Encryption Update

Information Technology Controls Division

Recent Changes

- 2017
  - 5A002 was restructured for readability – classifications changed from 5A002a.1 to 5A002.a
  - Note 4 was re-written into positive text
  - Technical note added defining 'cryptography for data confidentiality' and 'in excess of 56 bits of symmetric key length or equivalent'
  - Decontrol note j for dormant encryption was removed and new language added to the chapeau of 5A002.
  - Subparagraphs restructured so that all 5x002.b paragraphs are for encryption license keys

Recent Changes

- 2018 – Dormant Encryption
  - Changed the wording of the chapeau addressing dormant encryption
  - Changed the wording of 5x002.b for the encryption license keys
  - No change in scope of the controls

Bureau of Industry and Security
BIS 2019 | ANNUAL CONFERENCE ON EXPORT CONTROLS

Recent Changes

- 2019
  - Added a control on post-quantum cryptography
  - Added a decontrol note on certain IOT devices
  - Revised the text on dormant encryption yet again

Deemed Exports

- Increased scrutiny of deemed exports
- Specify ECCNs to the sub-paragraph level and provide justification
- Have a comprehensive Technology Control Plan (TCP) and supplement it as needed
- Provide technology roadmap and business plan updates as needed.

Bureau of Industry and Security
BIS 2019 | ANNUAL CONFERENCE ON EXPORT CONTROLS

Post Quantum Cryptography (PQC)

- ***"Asymmetric algorithm" where the security of the algorithm is based on any of the following:***
  - ***Shortest vector or closest vector problems associated with lattices (e.g., NewHope, Frodo, NTRUEncrypt, Kyber, Titanium);***
  - ***Finding isogenies between Supersingular elliptic curves (e.g., Supersingular Isogeny Key Encapsulation); or***
  - ***Decoding random codes (e.g., McEliece, Niederreiter).***

Technical Note

May be referred to as being post-quantum, quantum-safe or quantum-resistant.

PQC cont.

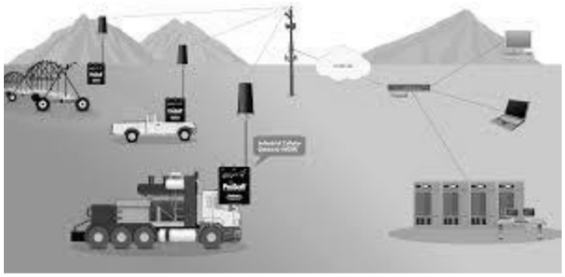
- NIST efforts on PQC standardization
- Too early to identify specific PQC algorithms and technical parameters (= key length)
- Eligible for License Exception ENC/Mass Market treatment

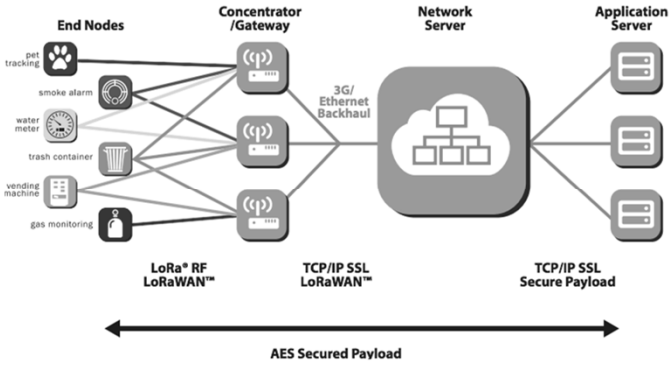
Bureau of Industry and Security
BIS 2019 | ANNUAL CONFERENCE ON EXPORT CONTROLS

IoT Decontrol

- End points:
  - limited to non-arbitrary data (sensor data) or Operations, Administration or Maintenance (OAM); or
  - Specific 'connected civil industry application' (camera, video)
- Associated networking equipment:
  - Limited to 'connected civil industry application' of end point; or
  - OAM of end points or itself.
- 'Connected civil industry application': consumer or civil industry application other than "information security", digital communication, general purpose networking or computing.

