From: IAB Executive Administrative Manager
To: iotrfc2017
Cc: iab@iab.org
Subject: Internet Architecture Board Comments to United States National Telecommunications and Information Administration (NTIA) on the Green Paper: Fostering the Advancement of the Internet of Things
Date: Thursday, March 02, 2017 3:08:58 PM

Internet Architecture Board Comments to United States National Telecommunications and Information Administration (NTIA) on the Green Paper: Fostering the Advancement of the Internet of Things that was released on January 12, 2017.

The Green Paper can be found on the NTIA website at <https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf>.

The Request for Comments [Docket Number 170105023-7023-01] on the Green Paper can be found at <https://www.ntia.doc.gov/federal-register-notice/2017/request-comments-benefits-challenges-and-potential-roles-government>.

The Internet Architecture Board is chartered with a responsibility to, among other things, "pay attention to important long-term issues in the Internet, and to make sure that these issues are brought to the attention of the group(s) that are in a position to address them. It is also expected to play a role in assuring that the people responsible for evolving the Internet and its technology are aware of the essential elements of the Internet architecture." (RFC 2850, "Charter of the Internet Architecture Board (IAB)," which can be found at <https://www.rfc-editor.org/rfc/rfc2850.txt>.)

In accordance with that role, the IAB is pleased to be able to respond to the National Telecommunications and Information Administration request for comments, offering a few observations, comments, and suggestions. These remarks are focused on three topics: Privacy, cryptographic algorithms, and software update.

PRIVACY

Section B.ii of the Green Paper is about privacy. The section covers many privacy issues thoroughly, but the IAB would like to draw attention to an aspect of privacy that was not covered. Privacy concerns in the Internet are not merely with those who own the devices and run the applications in the network. They are also affected by government policies and practices, for instance on pervasive monitoring of Internet traffic by some governments. We refer to the IETF statement on pervasive monitoring, RFC 7258 <https://www.rfc-editor.org/info/rfc7258>, for which the IAB has provided additional context in RFC 7624 <https://www.rfc-editor.org/info/rfc7624>. Although these documents discuss privacy concerns around pervasive surveillance in general, any privacy-sensitive information in IoT systems would be vulnerable to the effects of pervasive monitoring.

CRYPTOGRAPHIC ALGORITHMS

Section B.i.5 of the Green Paper covers some Technical Limitations regarding Cybersecurity. This section should strongly discourage the use of non-standard encryption algorithms or integrity protection algorithms.

SOFTWARE UPDATE

Section B.i.3 of the Green Paper discusses patching. Software updates need to be authenticated and integrity protected, and in many cases the IoT device owner needs to authorize them. Consumers want to have a means to continue to update the IoT device software even after a vendor goes out of business or abandons the product.

Section B.iii.1 of the Green Paper discusses Copyright. This section should point out that software copyright is another obstacle for a consumer to create software updates after a vendor goes out of business or abandons a product.

Section B.v.1 of the Green Paper talks about Current Initiatives, including the NTIA Cybersecurity Multistakeholder Process, which seems to focus on consumer awareness and understanding. We are pleased to find that this section recognizes that consumers will need assistance with products that are no longer supported by the vendor that produced them:

> Devices that consumers continue to use to connect to the Internet should be updated and protected even if device manufacturers discontinue them. There should be some mechanism (such as transferring the needed software keys to a designated consortium) for ensuring that devices function with the software updates needed to ensure security.

Some procurements require the vendor to place the source code for their product in escrow, and then if the vendor goes out of business or abandons the product, the software is released. This practice could be extended to include the cryptographic keys needed to authenticate and integrity protect software updates.