Charts from the January 2016 Federal Cloud Computing Summit

Justin F. Brunelle (MITRE Chair)

Cloud O&M: Challenges and Solutions

Sara Mosley, Jeff Wootton, Mano Malayanur

1. Intermediation Layer / Reference Arch. / IaaS/PaaS

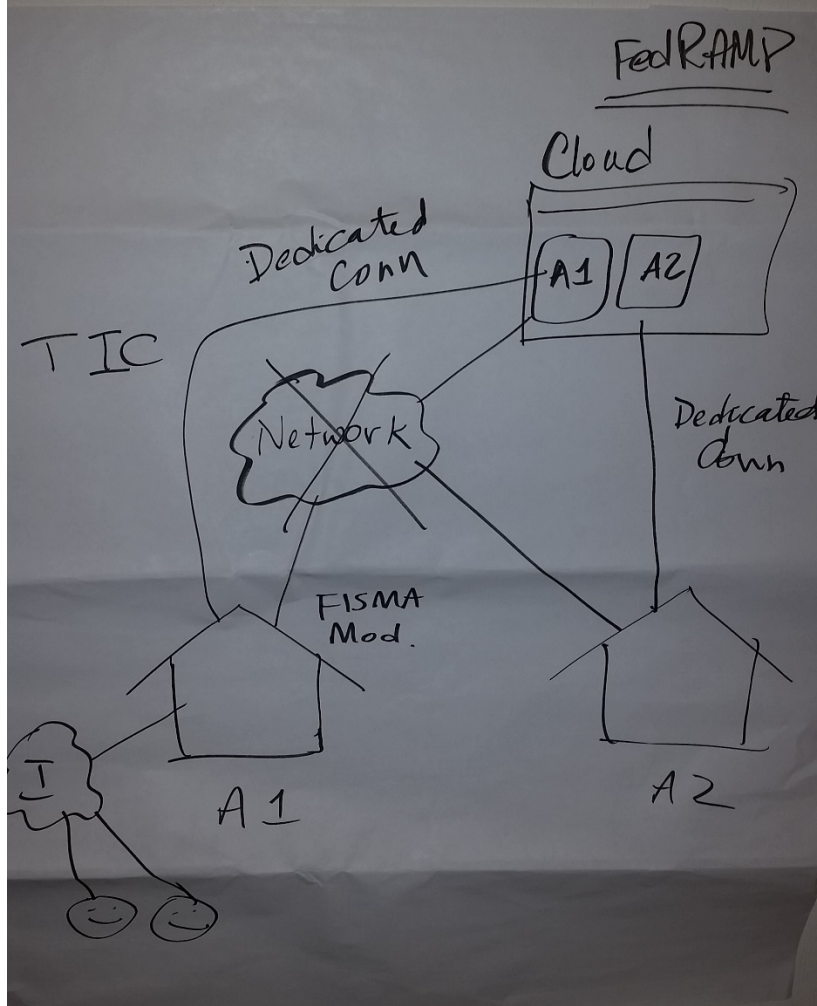
2. Human / Change Mgmt. Policy / Training / Education

3. Catalog of CSPs / Portability / Granularity

1. Intermediation Layer / Reference Arch. / IaaS/PaaS

2. Human / Change Mgmt. Policy / Training / Education

3. Catalog of CSPs / Portability / Granularity



C1. Challenge of inaction
⇒ Education, Training ⇒ Policy, Culture

C2. Traceability from consumption to charge back (who ordered)
- Monitoring of consumption
⇒ Metering

C3. ~~Th~~ Complexities when multiple providers are involved

C4. Control – human "tail"
⇒ Automation

C5. Acq counter-intuitive to "measured service"

C6. ⇒ Brokering technology that facilitates charge back.
(automated service mgmt platform)
(technologies exist)

C6. Legislation required
OMB policies
⇒ Ref architecture (process) that lays out a path to cloud adoption

⇒ Traceability from service catalog to billing
⇒ Companies may provide such services

C7. True config mgmt DB
- Monitoring
- Logs
⇒

C8. Agency is accountable but does not control the env. (R&Rs) – fine print

C9. Silos – culture
human element
⇒ Answer "what's in it for me" – training
⇒ point out the +ve

C10. Portability
⇒ open source
⇒ part of the contract
⇒ cloud broker SLA
⇒ CSA – roles & resp
⇒ NIST – ~~dept~~ ref. arch. 500-2917
⇒ Independent entity to rate CSP

C11. Complex relationship ⇒
between CSP, consumer, broker
- contractual/legal
- privity of contractor

C12. "Go to cloud" mandate; no specifics
- service model
- deployment model
⇒ categorization

C13. Where is JIE in standardization all this?

