Capabilities and Expectations Working Group

NTIA Multistakeholder Process

on IoT Upgradability and Patching

April 26, 2017, Meeting

WG2 Background

- Desired Outcomes:
  - A shared understanding of the component steps in an update, including a baseline for security purposes
  - A mapping between the steps of an update and the necessary technical capabilities of the device and its supporting systems

- Goals and audience
  - Voluntary, nonregulatory guidance
  - Update mechanisms should not introduce new security risks
  - Aimed at IoT manufacturers, solution implementers, system integrators, and those who deploy and maintain systems

- Scope: Connected, remotely addressable devices (as opposed to non-connected devices)

WG2 Summary of Activity

- Reviewed a wide range of device categories, capabilities, and use cases
- Reviewed/discussed several update mechanisms (both automated and human-intervening)
- Mapped out the necessary steps of a generalized update process, including basic and use-case specific steps
- Key Findings:
  - There is no one-size-fits-all model.
  - However, we can sketch out the components of a update that fits the general case.
  - Different use cases and security contexts will have different security needs and specific additional features of a update.

Basic and Use-Case Specific Update Scenarios

- We attempted to establish what might be seen as the minimum for a generalizable update, described in the first table on the handout
- Discussions are driven by use cases
- Some use cases will need further steps, which we lay out in the second table
- How this will be used
  - By themselves: steps understood as a baseline for updates
  - Mapping between the components and technical capabilities

- *Do you agree with the designations?*
- *What are we missing?*
- *What are the appropriate next steps?*