SERVING THE EXPORT COMMUNITY FOR OVER 50 YEARS ®

SIA

Est. 1967

COMPLIANCE IN THE CLOUD

3:45-4:30PM

Scott Edwards, President, Summit 7
Dave Harris

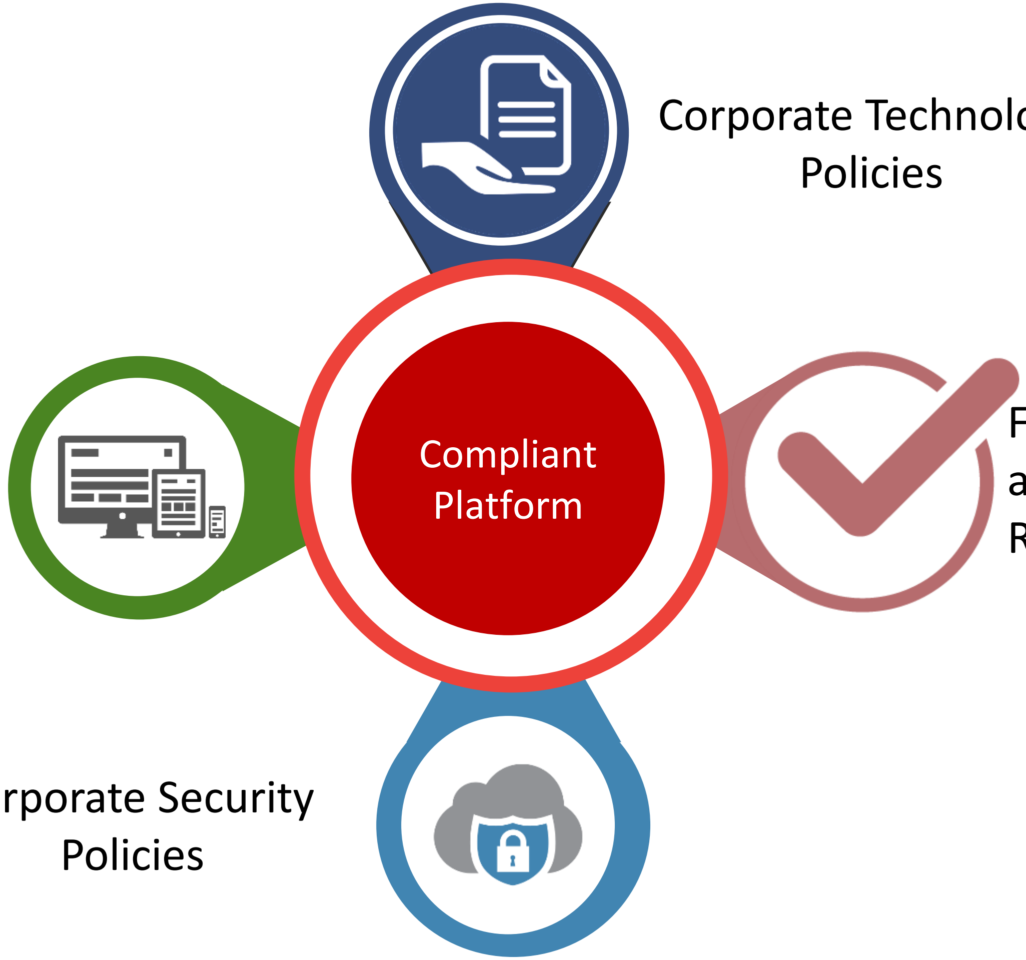
COMPLIANCE IN THE CLOUD

Scott Edwards

scott.edwards@summit7systems.com

256-541-9638

What does it Take to get a Compliant Platform?