C14. Does Mission Partner Env. resolve any issues related to cloud adoption?

C15. Identity & Access Mgmt.

C16. Is there an overarching entity that manages the "cloud"?
- O&M – ITIL
- Change mgmt
- Config ~~pr~~ mgmt
- Problem mgmt
- Incident mgmt
- COOP
- Rel mgmt

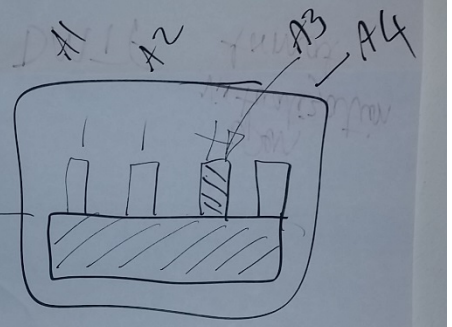
C17. Dev/Test env -
better in the cloud?
Prod?

Experience
- servers/db/storage
- physical or virtual

C18. CMDB (again)
⇒ Tied to change/release mgmt.
⇒ How much control do you need

C19. FISMA - cloud vs. agency
⇒ FedRAMP — A1 — A2 (III)

413



283 ✓
✓
✓
FedRAMP ✓

C20. (Includes CONUS requirement?)

Planning for Cloud migration: Fail Early and Often

Jimmy Jones, Greg Mundell, Howard Small

- Cloud IT Bill

Industry Needs

- Define Outcomes + mission objectives
- SLAs
- How contracts are written
- Tie contracts people to program people
- Standard contract language
- Cloud IPT
- Industry days + RFIs (less + more)
- One on One Meetings
- Open Process
- Less LPTA

Challenges (2)

- Vendor lock in
- Monitoring · Applications + Infrastruct
- Contracting
- Trust
- Culture
- No plan - adopting
- training
- Legacy
- Architecture
- Shadow IT
- Data Loss
- Impact Levels
- Policy - US + overseas

Govt Needs

- Seperate hosting from dev, (or not)
- SaaS
- SLA
- More customization
- Understand mission
- Hire more vets

- Start by standing up
  Dev/Test in the cloud

Quick wins
- Website in cloud
- SaaS
- Storage
- DR COOP
- Training Env.
- Sandbox
- leverage SLAs
- Portability

Case Studies
- Proof of Concept
  - ID challenges
  - Learning Process
- Review of classification levels
  - i.e. Fisma High
- Cloud Strategy
  - w/ Governance
  - Vision
  - roadmap

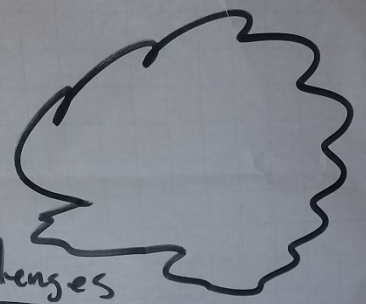
- Collaboration
  - Get people to the table
  - Invested in the outcome
  - Ownership
  - Create a cloud strategy
    - Mandate for implementation
  - Buy in outside of HQ
- Consolidation
- Create end goals + outcomes

- Process
  - How to use the cloud
- UI
  - Modify the apps + workflow to fit cloud
- Redefine mobility
  - Not tied to a device
  - Cloud is key
- Shared Service
  - Econ. of Scale

- Data Center Consolidation
  - Cloud as an option
- Need Value Prop for Cloud
  1
- Lack of common understanding of cloud → what it is
  - what it is you want to achieve
  2 Benefits of cloud
  3 Implementation steps
  } lack of understanding
- Need training + Education

- Cloud access point
- TIC is a challenge
  - time
  - cost
- Est. Gov't-wide connection points
- Shared Services Providers
  - Challenges w/ SLAs
- Data on performance + security
  - Monitoring
  - How do you define downtime