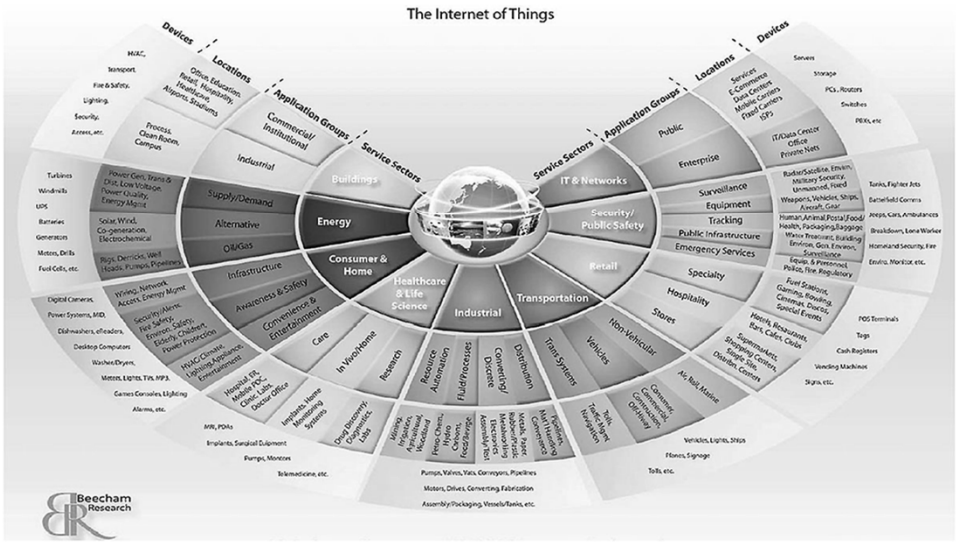
Bureau of Industry and Security
BIS 2019 | ANNUAL CONFERENCE ON EXPORT CONTROLS





end points (things) + networking equipment

Bureau of Industry and Security
BIS 2019 | ANNUAL CONFERENCE ON EXPORT CONTROLS



Connected civil industry applications

Customer based license keys

- "Cryptographic activation". (Cat 5P2) Any technique that specifically activates or enables cryptographic capability of an item, by means of a mechanism implemented by the manufacturer of the item, where this mechanism is uniquely bound to any of the following:
  - 1. A single instance of the item; or
  - 2. One customer, for multiple instances of the item.
  - Technical Notes to definition of "Cryptographic activation":
    - 1. "Cryptographic activation" techniques and mechanisms may be implemented as hardware, "software" or "technology".
    - 2. Mechanisms for "cryptographic activation" can, for example, be serial number-based license keys or authentication instruments such as digitally signed certificates.

Bureau of Industry and Security
BIS 2019 | ANNUAL CONFERENCE ON EXPORT CONTROLS

- 5A002.a: can be activated by means of "cryptographic activation" not employing a **secure** mechanism.
  - Hence activation needs to employ a **secure** mechanism for dormant item to be not controlled.
- Secure mechanism guidelines:
  - Secure distribution (TLS, SHA2)[i]
  - Single customer (bound by location, region, country)
  - Scope of multiple instances of the item (single model number)
  - Technically bound (to immutable aspect of the instances)
  - Secure validation (certificate)

[i] "Transport Layer Security" and "Secure Hash Algorithm 2"

Interpreted programs/Scripts

- Source code?
  - PERL Scripts, Java Scripts, Shell scripts, Python script
- Do not consider scripts that are calling executable encryption libraries to be source code

Bureau of Industry and Security
BIS 2019 | ANNUAL CONFERENCE ON EXPORT CONTROLS

5A002a.4

- Paragraph 5A002a.4 is meant to decontrol certain products that otherwise fail the old Note 4 test.
- Examples
  - Exercise bike with a web browser
  - Television with a web browser
  - Vending machine with a WiFi hotspot

5A002a.4

- Old Note 4: An item remains controlled if it is using encryption for or in support of a non-Note 4 function.
- New paragraph a.4: Even if an item is using encryption for or in support of a non-Note 4 function, it is released if the equipment or software doing the encryption does not fall under 5x002 as a standalone item.

Bureau of Industry and Security
BIS 2019 | ANNUAL CONFERENCE ON EXPORT CONTROLS

UN & Government End-User Definition

- Network infrastructure items under 740.17(b)(2)(i)(A) require a license to “more sensitive government end users” but not to “less sensitive government end users”
- UN agencies are treated as more or less-sensitive based on their functions.
- Exporters can apply for Encryption Licensing Arrangements (ELAs) specifically for UN agencies.