Corporate Technology Policies

Chosen Platform Capabilities

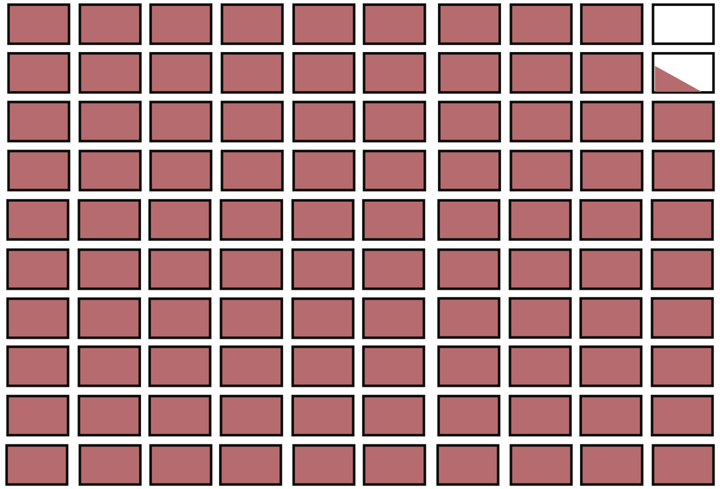
Compliant Platform

Functional, Technical and Compliance Requirements

Corporate Security Policies

DFARS 252.204-7012

87% of all DoD Contracts in 2017



Key Dates

December 31, 2017

December 31, 2018
FAR Changes

3 Major Components

1. Provide Adequate Security on all Covered Contractor Information Systems
    - FedRAMP Moderate
    - NIST SP 800-171 with mapping to NIST 800-53 Relevant Security Controls

