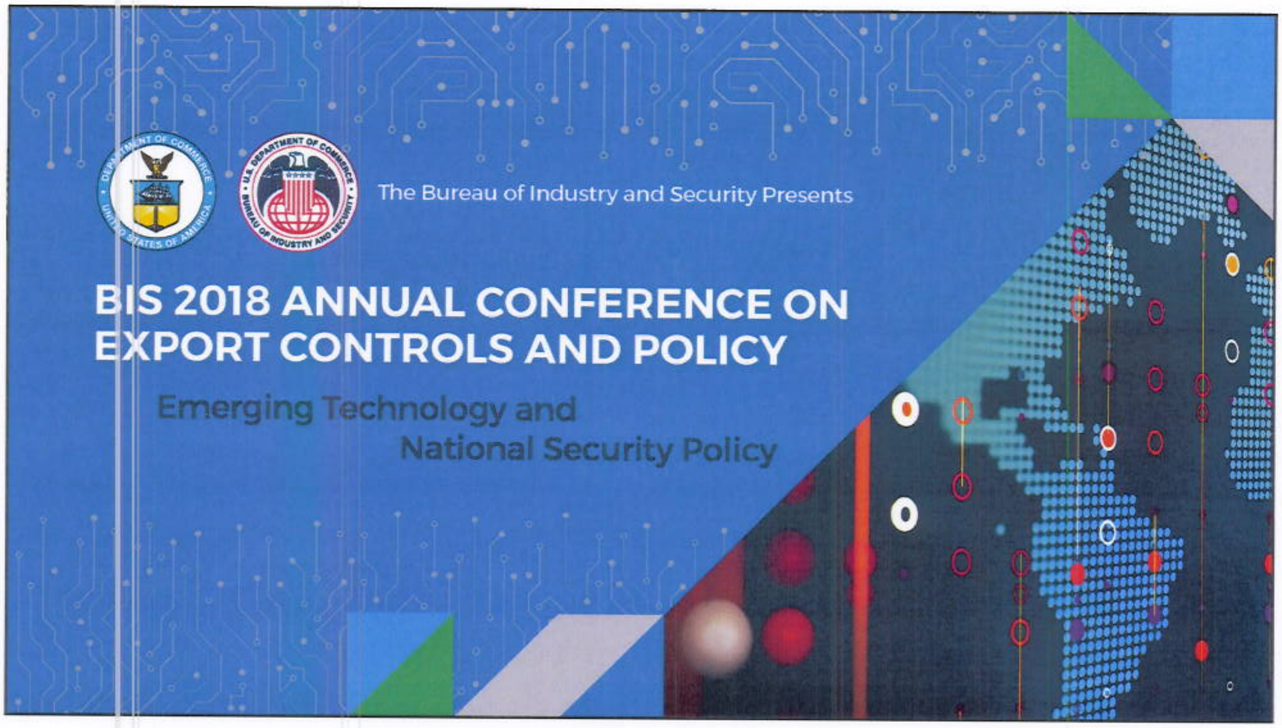


The Bureau of Industry and Security Presents

BIS 2018 ANNUAL CONFERENCE ON EXPORT CONTROLS AND POLICY

Emerging Technology and National Security Policy

Export Controls and Cloud Computing

Bob Rarog
Senior Advisor to the Assistant
Secretary for Export Administration
Bureau of Industry and Security
U.S. Department of Commerce
Robert.Rarog@bis.doc.gov

Anita Zinzuvadia
Senior Engineer
IT Controls Division
Bureau of Industry and Security
U.S. Department of Commerce
Anita.Zinzuvadia@bis.doc.gov

