Advanced Forum on
GLOBAL EXPORT CONTROLS

Protecting EAR and ITAR-Controlled Data

Moderator:
Michelle Schulz
Managing Partner
Schulz Trade Law PLLC

Derek Hawn
Senior Manager, Global Export Compliance
Nissan

Lynn Van Buren
Director, Global Compliance

Spire Global, Inc.

Waqas Shahid
Vice President, Forensic Services Practice
Charles River Associates

Agenda

- What is an Export?
- Trade Compliance Training
- Employing / Working with Foreign Nationals
- International Travel
- Remote Employees
- InfoSec Controls and Breaches
- Foreign Direct Product Rule (FDPR)
- Enforcement Case Studies
- Lessons Learned

What is an export?

§ 120.50 Export.

(a) ***Export,*** except as set forth in § 120.54 or § 126.16 or § 126.17 of this subchapter, means:

(1) An actual shipment or transmission out of the United States, including the sending or taking of a defense article out of the United States in any manner;

(2) Releasing or otherwise transferring technical data to a foreign person in the United States (a deemed export);

…

(6) The release of previously encrypted technical data as described in § 120.56(a)(3) and (4).

(b) Any release in the United States of technical data to a foreign person is deemed to be an export to all countries in which the foreign person has held or holds citizenship or holds permanent residency.

See also EAR § 734.13.

What is an export?

§ 120.56 Release.

(a) ***Release.*** Technical data is released through:

(1) Visual or other inspection by foreign persons of a defense article that reveals technical data to a foreign person;

(2) Oral or written exchanges with foreign persons of technical data in the United States or abroad;

(3) The use of access information to cause or enable a foreign person, including yourself, to access, view, or possess unencrypted technical data; or

(4) The use of access information to cause technical data outside of the United States to be in unencrypted form.

(b) ***Provision of access information.*** Authorization for a release of technical data to a foreign person is required to provide access information to that foreign person, if that access information can cause or enable access, viewing, or possession of the unencrypted technical data.

What is an export?

§ 120.55 Access information.

Access information is information that allows access to encrypted technical data subject to this subchapter in an unencrypted form. Examples include decryption keys, network access codes, and passwords.

What is (not) an export?

§ 120.54 Activities that are not exports, reexports, retransfers, or temporary imports.

(a) The following activities are not exports, reexports, retransfers, or temporary imports: . . .

(3) Transmitting or otherwise transferring within the same foreign country technical data between or among only U.S. persons, so long as the transmission or transfer does not result in a release to a foreign person or transfer to a person prohibited from receiving the technical data;

…

(5) Sending, taking, or storing technical data that is:

(i) Unclassified;

(ii) Secured using end-to-end encryption;

(iii) Secured using cryptographic modules (hardware or software) compliant with the Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology (NIST) publications, or by other cryptographic means that provide security strength that is at least comparable to the minimum 128 bits of security strength achieved by the Advanced Encryption Standard (AES-128); and

(iv) Not intentionally sent to a person in or stored in a country proscribed in § 126.1 of this subchapter or the Russian Federation; and

•Note 1 to paragraph (a)(5)(iv): Data in-transit via the internet is not deemed to be stored.

(v) Not sent from a country proscribed in § 126.1 of this subchapter or the Russian Federation.

…

See also EAR § 734.18.

What is (not) an export? (cont.)

§ 120.54 Activities that are not exports, reexports, retransfers, or temporary imports.

(b)

(1) For purposes of this section, end-to-end encryption is defined as:

(i) The provision of cryptographic protection of data, such that the data is not in an unencrypted form, between an originator (or the originator's in-country security boundary) and an intended recipient (or the recipient's in-country security boundary); and

(ii) The means of decryption are not provided to any third party.

(2) The originator and the intended recipient may be the same person. The intended recipient must be the originator, a U.S. person in the United States, or a person otherwise authorized to receive the technical data, such as by a license or other approval pursuant to this subchapter.

(c) The ability to access technical data in encrypted form that satisfies the criteria set forth in paragraph (a)(5) of this section does not constitute the release or export of such technical data.

See also EAR § 734.18.

What is (not) an export? (cont.)

§ 125.4 Exemptions of general applicability.

(a) The following exemptions apply to exports of technical data for which approval is not needed from the Directorate of Defense Trade Controls. The exemptions, except for paragraph (b)(13) of this section, do not apply to exports to proscribed destinations under § 126.1 of this subchapter or for persons considered generally ineligible under § 120.16 of this subchapter. . .