2. Rapidly Report Cyber Incidents to DoD at http://dibnet.dod.mil
    - 72 Hours
    - Medium Assurance Certificate

3. Contract Flowdown Requirements

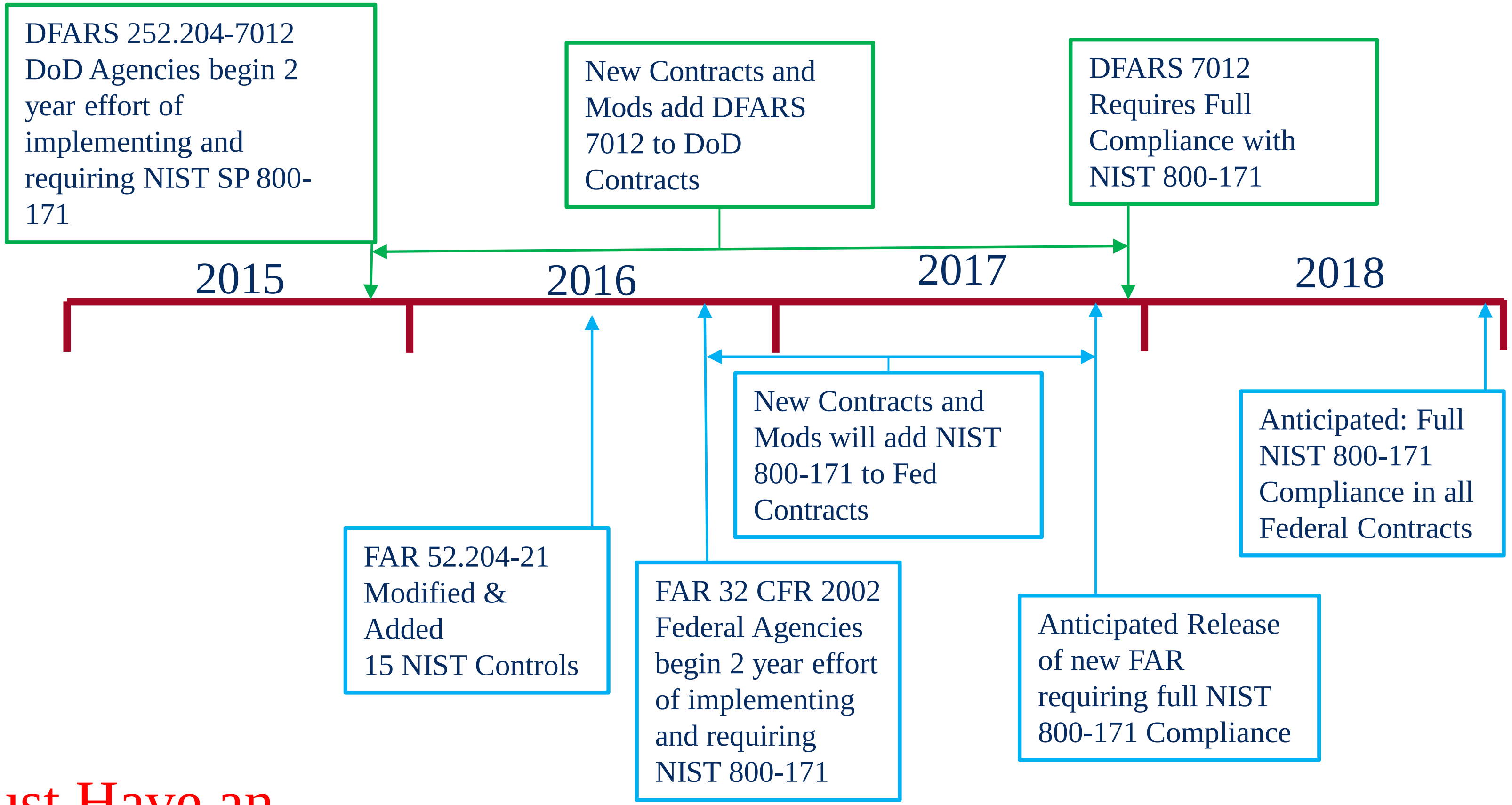
CUI / CDI

- CUI/CDI/CTI may be provided by the Government or developed in the performance of a contract
- 24 Categories / 83 Sub Categories listed in the CUI Registry at https://www.archives.gov/cui
- 2 Categories that almost all companies have
  - Controlled Technical Information
    - DoD 5230.24 “Distribution Statements on Technical Documents”
    - Engineering drawings and Data, Technical Reports, Specifications, Data Sets, Analysis, etc.
  - Procurement and Acquisition Information
    - ANY information related to acquisition actions
    - Cost and Pricing Information
    - Contract Information
    - Indirect Costs and Direct Labor Rates
- CUI Basic
  - Protect CUI Basic at the Moderate level with the controls in NIST 800-171
- CUI Specified (ITAR / HIPAA / etc.)
  - May only be upgraded to “CUI Specified” by a designating agency”
  - May require additional controls beyond NIST 800-171 and FISMA Moderate

What Does Adequate Security Mean?

- Type 1 System
  - Operated on Behalf of the Government
  - Must Comply with 252.239-7010
    - Calls out the DISA Security Requirements Guide v1R3
    - Specifies that the NIST 800-53r4 Control Set must be Used
    - If leveraging a Cloud Service Provider, the CSP must be FedRAMP Moderate and SRG L4
- Type 2 System
  - Operated by a Contractor, but not on behalf of the Government
  - Specifies NIST 800-171 Control Set must be Used
  - If leveraging a Cloud Service Provider, the CSP must be FedRAMP Moderate

NIST SP.800-171 DFARS/FAR Timeline



DFARS 252.204-7012 DoD Agencies begin 2 year effort of implementing and requiring NIST SP 800-171

New Contracts and Mods add DFARS 7012 to DoD Contracts

DFARS 7012 Requires Full Compliance with NIST 800-171

2015

2016

2017

2018

FAR 52.204-21 Modified & Added 15 NIST Controls

FAR 32 CFR 2002 Federal Agencies begin 2 year effort of implementing and requiring NIST 800-171