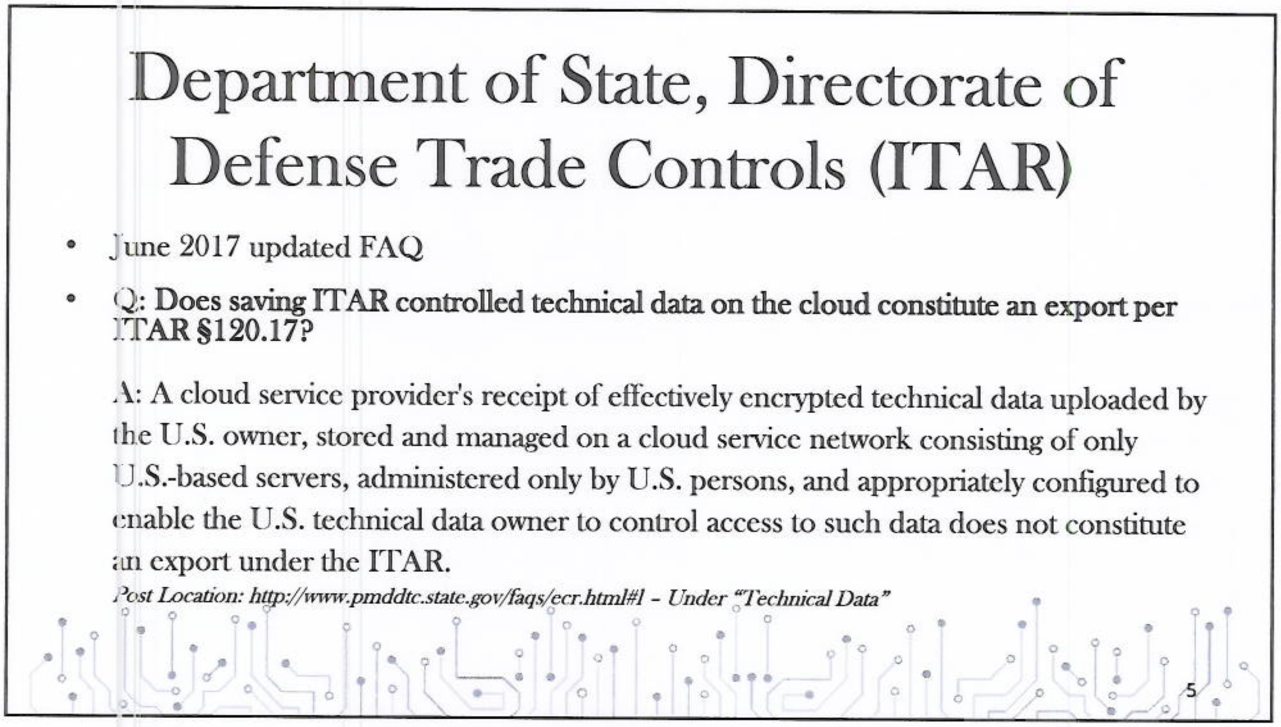
Treasury Department, Office of Foreign Assets Control~~s~~

- As of now, no formal guidance
- Verbal / informal guidance:
  - Providing a service, directly or indirectly, to an embargoed country or sanctioned party without authorization is a violation

Department of State, Directorate of Defense Trade Controls (ITAR)

- June 3, 2015 – Proposed Definitions Rule (80 FR 31525) – Similar to current BIS rule, but required compliance with FIPS 140-2 or its successors.
- June 3, 2016 – Final Definitions Rule (81 FR 35611) – Did not address cloud computing.
- September 8, 2016 – Final Rule Amending Definitions (81 FR 62004).
  - Clarified that theoretical or potential access to technical data is not a release: ... *however, a release will have occurred if a foreign person does actually access technical data, and the person who provided the access is an exporter for the purposes of that release.*

Minor point, but the June 3, 2016, ITAR definitions rule was actually an interim final rule with request for comment

