From: John Diamant <john.diamant@gmail.com>
Sent: Monday, October 18, 2021 6:24 PM
To: EO-pilots
Cc: John Diamant
Subject: feedback on DRAFT Baseline Security Criteria for Consumer IoT Devices (submitted by
Oct. 18th deadline stated in NIST URL)

Note that while the draft itself states the deadline for feedback is Oct.
17th, https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/iot-device-criteria
originally and continues to explicitly state: "Comments on the draft white paper are due no later than
October 18, 2021". Therefore please accept and treat these comments as on time within the NIST
published deadline as they are within the deadline from the above NIST-published web page (e.g. no
later than Oct. 18th). Thank you for soliciting important comments to improve this effort.

The Baseline Security Criteria for Consumer IoT Devices is a good initial draft, and the work NIST is
leading around the EO is critically important to addressing major security issues in IoT, critical and
consumer software, so thank you!

Below are my key comments.

1) Product Security (in both Tables 1 and 3): seems weak/incomplete. There is much to product security
and the criterial covers a very small percentage of it. These sections warrant beefing up to more
robustly reflect product security.
2) Documentation: 5e (Secure software development and supply chain practices) and 7 (Secure System
lifecycle policies and processes) needs to reference something robust and complete, such as the recently
published NISTIR 8397: Guidelines on Minimum Standards for Developer Verification of Software. In
other words, it's important to document relative to a standard so it is clear what minimum verification
has been done and what has been skipped - as all skipped verification represents a substantial
probability of insecurity (anything left untested likely has vulnerabilities).
3) While Documentation itself may not be part of the technical criteria, NISTIR 8397 specified developer
verification is technical and it is critical that it be included as part of the IoT security label (e.g.

"Criteria for the Label") – in other words, security features do not define security of the IoT product,
without the assurance/verification that goes with it, so that must be an essential part of the label. So
the label criteria must include the degree of conformity to NISTIR 8397 or something along those lines
or it will result in a false sense of security.
4) While my submitted position paper – Labeling Software to Dramatically Reduce Vulnerabilities was
primarily in response to software labeling, it applies equally to IoT security labeling. In it, I describe a
tiered approach along the lines referenced in the "Increasingly Comprehensive Levels of Testing and
Assessment (Tiers)" section of the Baseline IoT draft (see the 5-star labeling scheme I describe in my
above-linked position paper).

Thank you for your consideration, and best regards,

John Diamant, CISSP, CSSLP
founder of the secure development program for the largest technology company at the time (HP,
prior to its
numerous divestitures and splits), acknowledged by name for ìsignificant comments and
suggestions, which
greatly improvedî NISTIR 8151, ìDramatically Reducing Software Vulnerabilities: Report to the
White House
Office of Science and Technology Policyî, briefed senior staff of a Joint Congressional
Subcommittee on software
security, presenter at numerous conferences, and co-inventor on 11 issued patents (most security-
related).