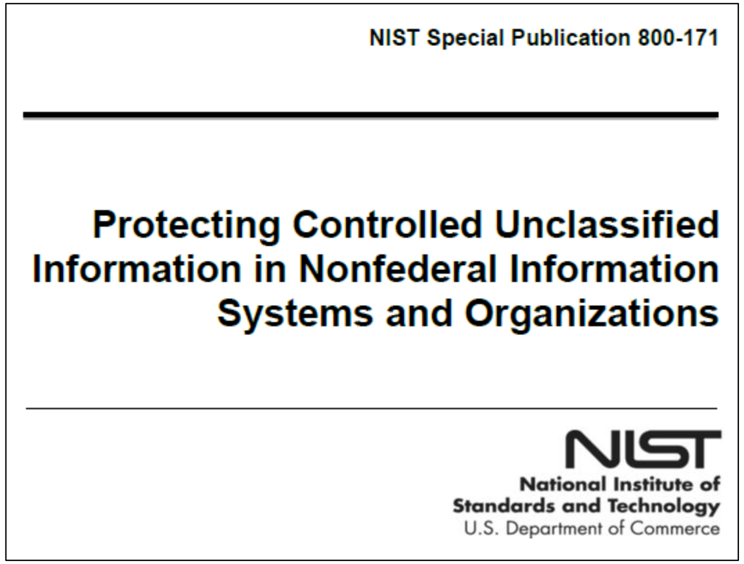
New Contracts and Mods will add NIST 800-171 to Fed Contracts

Anticipated Release of new FAR requiring full NIST 800-171 Compliance

Anticipated: Full NIST 800-171 Compliance in all Federal Contracts

Must Have an
SSP & POAM!

NIST 800-171 Compliance



NIST Special Publication 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Chapter 3
Security Control Families

- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System and Communications Protection
- System and Information Integrity

Policy Controls

Technical Controls

Office 365

SERVING THE EXPORT COMMUNITY FOR OVER 50 YEARS ®
SIA
Est. 1967

Industry’s Largest Compliance Portfolio

Worldwide

- ISO 27018
- ISO 27001
- Cloud Controls Matrix
- PCI DSS Level 1 *
- SOC 2 Type 2
- SOC 1 Type 2
- Shared Assessments
- Content Delivery and Security Association *

National

- HIPAA / HITECH
- European Union Model Clauses
- ENISA IAF
- EU-U.S. Privacy Shield
- Spain ENS
- Singapore MTCS Level 3
- Australian Signals Directorate
- New Zealand GCIO
- Japan Financial Services
- China MLPS*, TRUCS*, GB 18030*

Government

- Section 508 VPAT
- United Kingdom G-Cloud
- FedRAMP JAB P-ATO
- FIPS 140-2
- 21 CFR Part 11
- FERPA
- DISA Level 2
DISA Level 4
DISA Level 5
- CJIS
- IRS 1075
- FISMA
- NIST 800-171

How do you approach Compliance?

⬜ CSP manages

🟦 You manage (shared responsibility to protect)

▨ You or CSP manages (Depends on Provider and Configuration)

	SaaS	PaaS	IaaS	On-Prem
Data Governance and Rights Management	🟦	🟦	🟦	🟦
Client End-points	🟦	🟦	🟦	🟦
Account and Access Management	🟦	🟦	🟦	🟦
Identity and Directory Infrastructure	▨	▨	🟦	🟦
Application	⬜	▨	🟦	🟦
Network Controls	⬜	▨	🟦	🟦
Operating System	⬜	⬜	🟦	🟦
Physical Hosts	⬜	⬜	⬜	🟦
Physical Network	⬜	⬜	⬜	🟦
Physical Datacenter	⬜	⬜	⬜	🟦
Security	⬜	⬜	⬜	🟦
Privacy and Control	⬜	⬜	⬜	🟦
Compliance	⬜	⬜	⬜	🟦
Transparency	⬜	⬜	⬜	🟦
Reliability / Availability	⬜	⬜	⬜	🟦

Microsoft SaaS Platforms

	Office 365 Commercial	Office 365 GCC	Office 365 GCC High	Office 365 GCC High DoD
Customer Access	All	Government / Contractors	Government / Contractors	DoD Agencies
FedRAMP	Moderate	Moderate	Moderate	Moderate
DISA	Level 2	Level 2	Level 4	Level 5
ITAR Capable	No	No	Yes	Yes