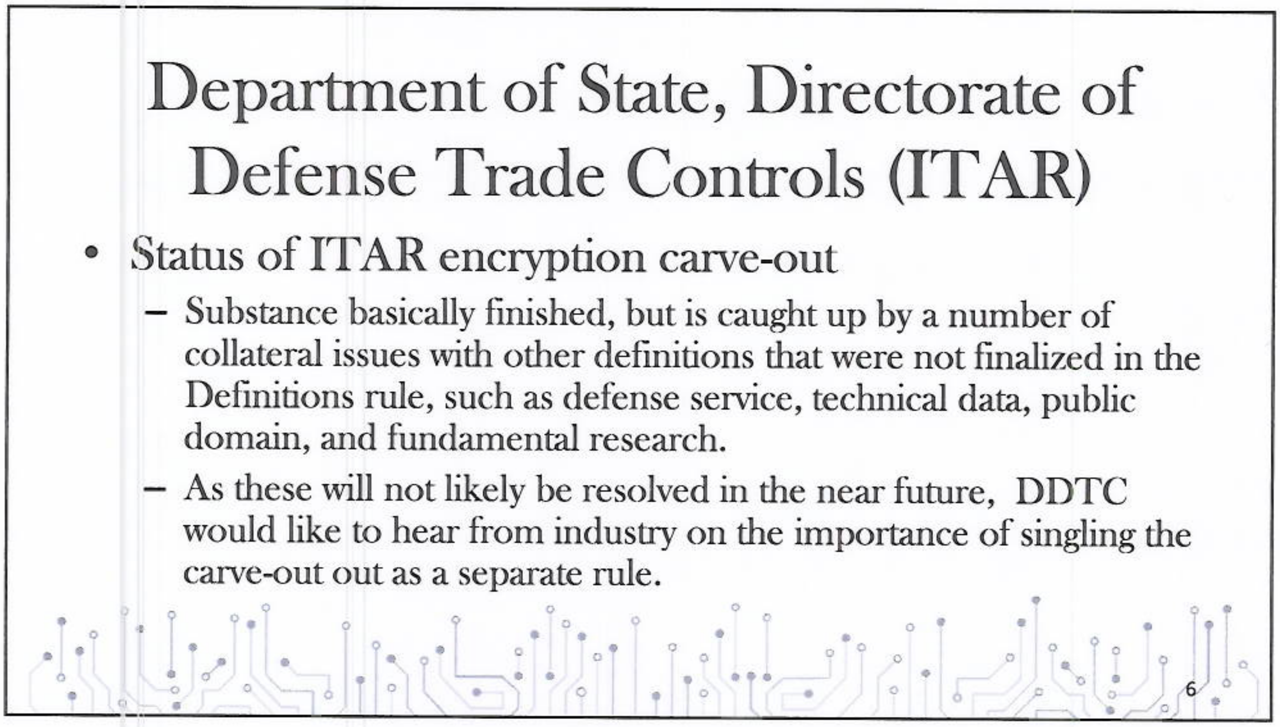


Department of State, Directorate of Defense Trade Controls (ITAR)

- June 2017 updated FAQ
- **Q: Does saving ITAR controlled technical data on the cloud constitute an export per ITAR §120.17?**

A: A cloud service provider's receipt of effectively encrypted technical data uploaded by the U.S. owner, stored and managed on a cloud service network consisting of only U.S.-based servers, administered only by U.S. persons, and appropriately configured to enable the U.S. technical data owner to control access to such data does not constitute an export under the ITAR.

Post Location: http://www.pmddtc.state.gov/faqs/ecr.html#1 - Under "Technical Data"



Department of State, Directorate of Defense Trade Controls (ITAR)

- Status of ITAR encryption carve-out
  - Substance basically finished, but is caught up by a number of collateral issues with other definitions that were not finalized in the Definitions rule, such as defense service, technical data, public domain, and fundamental research.
  - As these will not likely be resolved in the near future, DDTC would like to hear from industry on the importance of singling the carve-out out as a separate rule.

BIS Guidance on Cloud Computing

- Three directly relevant, published, Advisory Opinions, 2009-2014.
- Definitional changes published in a June 3, 2016, FR notice, including the "encryption carve-out."

BIS Guidance on Cloud Computing

- **Jan. 2009** – a cloud provider that provides access to computational capacity is not the exporter of data derived from the computations because they are not the principal party in interest.
- **Jan. 2011** – if the cloud provider is not the exporter, the cloud provider is not making a "deemed export" if their foreign national network administrators access the data.
- **Nov. 2014** – remotely using controlled software is not an export itself, unless there is a transfer.

2016 FR Notice on Definitions

- Opportunity to address the issue; relevant changes in multiple locations in the proposed language.
- The term "cloud" not used in regulatory text – changes affect cross-national data transmission and release to non-U.S. nationals.
- Primary citation in EAR is in a new section, §734.18, "Activities that are not exports, reexports, or transfers."

734.18: "End-to-End" Encryption

Not an export if you are transferring technology or software that is:

- Unclassified;
- Secured using end-to-end encryption (as defined);
- Secured using FIPS-140 compliant encryption modules or equivalents;
- Not intentionally stored in D:5 country or in Russia

