NTIA Multistakeholder Process on IoT Upgradability and Patching
Capabilities and Expectations Working Group
For Discussion: Components of an Update

Common for All Use Cases	
Components	**Technical requirements of each step**
Update is prepared	Size of memory
Update is signed by vendor or trusted party	Cryptographic operations vary by implementation
Transmit the updated code	Method of secure transmission
Verify the signed update • Including verification that it is not a downgrade attack	Cryptographic operations vary by implementation
System/User Awareness of update on device	Defined, technically enforced policy of when update is applied Can trigger local automatic process or require user involvement
Trigger update process	Root of trust: Only a special subset of code can trigger a SW update
Apply update step	
Post-update verification	Further storage & state capabilities (but could be lightweight, w/ just a checksum)
Activate new code, portions of code, or components	May require rebooting / reset / restart Possible secure boot Alternatively, could reload individual processes without a reboot In service software update

DRAFT
April 26, 2017

NTIA Multistakeholder Process on IoT Upgradability and Patching
Capabilities and Expectations Working Group
For Discussion: Components of an Update

Possible Additional Components by Use Case	
Components	**Technical requirements of each step**
Encrypt update	
Validate source	PKI
Validate endpoint	PKI
Decrypt update	Keys to decrypt, secure memory in which to decrypt & store update See NIST 800-147 for handling
Re-validate/check update prior to application, but within the root of trust code	
System checks update for validity/size/other constraints	
System documents pre-update state	Storage of state beyond that which is to be updated
System documents persistent, non-volatile data	
Potential fall back to the last known good state	State & storage
Post-update testing	
Update, convert, and integrate persistent data	
Post-processing messaging and verification (internal, component-to-component)	
Post-process messaging (external) • Local area network or initial vendor	Communication and global state information for versioning, etc.

DRAFT
April 26, 2017