- All Platforms can be made NIST 800-171 Compliant with proper policy and configuration
- Some features in Office 365 Commercial are not yet available in Office 365 GCC
- Office 365 GCC Requires a valid and approved DS-2032 Statement of Registration form

Microsoft IaaS / PaaS Platform

	Azure Commercial	Azure Government	Azure Government DoD
Customer Access	Government / Contractors	Government / Contractors	DoD Agencies
FedRAMP	Moderate	High	High
DISA	Level 2	Level 4	Level 5
ITAR Capable	No	Yes	Yes

- All Platforms can be made NIST 800-171 Compliant with proper policy and configuration
- Some features in Azure Commercial are not yet available in Azure Government
- Azure Government Requires a valid and approved DS-2032 Statement of Registration form

Key Office 365 Security Features

- Advanced Security Management
- Advanced Threat Protection
- Advanced Threat Analytics
- Azure Information Protection (Data Classification)
- Customer Lockbox
- Data Loss Prevention
- eDiscovery
- Mobile Device Management / Intune
- Office 365 Multifactor Authentication

Lessons Learned

CUI / CDI Lessons Learned
Every Defense Industrial Base company has CUI / CDI content
Outside of CUI / CDI needs, ITAR content is a major driver.

Office 365 Lessons Learned
Office 365 GCC High (Level 4) Environments take 6 weeks to provision
Custom Office 365 Deployment and Migration takes 4 – 9 Months
Templated Office 365 Deployments take 4 - 6 Weeks

Industry Lessons Learned
87% of all contracts released in 2017 have the DFARS 7012 Clause
Every DIB company we have talked to has at least 1 contract with the DFARS 7012 clause
Corporate IT and Security Policies are not well understood or implemented
Mobile Devices are ubiquitous and BYOD is the standard

COMPLIANCE IN THE CLOUD

David Harris
dharriscom@gmail.com
(253) 495-7974

Compliance in the Cloud

Compliance in the Cloud

AGENDA

1 **WHO IS AT RISK?**
Types of clouds, approach of cloud vendors, risk.

2 **CLOUD TYPES /= DATA TYPES**
What types of data can I place into which kind of clouds?

3 **CLOUD SECURITY STANDARDS**
What do I hold my cloud vendor accountable to and what do I look for in Trade Compliance insight?

4 **CLOUD RESIDENCY ISSUES**
How do I ‘know where’ and export is occurring and where it is initiated? What are the residency issues I need to be concerned with?.

5 **VALUE INTEGRATION**
How do I leverage electronic policy and enterprise release rules when using the cloud?

WHO IS AT RISK?

Are the Cloud Vendor's at Risk?

Generally, only for their own technology/technical data

Multiple AO's have been developed to address the Cloud Vendor and limiting or negating their risk as to Trade Control.

Most of ‘The Cloud’ is made up of SaaS vendors.
SaaS “Software as a Service”

PaaS
“Platform as a Service”

The ‘publisher’ of the content to ‘the cloud’ is considered the ‘exporter’ in most cases.

Although this can change with encryption and release/use when decrypted.

What is published to ‘The Cloud’ is subject to Trade Control Compliance when applicable.

If the wrong party gets access to the information and a disclosure ensues, it is the publisher of the information who may be most at risk of an export violation.

IaaS
“Infrastructure as a Service”

CLOUD TYPES /= DATA TYPES

What types of data can I place into which kind of clouds?