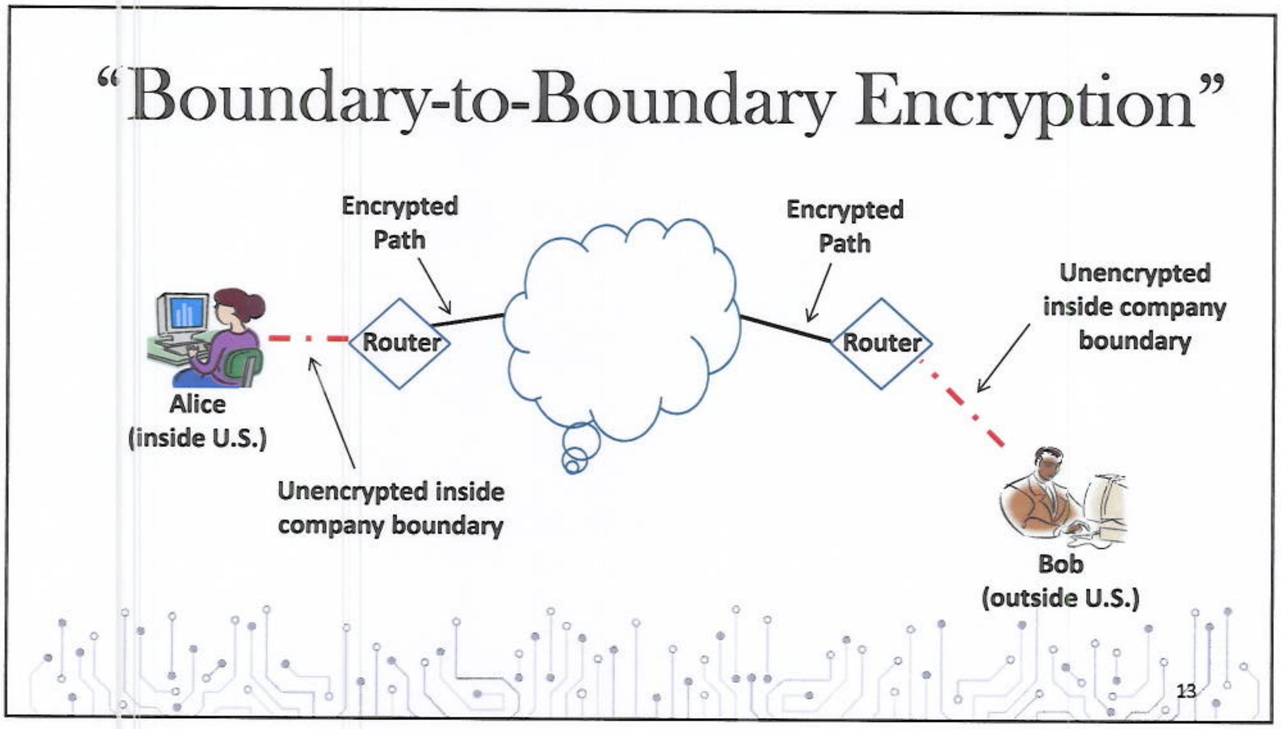
§734.18 references
FIPS-140-2
(or its successors)
←

“End-to-End” Encryption

- Defined as *uninterrupted* cryptographic protection between an originator (or the originator’s in-country security boundary) and an intended recipient (or the recipient’s in-country security boundary).
- Definition is intended to be flexible enough to accommodate different technical approaches (e.g. IPSEC VPN, SSL VPN, etc.)
- Definition is not intended to preclude service provider involvement (i.e., security can be delegated to a third party).

“Boundary to Boundary”

- In the June 3 FR notice, definition of “end-to-end” was changed from “system-to-system” encryption (e.g., PGP) to “security boundary to security boundary.”
- Reflects common industry practice and provides more flexibility.
- Allows necessary services to be performed within the security boundaries while meeting the objectives of the rule.
- Caveat: boundary must be in-country – data cannot cross a national border in the clear.



“Boundary-to-Boundary Encryption”