(b) The following exports are exempt from the licensing requirements of this subchapter.

(9) Technical data, including classified information, regardless of media or format, exported, reexported, or retransferred by or to a U.S. person, or a foreign person employee of a U.S. person travelling or on temporary assignment abroad, subject to the following restrictions:

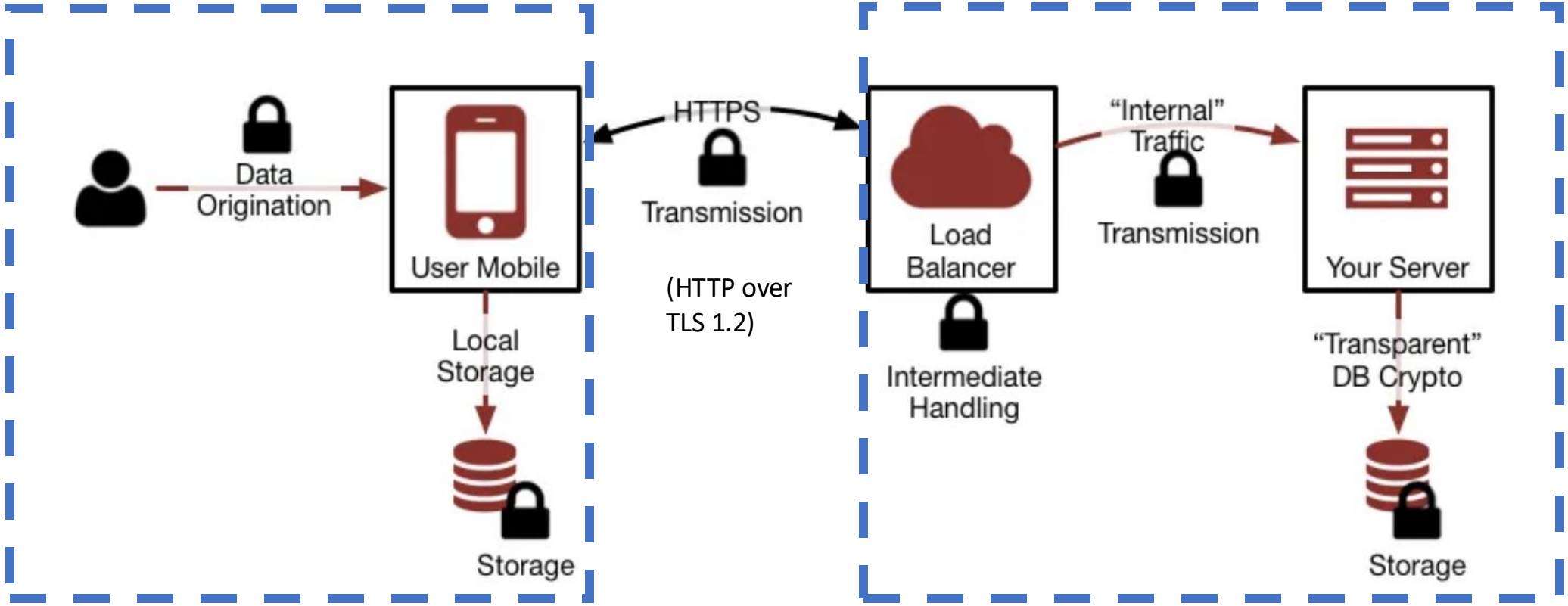
(i) Foreign persons may only export, reexport, retransfer, or receive such technical data as they are authorized to receive through a separate license or other approval.

(ii) The technical data exported, reexported, or retransferred under this authorization may only be possessed or used by a U.S. person or authorized foreign person. Sufficient security precautions must be taken to prevent the unauthorized release of the technical data. Such security precautions may include encryption of the technical data; the use of secure network connections, such as virtual private networks; the use of passwords or other access restrictions on the electronic device or media on which the technical data is stored; and the use of firewalls and other network security measures to prevent unauthorized access.

(iii) The individual is an employee of the U.S. government or is directly employed by a U.S. person and not by a foreign subsidiary.

Similar Exception under the EAR - TMP “Tools of the Trade” EAR 740.9(a), though somewhat different in application

End-to-End Encryption – A picture



Security boundary?