- Moving platforms + DBs to the cloud
  - Evaluate options
  - Re-arch.
- HA in the cloud
- Choose 2 CSPs
- Leverage IDIQs to buy cloud services
- Seperate contracts for data + hosting
- Funding needs to change
  - utility model
  - FAR changes
  - COLOR OF MONEY



Challenges
- Connect to "things" not in the cloud
- Data ID
- Security
- Lost control
- Costs / Financial Model
- Exit strategy / Portability
- Leadership buy in
- People
- Change Management
- Optimizing to leverage cloud

Architecting Future Clouds

Greg Fritz, Adam Alphin, Duy Huynh

Challenges

- DoD: Low bandwidth, at-the-edge, isolated remote networks, multi-tenancy, storage/software as a service
- DoE: Provide services to Students and Financial aid across the Universities across the US.
- DoL: Pensions/minimum wage fraud, sensors in mine, users in the field doing investigations
- DoJ: Few enterprise services, commoditized services, manageable software as service, security, procurement
- Procurement process: getting the best bang-for-the-buck, instead of just getting the best price.
- Classification/Segmentation of data: move non-classified data onto clouds
- Limited service/agility
- Security: some government community clouds are being targeted because they stand out
- FedRamp bottleneck
- SLAs are inadequately defined or even left out
- Baselining - understanding where government system are before moving over to the cloud
- Cloud computer for OCONUS
- Not being locked in to proprietary technology
- Data portability
- Open standards for software

Discussion Summary

- What is the scope of the discussion of what pertains to the cloud?
  - Government Community Cloud
  - Public Cloud
  - Hybrid Clouds
- Provide everything outside of agency's core competencies as a service
- The future is in the mobile based realm; applications are moving towards mobile platforms.
- Agile development – go towards creating an organization with increase agility and rapid development
- Government to move towards a community cloud and eventually move towards a public cloud
- Cloud is more complex than previous technologies due to the many things it covers and will take more time to adopt
- Cloud implementation will struggles with security, procurement, training, and the need for culture change.
  - There needs to be a culture change from top-to-bottom.

Important Findings

- Training of decision makers, engineers, etc to be more aware of cloud technologies.
- Start “getting your feet wet” by putting unclassified data into the community/public cloud and start somewhere.
- Research automated data classification
  - Product that differentiate between data types (classified data, non-classified), so they can be parsed out and placed in the appropriate environment. This allows more data to be placed on the public clouds instead of creating a private or hybrid cloud.
- Move towards are going towards the public cloud, and DOD IC will stay on the community cloud with sensitive data.
- Move towards utility computing
- SLA need to be incorporated early on and vetted well when moving over to the cloud environment
- Future cloud architecture should include the computing all the way to the end-user
- Have reserve funds in a pilot project to adapt to new technologies
- Review what’s worked in the past and pick what’s been successful and lessons learn and adapt that towards future projects/task

Adapting Cloud to Technology

Wu Feng, Chet Hayes, Demetrius Davis

Bottom Lines Up Front

1) Our message to leadership should not be about moving everything to the “cloud” – it needs to be about changing the way the government does IT to better adapt to and implement new technologies, market shifts, standards and best practices.
    - Our biggest challenges are not technology-related
    - Cultural changes are needed to cut through bureaucracy and outdated IT policies that impede government use of emerging technologies such as Internet of Things (iOT) and wearables
2) Fear of the unknown impedes our ability to identify and assess risks and forge true partnerships with industry.
    - Switch from being “risk-averse” to being “risk-tolerant”

“To Do” List

- “Order from the menu” (when possible)
  - Talk mission and business objectives with vendors – not just “requirements”
  - Custom, hard-to-integrate solutions have short ROI, long maintenance tails
- Revamp business processes (e.g., governance, acquisition, management)
  - Technology is moving too fast for current set of policies, processes
- Continue educating the government community, leadership
- Strategic planning is needed before any mass migrations to cloud
  - Assess portfolio before forklifting apps, data to the cloud
  - Use tech refresh cycles as an opportunity to re-engineer major systems

