cooperation – many companies are publishing specific details about the terms under which they will share a customer's information with Law Enforcement, including periodic reports on the number of LEA information requests received and complied with, or a "warrant canary" to confirm that none have been received. Since providing information to law enforcement in the age of pervasive monitoring is often viewed to be a privacy consideration, a discussion of this within the IoT trust framework is appropriate.
Examples:
Google Transparency Report:
https://www.google.com/transparencyreport/userdatarequests/legalprocess/
Twitter Transparency Report:
https://transparency.twitter.com/
Time Warner Cable Transparency Report: http://help.twcable.com/privacy-safety.html
CanaryWatch – looks in transparency reports for Warrant Canaries
https://canarywatch.org/
See also IETF RFC 7528. https://tools.ietf.org/html/rfc7258

Responsible Disclosure – Companies should have a publicly visible and easily located method for security researchers and other external organizations not otherwise affiliated with the company to privately and responsibly disclose vulnerabilities to the manufacturer. This should be accompanied by a public policy for how these reports are analyzed and resolved including such things as the requested timeframe to provide an update before public disclosure (i.e. how long does a manufacturer need after a vulnerability is disclosed privately to issue a patch so that it can be issued before the vulnerability is publicly disclosed). Similarly, the policy should include active follow-up with the reporting party to prevent premature public disclosure. This could be managed in conjunction with either a standalone bug bounty program, or a cooperative program such as https://hackerone.com.

Examples of responsible disclosure policies:
Microsoft: Report a Computer Security Vulnerability
https://technet.microsoft.com/en-us/security/ff852094.aspx
Google Report security issues
https://www.google.com/about/appsecurity/
Facebook
https://www.facebook.com/whitehat
ZDI Disclosure Policy
http://www.zerodayinitiative.com/advisories/disclosure_policy/

Third party hardware and software sources – Few companies develop all of their hardware and software in-house. Many systems and features incorporate libraries, software packages, and chipsets from OEMs and other third parties e.g. web servers, OS Kernels, chipset drivers, etc. This document could use some discussion about ensuring that source libraries and tooling are using the most up to date versions. Many of the recent IoT security breaches are taking advantage of old vulnerabilities

in component libraries that were exposed and fixed long ago, but are still present because manufacturers used downrev versions of these libraries, sometimes years out of date and obsolete before the device was ever shipped. Best practice needs to include an evergreen model to update the component parts to the systems and the tooling to manage them, especially when sourced from third parties.

Long-term (indefinite) support model- also as with #12 above, it may be appropriate to recommend a long-term support model, including, at a minimum, code escrow and a succession plan should the company fail. Another model to recommend may be one that open-sources the code and libraries so that if the manufacturer has not failed, but no longer wishes to provide security and privacy fixes, a community of interest within the open source community could assume this role.