SQUIRE PATTON BOGGS

EGADD
Export Group for Aerospace, Defence & Dual-Use

ROLLS ROYCE

Export in the Digital Age

Colleen Swinburn
Rolls-Royce UK plc

IT and Export Control

IT in the 21st Century

- Clouds: A desire to outsource to achieve flexibility, capability uplift
  - "...as a Service" and what are the different types of support
  - Use of Public Clouds, IoT and 'big data'
  - What the governments say
- Increased reliance on 'Digital' capability
  - Artificial Intelligence – computers perform tasks 'normally' done by people
  - Robotics to increase automation
  - Developing virtual models rather than physical prototypes
  - Encryption – is it an effective alternative to licensing and when is it regulated
  - Your digital footprint
- Parting thoughts – where do you place your attention?

Cloud

And export implications

SQUIRE PATTON BOGGS

EGADD
Export Group for Aerospace, Defence & Dual-Use

ROLLS ROYCE

The justification for Cloud

- Key business driver – to simplify cost of IT for business (e.g. one bill every month for the ‘same’ amount)
  - Service provider (supplier) owns and manages the hardware
  - Service provider (supplier) hires, retains and trains the technical support
  - Service is always available and with unlimited capacity
- How is this outcome achieved?
  - Hardware sourced in low cost locations
  - Support can be from anywhere globally – best resource for lowest price
  - Commercial contract terms key

.gov Clouds

- Government certified Clouds
  - .gov clouds – an agreement between a government and the cloud supplier
  - Business is a 3rd party in this transaction
  - Normally a cloud hosted and supported on domestic soil
  - Does not remove Export requirements

Cloud Infrastructure and Considerations

- "...as a Service" (Software, Infrastructure or Platform)
  - Continuum of how much you 'hand over' to the supplier
  - Public Cloud versus Private Cloud versus 'Hybrid' (mix)
  - Server location(s) – you decide!
  - 'Follow the Sun' support
  - Cyber support versus Business as Usual
- Export Control Considerations
  - Most Cloud offerings have a Global component
  - IT Support can take many forms (and have many suppliers involved)
  - Commercial Contract is the key tool to manage compliance

Use of Cloud: Some Export suggestions

- Data classification is vital - both for Export and other sensitive data-types (e.g. GDPR might also be a concern)
- Business requirements document must include:
  - Specific geographical locations of Cloud servers (main and failover)
  - ALL suppliers who will expect to interact with the service (IT administrative support, IT Security, Report Developers as examples)
  - Plans for governance to ensure access to Cloud is managed ongoing
- Remind project teams that *requesting* an export license *does not guarantee approval*

Big Data and Internet of Things

- Use of Cloud capability to link and access large datasets
- Sources of data larger than company datasets
  - SITA, Flightaware
  - Customer data (e.g. airframers AND airlines)
  - Supplier Data
  - Military/government data (?!)
- Governance and Data labelling are key factors
  - How will project get classification for non-company data?
  - What artefacts are required to prove permission to use data is granted?

Cloud Summary

- Relatively new technology so not much guidance (FEDRAMP the exception)
- Know where the data will reside – server location(s)
- Know who will have access to the data – suppliers and their suppliers
- Have a plan to prove (ongoing) how you are compliant

Digital Capability

Some terms and tips

SQUIRE PATTON BOGGS

EGADD
Export Group for Aerospace, Defence & Dual-Use

ROLLS ROYCE

Artificial Intelligence (AI)

- Definition: *"In computer science, artificial intelligence, sometimes called machine intelligence, is intelligence demonstrated by machines, in contrast to the natural intelligence displayed by humans."* *https://en.wikipedia.org/wiki/Artificial_intelligence*
- Usually relies on large datasets to allow machine *learning* opportunities
- Export Considerations:
  - Where is the oversight?
  - Is the AI process auditable?
  - Data classification at every step:
    - ✓ input versus output
    - ✓ Understanding all systems/interfaces

Robotics

- Definition: "***Robotics*** *deals with the design, construction, operation, and use of* ***robots****, as well as computer systems for their control, sensory feedback, and information processing. These technologies are used to develop machines that can substitute for humans and replicate human actions."* https://en.wikipedia.org/wiki/Robotics
- Can be for automating manufacturing *as well as* office/clerical tasks

Export considerations

- Understanding data flows important (interfaces, data storage locations)
- Remote Vendor Access
- Clearing down the machine(s)
- Some robots are themselves export-controlled; so is the software for their development, production and use - hence 'operation', 'maintenance' etc

Digital ‘Twins’ and Virtual Modelling

Definition: *“A **digital twin** is a digital replica of a living or non-living physical entity...*

- ✓ *the virtual entity...exist(s) simultaneously with the physical entity.*
- ✓ *(an important component is) the connection between the physical model and the corresponding virtual model or virtual counterpart.*
- ✓ *(physical and virtual) connection is established by generating real time data using sensors.”*
  https://en.wikipedia.org/wiki/Digital_twin#Manufacturing_industry

Export Considerations:

- Where will the data gathered from the twins be stored/accessed?
- Does the output create an export issue (IoT, AI, etc)?
- If the entity is export controlled, are ALL parties export authorised?
  - Business process flows can help!