Corporate security boundary – Can be very tricky with modern cloud infrastructure and reliance on third-parties

Hypothetical

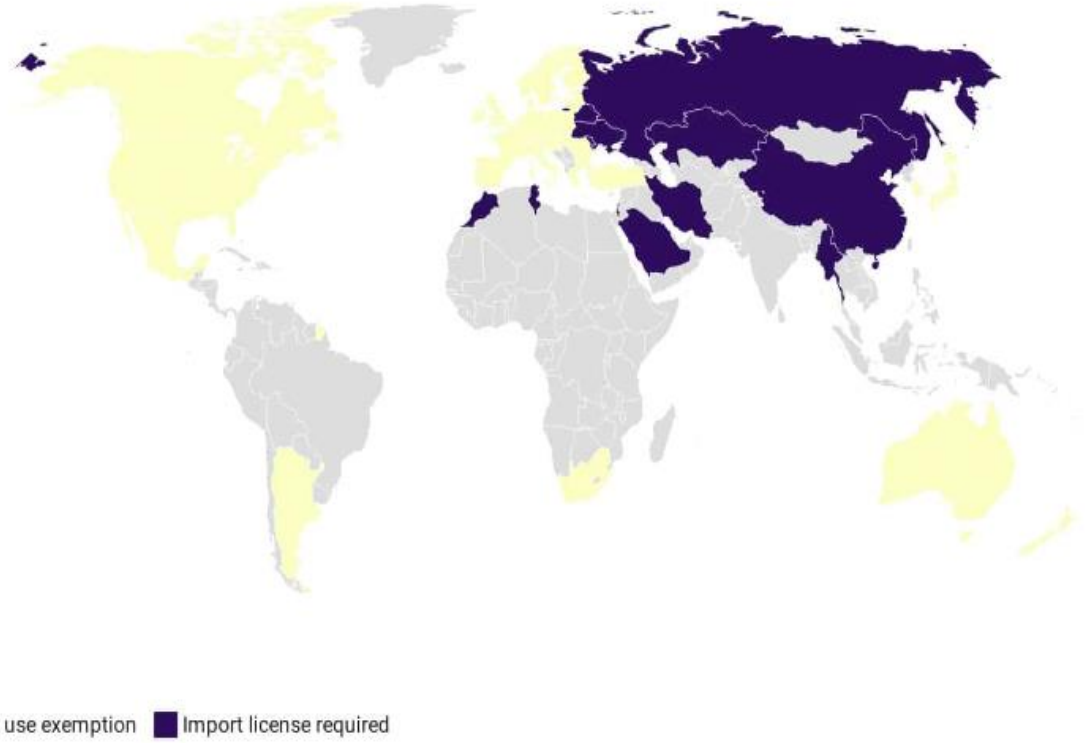
- Waqas is a software engineer at Acme Co., a US tech startup, and is working on an ITAR-controlled software project
- He has to travel to Turkiye to trouble shoot an installation of the software at a client. He is taking a clean laptop
- While in Turkiye, he logs into his company's secure network via VPN. All data on his network is encrypted at rest
- He pulls up the software code and looks through it on his laptop, alone
- Has an export occurred? What authorization, if any, does he need?

Hypothetical Variations (Same Questions)