To-Do List

- Continuing education
- Strategic planning-
  - → high-level planning needed (get away from "weeds")
- Revamp acquisition, management processes
  - → i.e., FedRAMP
- Truly partner w/ industry
  - → Resist fear of unkno
  - → Risk tolerant (vice risk adverse)
  - Manage risks

~~Challenges~~ Opportunities

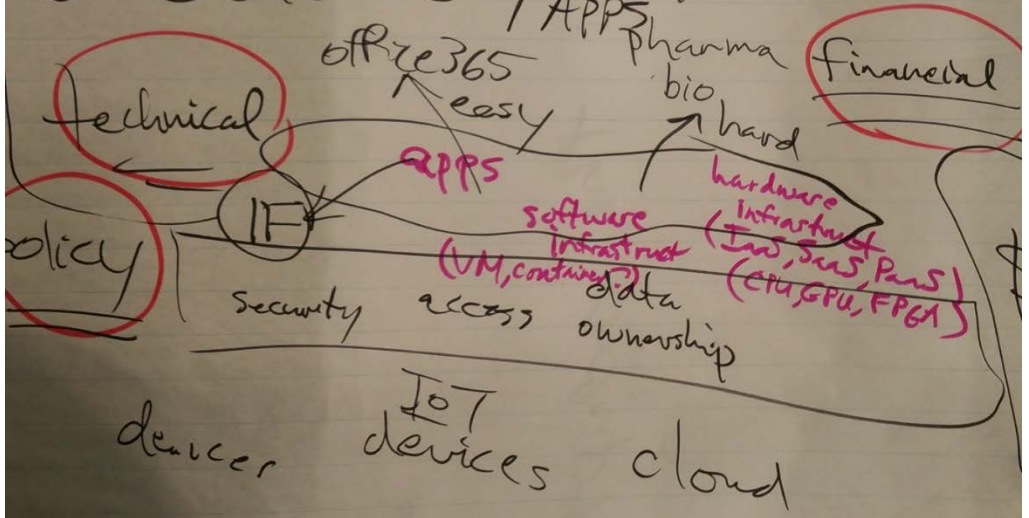
- Bureaucracy
  - Policies
- Risk acceptance