- SaaS – Software as a Service

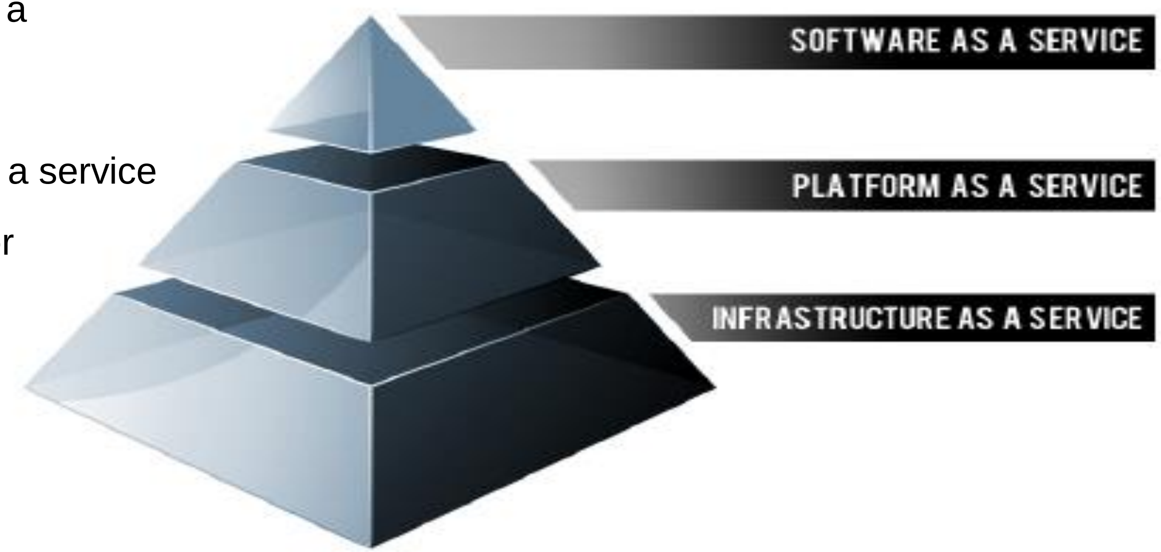
  Execute Applications

- PaaS – Platform as a Service

  Develop applications using a common platform

- IaaS – Infrastructure as a service

  Provide an Infrastructure for applications and platforms



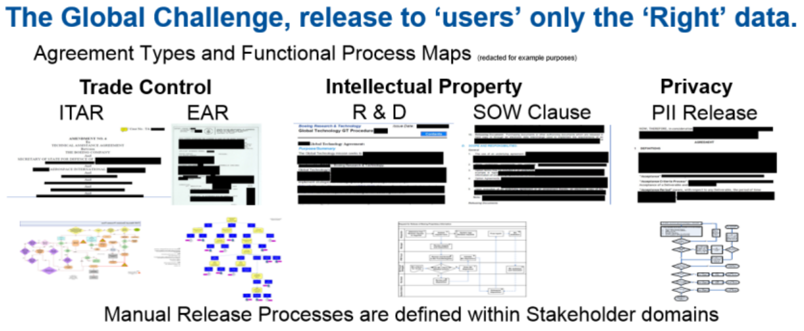
CLOUD SECURITY STANDARDS

What do I hold my cloud vendor accountable to and what do I look for in Trade Compliance insight?

1. The SLA (Service Level Agreement)
2. Record keeping and forensics
3. Cloud access, performance and global availability
4. Compatibility with your infrastructure
5. Federation of your existing SOA and BPM (Business Process Management)
6. Understanding of Trade Control sensitivities
7. Disclosure and restriction of resource allocation to ‘your servers and data’
8. DDTC Registration
9. Disaster Recovery and Fault Planning
10. Computing and Cyber security standards and certifications

CLOUD RESIDENCY ISSUES

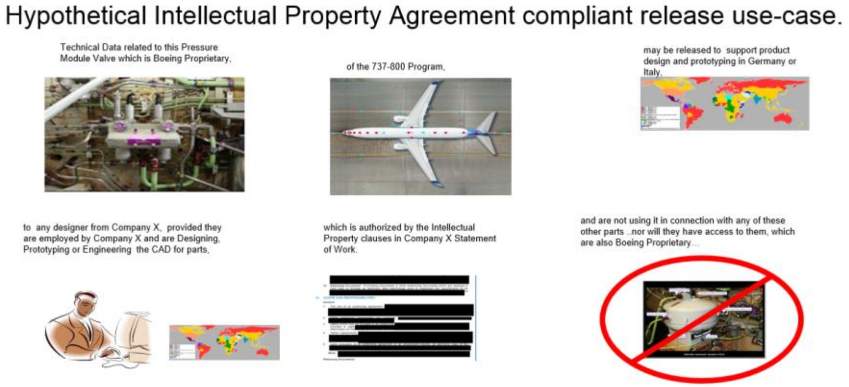
How do I ‘know where’ an export is occurring and where it is initiated? What are the residency issues I need to be concerned with?.