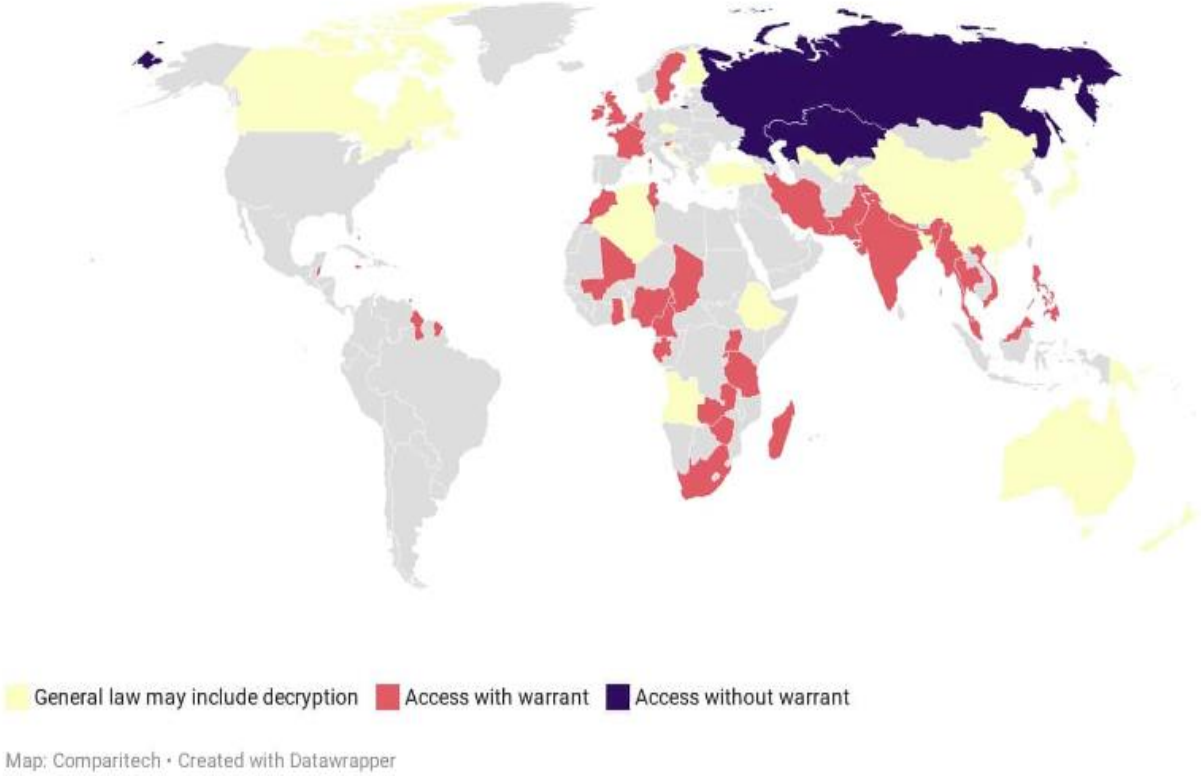
- He pulls up the software code and looks through it on his laptop, with the client's (Turkish) software lead looking over his shoulder
- On his way back, he has a stopover in Paris, and uses airport wifi to log into a secure company website (HTTPs) on his tablet and continue work on the ITAR software in the web interface
- On his way back, he has a stopover in Paris, and uses his company VPN to download encrypted software files to his laptop, though he does not decrypt and open them before boarding his flight back to the US
- On his way back, he has an emergency landing in Cyprus, and uses his company VPN to download encrypted software files to his laptop, though he does not decrypt and open them before boarding his flight back to the US

Also, keep in mind…

Where can you travel with a personal laptop that's encrypted?



Which countries require encryption users to decrypt data for law enforcement?



Trade Compliance Training

We all know training is an important part of compliance. The most difficult part can be the implementation.

Hypothetical Exercise

Barney, Inc. in Austin, Texas filed a Voluntary Self-Disclosure with DDTC and BIS for approximately 110 inadvertent releases of technical information about a variety of military and dual-use ocean vessels.

Barney – Owner of Barney, Inc.

Hypothetical Exercise (cont'd)

Chief Engineer Amber maintained a ShareFile folder in the engineering department for quick reference on repairs and maintenance of the control panel for each item. Anyone in Barney's engineering department could access it, including an H-1B holder, a contractor with unknown nationality, and an intern on a J-1 visa. Amber figures HR has that all worked out.

Amber – Chief Engineer

Hypothetical Exercise (cont'd)

The folder was also accessible by anyone at an unrelated London repair station called Smokie, Inc.

Smokie – Rookie
Employee at Smokie, Inc.

Hypothetical Exercise (cont'd)

Later, Amber found out there was IT personnel who could see it. The engineers were not aware of export controls because they are super busy, and the export group works remotely anyway so they don't really see each other often apart from the Barney holiday party.