Fear

Need to mitigate

Infrastructure ↕

- Leadership buy-in



Standards and Best Practices for Security and Privacy Management in Cloud

Joe Paiva, Federico Simonetti, Bob Natale

RNATALE@MITRE.ORG

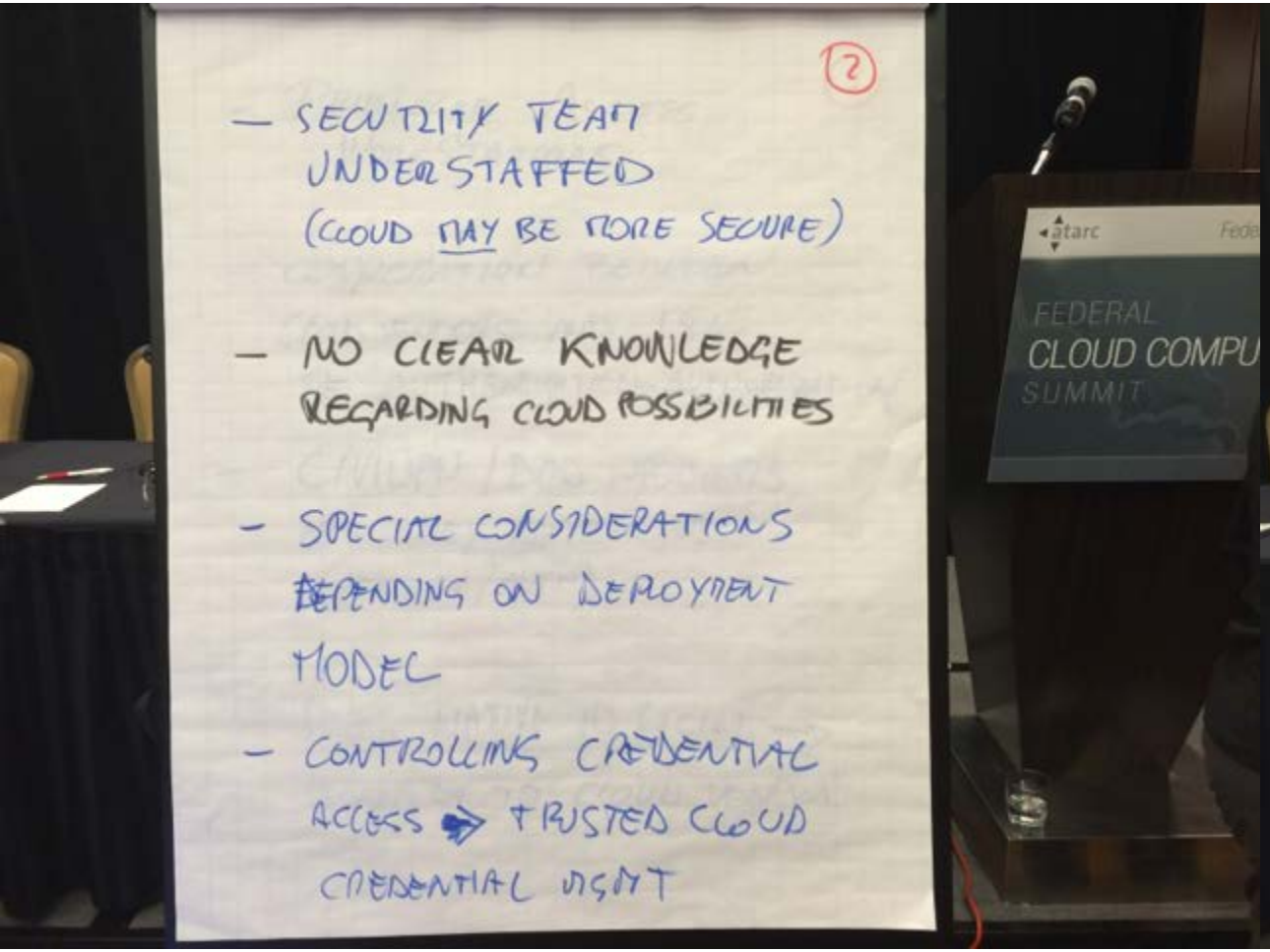
FEEL FREE TO E-MAIL COMMENTS TO ME FOR INCLUSION IN SESSION WHITE PAPER

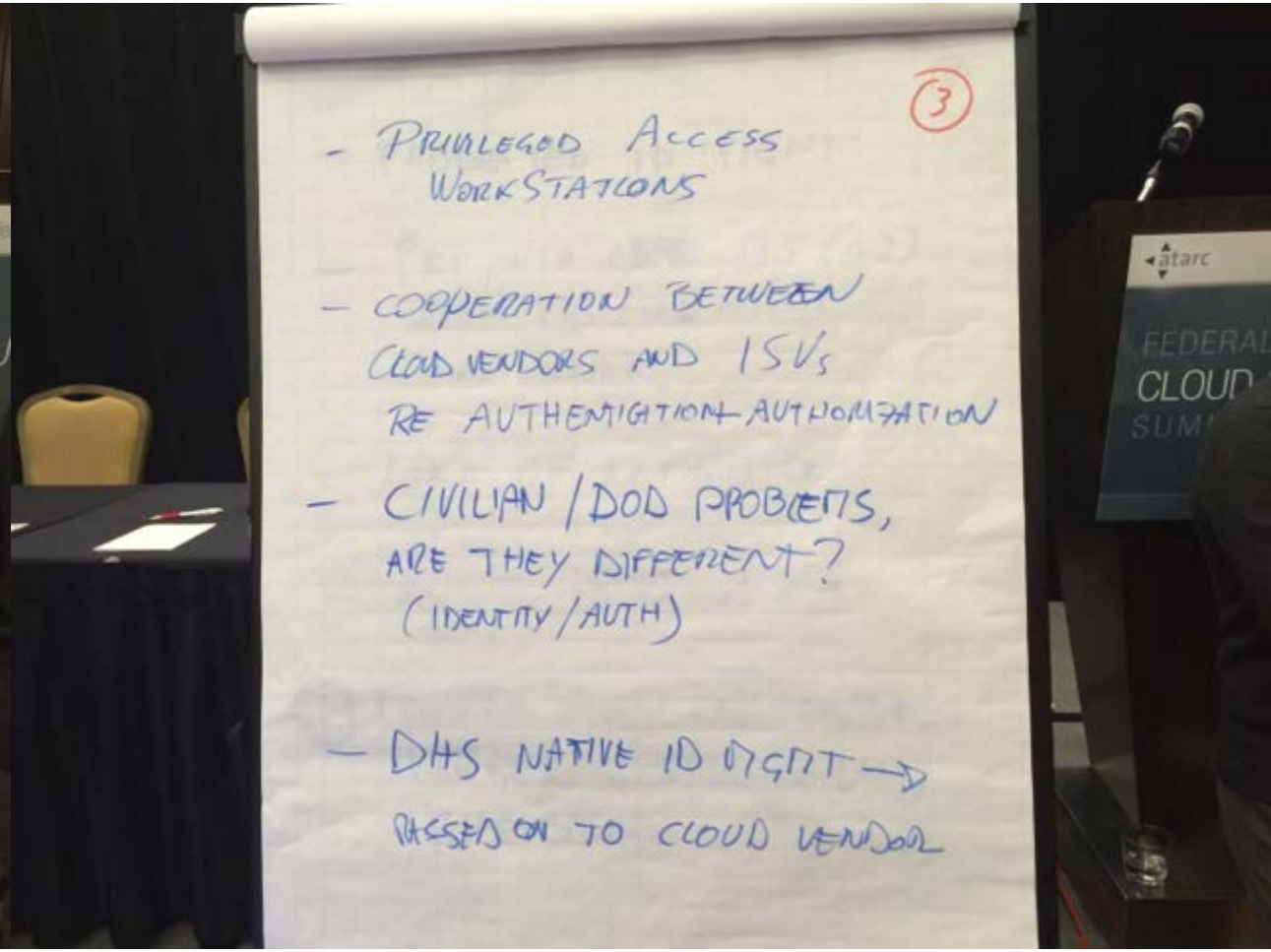
Joe.Paiva@Trade.gov

F.SIMONETTI@EXTENVA.COM

1

- ARE THERE EXISTING STANDARD OR DO WE NEED NEW ONES
- INFRASTRUCTURE: COMPUTING NOT THE SAME AS STORAGE
- PRIVACY PRACTICES


2
- SECURITY TEAM UNDERSTAFFED (CLOUD MAY BE MORE SECURE)
- NO CLEAR KNOWLEDGE REGARDING CLOUD POSSIBILITIES
- SPECIAL CONSIDERATIONS DEPENDING ON DEPLOYMENT MODEL
- CONTROLLING CREDENTIAL ACCESS → TRUSTED CLOUD CREDENTIAL MGMT
atarc
FEDERAL
CLOUD COMPU
SUMMIT


3
- PRIVILEGED ACCESS WORKSTATIONS
- COOPERATION BETWEEN CLOUD VENDORS AND ISVs RE AUTHENTICATION AUTHORIZATION
- CIVILIAN / DOD PROBLEMS, ARE THEY DIFFERENT? (IDENTITY / AUTH)
- DHS NATIVE ID MGMT → PASSED ON TO CLOUD VENDOR
atarc
FEDERAL
CLOUD

