My name is Spencer Chan and I am a student at the University of Maryland.

I mostly agree with the criteria proposed in the consumer cybersecurity label draft [1].

I think an additional criteria should be added, and that is the software license. At minimum the user should know: is the software free (as in freedom) or proprietary? Is it open source or not? (Open source and free software are not the same thing [2]) Users should be informed of this because security best practices and responses can differ between these licenses models. In the case of open source software, users also have the opportunity to inspect and audit the software themselves. This also informs the users of the rights they may have with free software ("to run, copy, distribute, study, change and improve the software" [3]) and the rights they may (not) have with nonfree software (namely the right to not reverseengineer the software, etc).

Additionally I hope that NIST may work to standardize software labels.
Leaving software manufacturers to provide their own labels gives them the possibility to lie or otherwise misrepresent various elements of the software. For example, a software company could claim to use encryption, but the specific algorithms they use have been shown to be insecure (eg AES with ECB mode [4] or salted MD5 passwords [5]). Or the company could have rolled their own crypto algorithms which is potentially risky [6], and users would never know. Users need to be guarded against attempts like these.

Thanks,
Spencer

Sources

1. https://www.nist.gov/document/draft-baseline-criteria-consumer-software-cybersecurity-labeling
2. https://www.gnu.org/philosophy/open-source-misses-the-point.en.html
3. https://www.gnu.org/philosophy/free-sw.html
4. https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Electronic_codebook_
5. https://security.stackexchange.com/questions/19906/is-md5-considered-insecure
6. https://security.stackexchange.com/questions/18197/why-shouldnt-we-roll-our-own