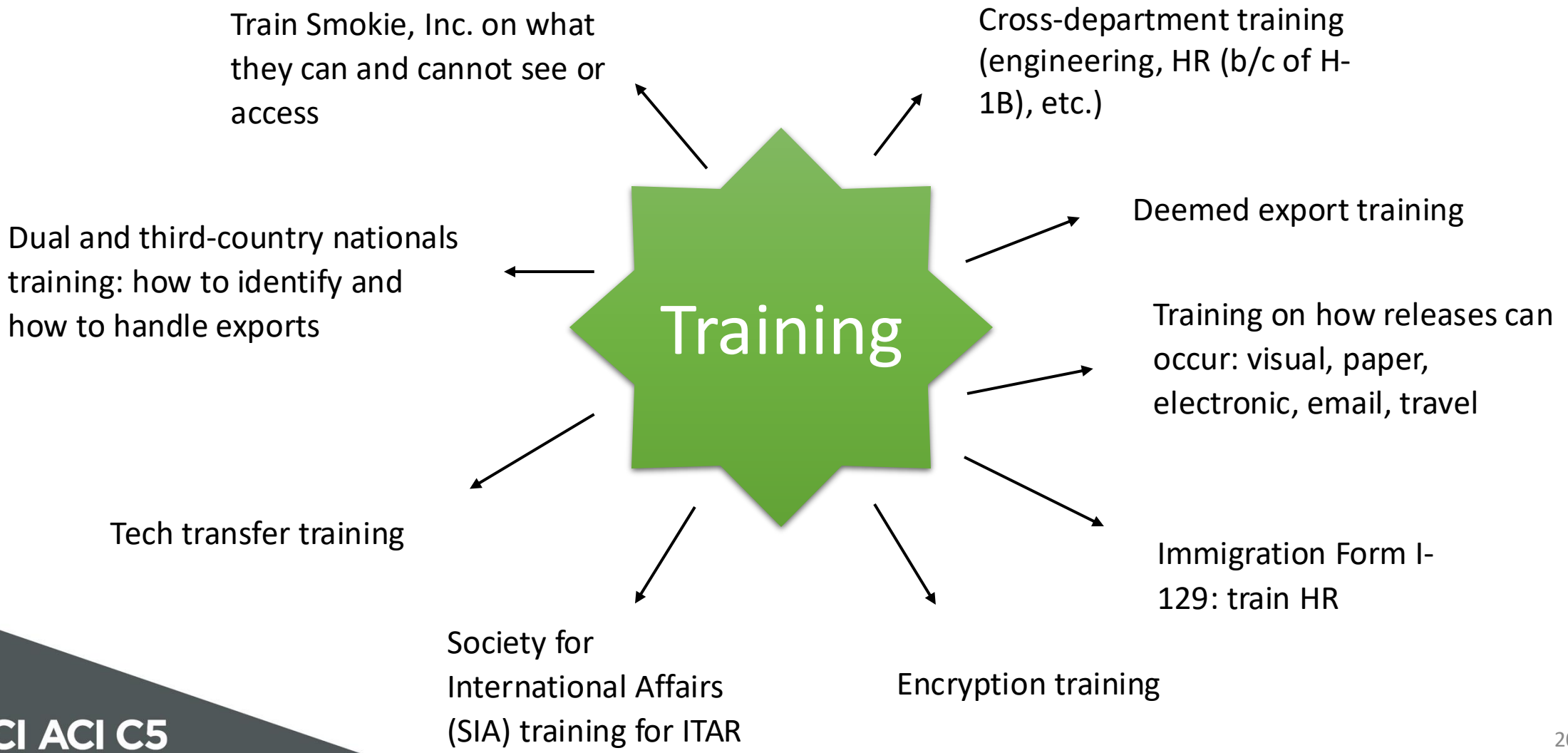
Hypothetical Exercise (cont'd)

Now Barney, Inc. has filed a VSD, Barney's Trade Compliance Team recognizes a need for export compliance training as a corrective measure (one of several).

Hypothetical Question #1

What kind of training would you recommend for this company?

Hypothetical Answer #1



Hypothetical Question #2

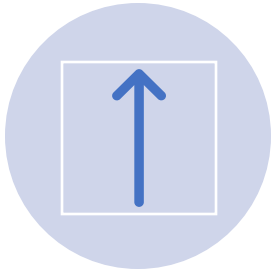
- How could Barney document this training for the VSD?