Encryption

The answer to all our problems?

SQUIRE PATTON BOGGS

EGADD
Export Group for Aerospace, Defence & Dual-Use

ROLLS ROYCE

Encryption as a controlling mechanism

- UK still sees the cross-border movement of controlled technology as an export, whether encrypted or not
- Many other jurisdictions have not yet weighed in – ITAR has not taken a stance either way (intentionally)
- Key is to understand all data movement as re-export could be a consideration

Encryption and the Cloud

- Export considerations
  - How do you ensure you have exclusive access to the keys?
  - Ensure good data segregation in ‘feeding’ systems
  - Use of encryption with IoT datasets - more effort than its worth?
  - Is it possible to interact meaningfully with encrypted data?

Encryption Classification and Re-export

- Mechanism for encryption can itself be subject to control
  - Wassenaar guidance used by many jurisdictions
    - Ease of purchase
    - Ease of installation
  - Software that carries encryption classification (rather than more publicly available classification) could be subject to export and re-export licenses
- Export considerations
  - When you buy software, ask the vendor for the (full) classification
  - Ensure you find out if any licensing requirements apply if you intend to export the software, or have cross-border interaction with the software
  - If the company asserts their encryption software is not ENC classified, get it in writing!

Your Virtual Presence

- Use of ‘smart’ devices means a user is linked across many systems
- More Commercial Off the Shelf (COTS) software with limited amendment capability
- Software and network access is available across multiple platforms
- Export Considerations:
  - Well-trained users are the key component to success
  - Reminders, notifications, regular refresher training
  - Company policies supporting ‘good’ user behaviours (e.g. Code of Conduct)

Some final guidelines

- Know the export classification(s) and jurisdiction(s) – something many IT people don't know to ask about
- Know the transfer paths planned for all phases of the installation; what they do for go-live might not be what they want to do for the next phase of the project.
- Get in the project early and remind, remind, remind of license timelines.
- Link as closely as possible with your IT/Cyber Security team and other sensitive data stakeholders

A case study

Your friendly but confused contract Project Manager needs your help to ensure her Digital Twin project is Export Compliant. She has been tasked with building a Digital Twin Shop Floor capability where IoT weather data is merged with sensor data from the new product your business is developing to analyse changes to output based on changing weather parameters.

She is hoping to use a Public Cloud to manage the large datasets and will need the help of the manufacturing machine OEM to set up the different test cases.

This is a UK military component and when you ask about other jurisdiction's content, she gives you a blank look but then recovers and says it'll be fine because all of the data will be encrypted.

What do you tell her?

Appendix

Risk Assessment of different Cloud options

On Premise

Private Cloud

Mix of types (Hybrid Cloud or Cloud/On Prem)

Public Cloud

Customer Retains Control

Cloud Supplier Controls

Traditional **'On Prem'**

IaaS – **you** manage data, software applications and system support, **Cloud supplier** manages storage and server connections

PaaS – **you** manage data and software applications, **Cloud supplier** manages servers and system support

SaaS –you hand your data to the **Cloud supplier** who manages all IT tasks

SQUIRE PATTON BOGGS

EGADD Export Group for Aerospace, Defence & Dual-Use

ROLLS ROYCE

UK/EU Encryption Classifications

- From the ‘Cryptography Note’ – Note 3 to Category 5 Part 2, Information Security as it appears in Annex I to Council Regulation (EC) No. 428/2009 (as last amended by Regulation (EU) No. 2268/2017)
- Products that use cryptography are typically controlled under the dual use list. Note 3a is intended to exclude goods from control that:
  - can be easily acquired by the general public
  - require little or no support to install
  - where the cryptographic functionality cannot be easily changed by the user
- A very important general principle of control in Category 5 Part 2 is that a product is classified on the basis of its functionality and characteristics and considered as a standalone item. The item’s control list classification cannot be worked out solely from the classifications of individual component parts.
- *If you’re not sure whether Note 3 applies to one of your products, you can consider applying to the ECJU for a Control List Classification.*

Source: https://www.gov.uk/government/publications/notice-to-exporters-201807-guidance-on-the-cryptography-note/notice-to-exporters-201807-guidance-on-the-cryptography-note

Useful Links

- EU Commission Recommendation on Internal Compliance Programmes for Dual-Use Trade Controls
  - https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1565015135434&uri=CELEX:32019H1318
- Guidance on what encryption standards are required globally (effective as of 2016):
  - http://www.cryptolaw.org/
- OGEL for Info Security Items (encryption)
  - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/700925/18-ogel-information-security.pdf

Thanks for listening!

SQUIRE PATTON BOGGS

EGADD
Export Group for Aerospace, Defence & Dual-Use

ROLLS ROYCE