Encrypted Path

Encrypted Path

Unencrypted inside company boundary

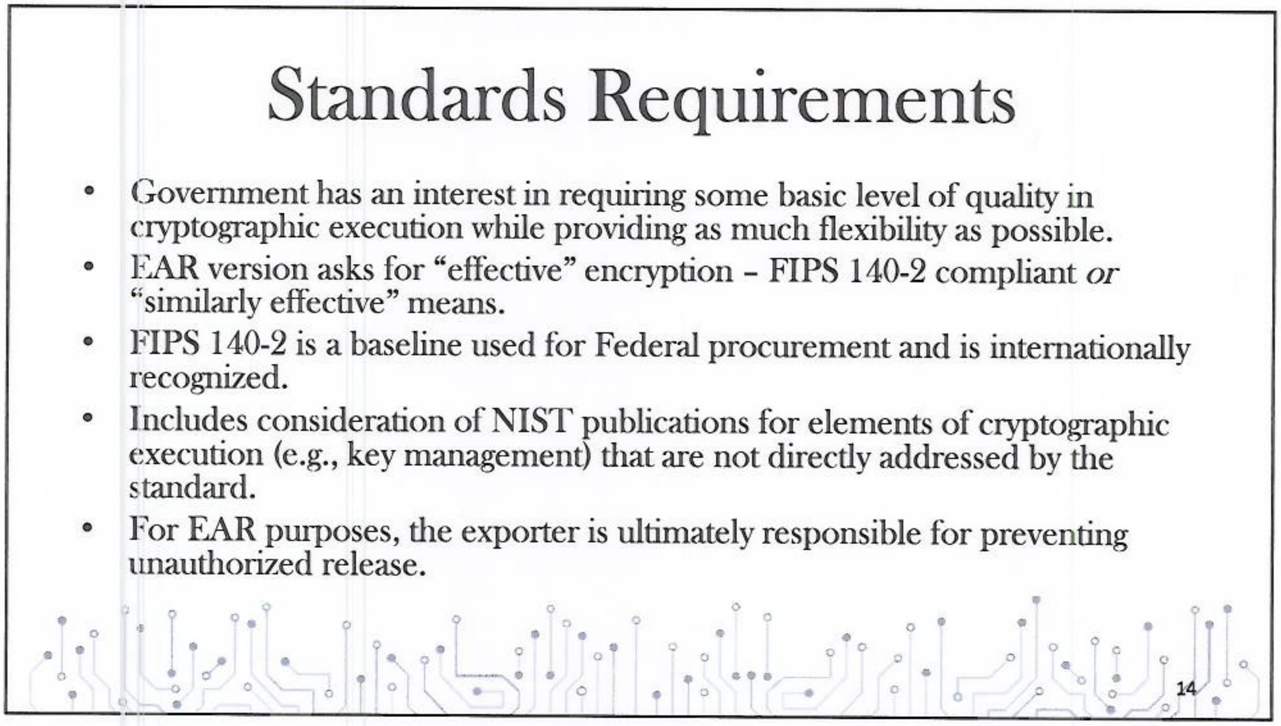
Router

Router

Alice (inside U.S.)

Unencrypted inside company boundary

Bob (outside U.S.)



Standards Requirements

- Government has an interest in requiring some basic level of quality in cryptographic execution while providing as much flexibility as possible.
- EAR version asks for “effective” encryption – FIPS 140-2 compliant *or* “similarly effective” means.
- FIPS 140-2 is a baseline used for Federal procurement and is internationally recognized.
- Includes consideration of NIST publications for elements of cryptographic execution (e.g., key management) that are not directly addressed by the standard.
- For EAR purposes, the exporter is ultimately responsible for preventing unauthorized release.

Storage Restrictions

- "Intentional" storage prohibited in D:5 and Russia.
- Temporary storage on Internet servers while in transit not considered intentional storage.
- Storage on PCs while in D:5 *is* considered "intentional"; in such circumstances, another authorization (e.g., TMP) is required.
- Cloud providers serving western customers have generally not located their resources in these countries.

734.15 Definition of "Release"

- Release must reveal technology or source code subject to the EAR.
- Release of keys, passwords or other data with "knowledge" that such release or transfer will result in release of underlying technical data is a controlled event.
- Keys and other access data are *not* considered "technical data," and can thus be managed independently.

Issues Related to Execution

- Decryption outside the U.S. does not, of itself, constitute an export or release.
- Storage in the clear (after decryption) outside the U.S. does not, of itself, constitute an export or release.
- Provisions must be read along with 734.20 – activities that are not deemed reexports.

Issues Related to Execution

- When transmission is decrypted and re-encrypted, "end-to-end" no longer applies. Subsequent transmission is a separate, new transmission.
- A user may delegate security to a third party provider, but must ensure that such provider meets carve-out criteria (e.g. encrypts between cloud resources).
- Non-U.S. origin data is subject to U.S. controls on export and release to non-U.S. nationals while in the U.S., but does not become "U.S.-origin" when exported unless changed or comingled.

Treatment Outside the U.S.

- Japan
  - 2013 Advisories on Storage and SaaS;
  - No export by provider when user makes storage available to itself only;
  - No other guidance (e.g. level of security);
  - Use of software outside of Japan (SaaS) does constitute export by user.
- Other countries, including EU and Canada, still studying the issue.

Conclusion

- Changes are intended to provide maximum flexibility to providers and users.
- BIS will provide additional guidance as more fact patterns emerge and technology evolves.