Hypothetical Answer #2

SIGN-IN SHEETS

ONLINE SIGNATURES

TRAINING MATERIALS



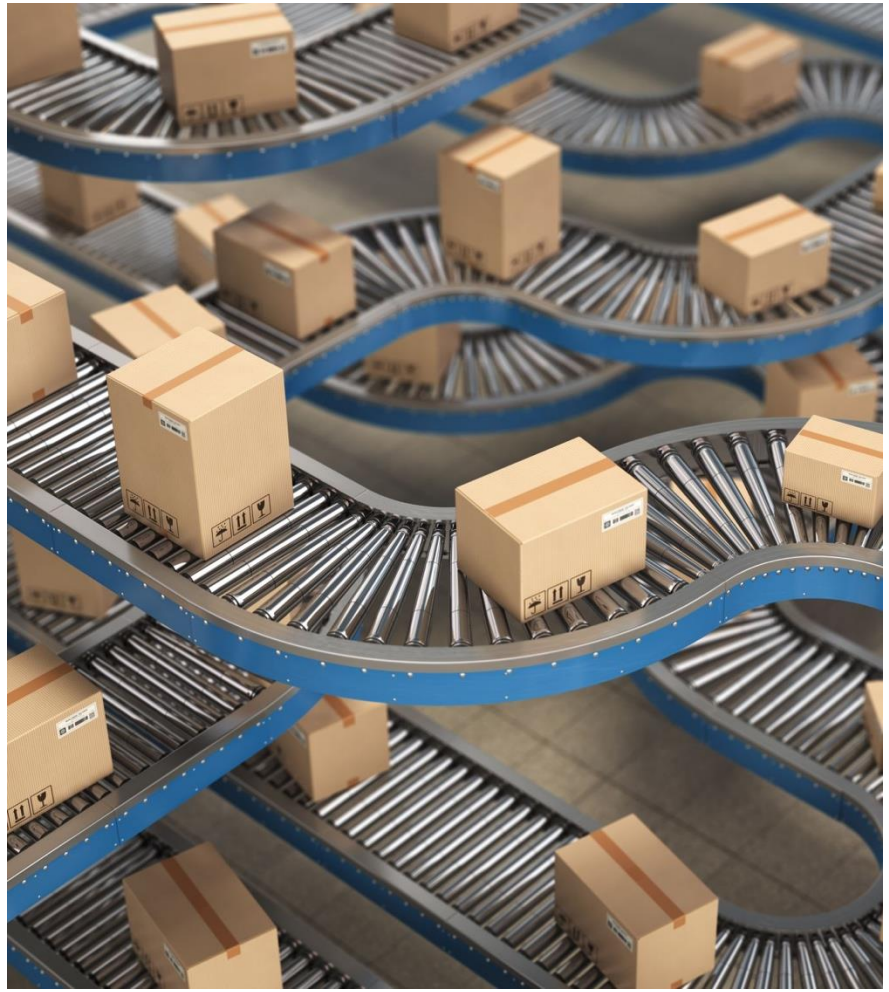
ALL THE ABOVE

Polling Question

- What is your favorite thing about the existing export compliance training program at your company?
  A. Interactive discussions and Q&A.
  B. Handouts and tools we can take with us.
  C. Learning about new developments in trade law.
  D. Bringing the Sales team and other departments on board with compliance.
  E. My company has no compliance training.

Employing / Working with Foreign Nationals

- Export Administration Regulations
  - Most technologies can be shared with most foreign nationals without a license
  - This includes physical exports of technology, e.g., shipping drawings to a foreign partner via courier, and electronic exports, e.g., sending the same drawings via e-mail
- International Traffic in Arms Regulations (ITAR)
  - A license or other authorization such as a Technical Assistance Agreement is required to share virtually all technical data with a foreign national



Compliance Processes

- Classify Technology and Underlying Product
  - Pre-requisite to engaging in any export
  - Understand controls on item and related technology
  - Mark drawings, other forms of technology with appropriate classification

- KYC on Recipient of Technology
  - Licensing requirement based on recipient's nationality
  - End-use of technology may also impact license requirement / determination
  - Credibility of recipient to identify risk of diversion, misuse
  - Obtain certification, other confirmation that recipient will not share technology unlawfully

Technology Control Plans (TCP)

- Policy / process document to maintain controls on technology
- Specific instructions for marking, storing, protecting technology
  - Can cover hard-copy or electronic copies of technology
  - May include facility controls, e.g., access restrictions to certain areas of a facility, badging requirements, etc.
  - Can be specific to individual, specific type of technology, particular facility or office
- Required by NISPOM in some situations; otherwise simply a best practice

Compliance Challenge – International Travel

- Employee laptop may contain controlled technical data on hard drive
- Employee may access data from overseas through VPN connection
- Employee may participate in telephone call from abroad where controlled technical data is involved
  - Additional risk with Zoom, Teams screen sharing if in public space

- Best Practice
  - Require personnel to travel with loaner laptop
  - Prohibit downloading of technical data while outside United States
  - No printing of any technical data outside United States
  - Store laptop, other devices in safes in hotel rooms if not in possession of laptop
  - No international travel with any hardcopy technical data