The Global Challenge, release to ‘users’ only the ‘Right’ data.

Agreement Types and Functional Process Maps (redacted for example purposes)

Manual Release Processes are defined within Stakeholder domains



Hypothetical Intellectual Property Agreement compliant release use-case.

Technical Data related to this Pressure Module Valve which is Boeing Proprietary,

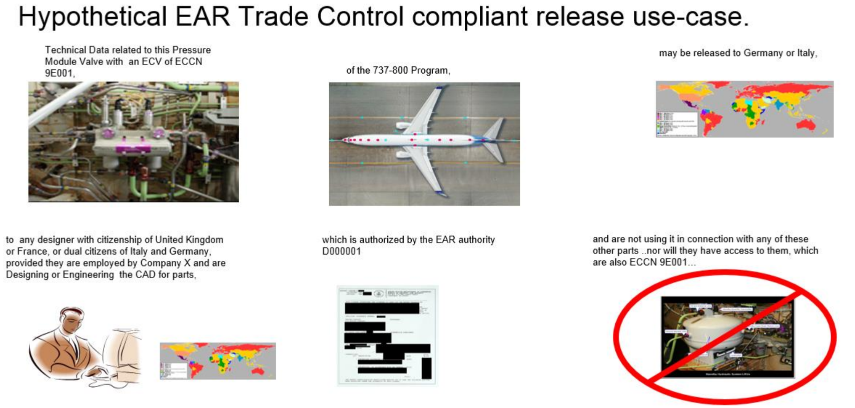
of the 737-800 Program,

may be released to support product design and prototyping in Germany or Italy,

to any designer from Company X, provided they are employed by Company X and are Designing, Prototyping or Engineering the CAD for parts,

which is authorized by the Intellectual Property clauses in Company X Statement of Work.

and are not using it in connection with any of these other parts ..nor will they have access to them, which are also Boeing Proprietary...



Hypothetical EAR Trade Control compliant release use-case.

Technical Data related to this Pressure Module Valve with an ECV of ECCN 9E001,

of the 737-800 Program,

may be released to Germany or Italy,

to any designer with citizenship of United Kingdom or France, or dual citizens of Italy and Germany, provided they are employed by Company X and are Designing or Engineering the CAD for parts,

which is authorized by the EAR authority D000001

and are not using it in connection with any of these other parts ..nor will they have access to them, which are also ECCN 9E001...

The Right Information
From the Right place
To the Right place,
The Right Person,
The Right Company,
For the Right Reason,
Aligned to the Right authority…
Right Away!

VALUE INTEGRATION

How do I leverage electronic policy and enterprise release rules when using the cloud and/or Microservices?

Federation throughout the extended ecosystem requires technology and business process management alignment for success.

The culture must adopt a new way of thinking about and leveraging the value of data.

My Skill Cloud

skills
friends
sharing
enjoyed
help
solving
career
supporting
problems
experience
good
learning
mentoring
relationship
training
networking
positive
scheme
mentor
staff
security
International
trade
rights
intellectual
property
safety
business
protection
technology
people
network
computer
lock
secrecy
law
identity
attack
theft
crime
criminal
cyber
SECURITY
RISK
COMPLIANCE
PLAN
FIREWALL
GOVERNANCE
AUDITORS
SCOPE
FINDINGS
CONTINUITY
MANAGEMENT
BACKUP
DISASTER
RECOVERY
PASSWORDS
AUDIT

Questions and Answers

Thank you

David Harris
dharriscom@gmail.com
(253) 495-7974

http://SIA.socialqa.com