Remote Non-US Employees

- DDTC
  - The ITAR generally requires the issuance of an export license to share controlled technical data with a foreign person or entity
  - Exceptions for DN/TCN “regular employees” of foreign entities and governments who are themselves licensed (*e.g.*, ITAR 126.18)
  - A “regular employee” in the ITAR includes permanent/direct employees and long-term contractors who are subject to the control of the company and work full-time at a company facility (ITAR 120.64)
  - Requirement that long-term contractors work at the facility suspended temporarily, so long as the individual is not located in an ITAR 126.1 country (86 FR 30778 (June 10, 2021), 88 FR 12210 (Feb. 27, 2023))
- BIS
  - EAR 734.20 (activities that are not deemed reexports) regular employees include direct employees and individuals "in a long-term contractual relationship with the company where the individual works at the entity's facilities or at locations assigned by the entity (such as a remote site or on travel)"

- *Tip: Local laws also may require export licenses between the remote (PEO) employee and the company location(s)*

Hypothetical

- Jane Smith is a US citizen employee of US company Acme Co, which is a manufacturer of both EAR- and ITAR-controlled products. Jane, an engineer, needs to travel to Germany, India, and Australia for work meetings with suppliers and customers. Since she will be gone for nearly 2 weeks, she wants to take her own laptop as opposed to loaner laptop because she has lots of material saved on her laptop.

Hypothetical (cont'd)

If Acme decides to allow Jane to travel with her own laptop, what compliance steps should they take?

(a) Implement a TCP for Jane's travel

(b) Provide Jane with refresher training on compliance with technology export controls

(c) Require Jane to certify that she will not download any EAR-controlled data while traveling

(d) Require Jane to certify that she will not download any ITAR-controlled data while traveling

(e) Mandate that Jane store her laptop in a safe anytime she is not in possession of it

(f) Other steps

Hypothetical Discussion

(a) Implement a TCP for Jane's travel. *This is not really what a TCP is designed for, though developing specific guidance for Jane to follow – in accordance with training under (b) – makes sense.*

(b) Provide Jane with refresher training on compliance with technology export controls. *This is a good idea if Jane has not frequently traveled internationally or has not recently received export compliance training. But it may not be necessary if Jane has recently received training and otherwise demonstrates a good understanding of her compliance obligations*

(c) Require Jane to certify that she will not download any EAR-controlled data while traveling. *This may not be necessary depending on the classification of EAR-controlled data Jane has on her laptop. Moreover, requiring an employee to certify to compliance may have a chilling effect on the employer-employee relationship.*

(d) Require Jane to certify that she will not download any ITAR-controlled data while traveling. *While requiring a certification might not be ideal for the employer-employee relationship, because a license is required to export virtually any ITAR-controlled data to any foreign national or country, a certification in this case – or something similar to a certification – may make sense. At the same time, if Jane will only be traveling to locations to which Acme already is authorized to export the data on Jane's laptop, a certification may not be needed.*

(e) Mandate that Jane store her laptop in a safe anytime she is not in possession of it. *This is strongly advisable.*

(f) Other steps. *Depending on the nature of Jane's business meetings, and information she may share during those meetings, any materials she would be sharing with foreign nationals should be reviewed for classification and jurisdiction purposes. Copies of materials, if shared in hard copy, may need to be shredded after meetings to protect against diversion or unauthorized access. Other compliance measures should also be implemented as appropriate.*

InfoSec Controls

Many companies are standardizing security measures to prevent unauthorized access to / loss of sensitive data (not just ECI):

- Encrypting laptop hard drives by default
- Disabling thumb drives and disk drives (if you still have them)
- Implementing end-point security software for ability to remotely control and wipe laptops / cell phones
- Digital loss prevention (DLP) tools to flag/prevent exfiltration of data outside the network
- Multi-factor authentication for laptop login
- Geofencing – Preventing network access from outside certain geographical boundaries, except by exception
- Just-in-time Admin Privilege Management
- Separation of network/infrastructure administration and content administration
- Zero-trust architecture

If your company has sensitive data (including ECI) and your company does NOT implement most or all of these measures, you should have a long talk with you IT folks

Data Breach and Export Controls

Data breaches are stressful, even more so for companies with ECI

Unauthorized access or transfer of sensitive technology/technical data to unauthorized parties could potentially constitute unauthorized access/regulatory violations; may even require mandatory disclosure under ITAR, DFARS provisions, new SEC cyber rules

Have to bring in trade compliance (and counsel) on breach investigations at companies handling ITAR-controlled ECI

Data breaches within the supply chain could lead to unauthorized access to, or transfer of export-controlled data, implicating multiple parties in potential violations

Foreign Direct Product Rule (FDPR)

15 CFR § 734.9

States if a product was made using American technology, the U.S. government has the power to stop it from being sold – including products made in a foreign country.

(FDPR) Spotlight Case – Seagate Technology LLC

BIS imposes $300 million penalty against Seagate Technology LLC Related to shipments to Huawei.

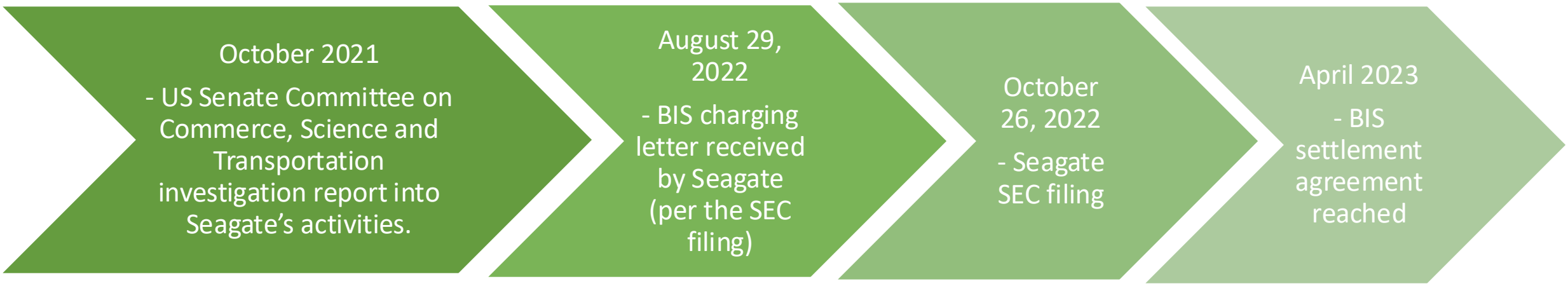
Case Background

- Seagate ordered or caused the reexport, export from abroad, or transfer (in-country) of approximately 7,420,496 foreign-produced HDDs, valued at approximately $1,104,732,205, to Huawei entities listed on the BIS Entity List or where such entities were a party to a transaction without authorization from BIS.
- This historic foreign direct product enforcement case and settlement represents the largest standalone administrative penalty in BIS history.

Seagate Enforcement Timeline

Seagate Enforcement Timeline (cont'd)

Seagate Enforcement Timeline (cont'd)



Lessons Learned: Enforcement Cases

- Do you know the classification of your technology/tech data/software?
- Do you know where your controlled technology/SW is being housed, including backups, and who has access to them?
  - *3D Systems* – EAR & ITAR controlled aerospace items to China; backup servers in Germany with emails containing controlled design information to subsidiary in Germany; $3.7 million fine (BIS); $20 million fine & consent order (DDTC); $4.5 million (DOJ) for False Claim Act violations
  - 3D Systems handled technical data of its customers w/o requesting jurisdiction/classification information
  - No controls on hiring foreign persons
  - All employees had access to controlled data; used listserves, etc. w/o maintaining records of membership lists = recordkeeping violations

Lessons Learned: Enforcement Cases

- Do you know how your technology/tech data/software is being used – by overseas subsidiaries, partners, customers, vendors, etc.?
- Do you know whether your items are subject to the EAR under the FDPR?
  - *Seagate US & SG* – 429 unauthorized re-exports/transfers to Huawei of approx. 7000+ HDD subject to the EAR under the FDPR between Aug. 17, 2020 and Sept. 29, 2021; $300 million fine + audits + suspended denial order
  - According to Charging Letter, Seagate incorrectly interpreted the FDPR to require evaluation of only the last stage of its HDD manufacturing process rather than the entire process
  - Manufacturing process included ECCN 3B992 automated inspection system equipment that was the direct product of US-origin ECCN 3E991 technology & various ECCN 3B992 etch and deposition equipment that was the direct product of US-origin ECCN 3E991 technology

Polling Question

- What year was FDPR first introduced?

A. 1934
B. 1946
C. 1959
D. 1973

HAVE A QUESTION?