4

- FEDERATED ID MGMT
- PKI AUTH OVER TLS (1.2) WITH PFS (AND CLIENT CERT AUTH)
- LACK OF DEFINITIONS
- NIST 800-173

⊕ TRUSTED CLOUD CREDENTIAL MANAGER (LEVERAGING IAM)
- ROLE-BASED

5

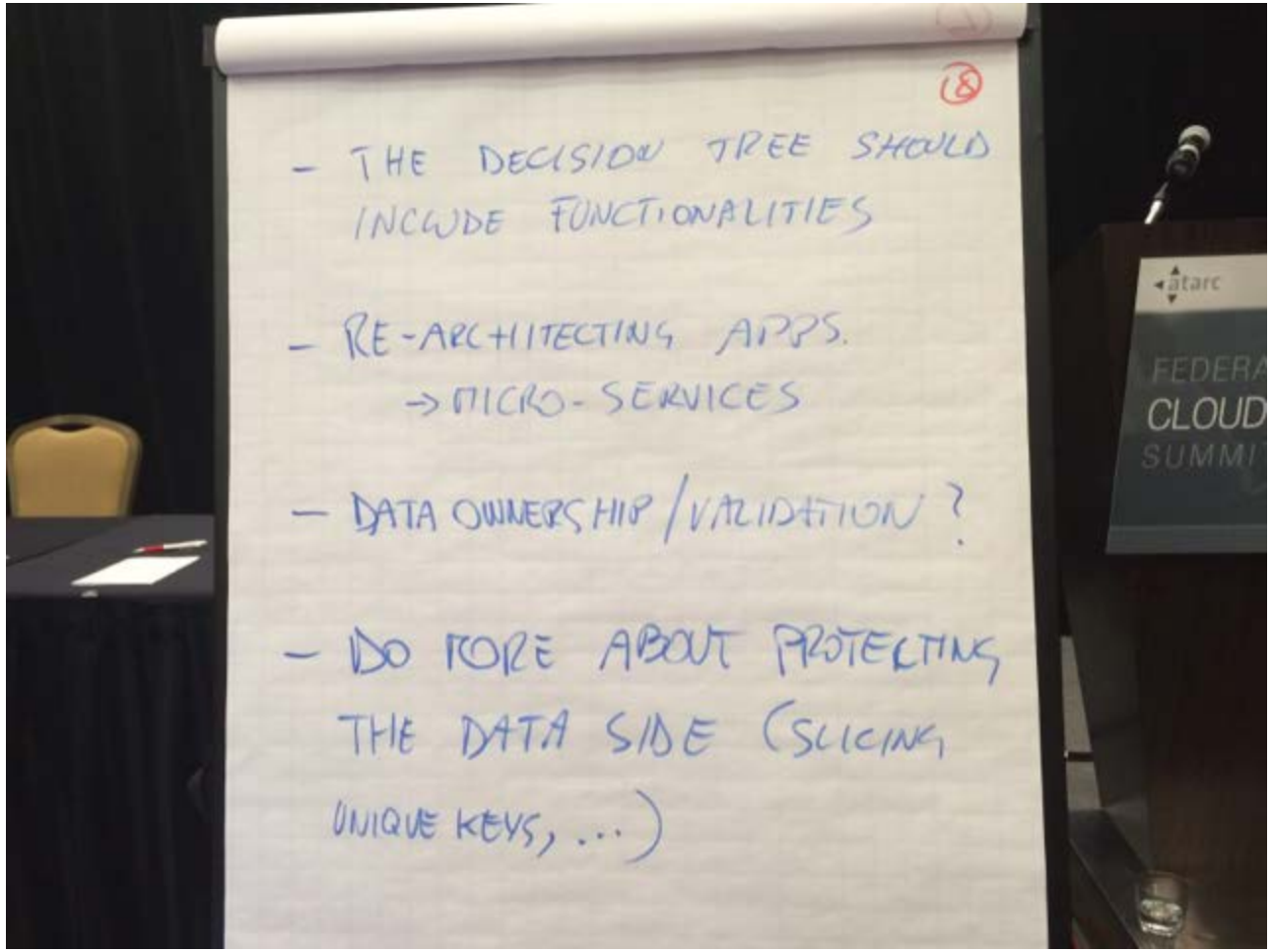
- BEST PRACTICES FOR NETWORK SEGMENTATION ?
- TWO-FACTOR AUTH
- SOFTWARE-DEFINED PERIMETER (NETWORK)
- CLOUDSECURITYALLIANCE.ORG
- CLOUD STG ACCESS SECURITY TOOLS OWNED BY ENTITY DEPLOYED TO 3RD PARTIES

6

- CLOUD ACCESS SECURITY BROKER
- CENTRAL SECURITY MGMT SYSTEM → CLOUD AGNOSTIC
- CENTRALIZED MGMT OF DATA ACCESS POLICIES – INDEPENDENT OF AUTHENTICATION (SUPPORT MULTIPLE AUTHS)
- CENTRALIZATION OF CSP IS KEY

7

- MOVING APPS TO CLOUD BUT SUCH APPS NEED ACCESS TO LOCAL DATA
- A LOT OF SYSTEMS ARE NOT MODERN
- MAYBE IT'S BETTER TO NOT MOVE THINGS THAT AREN'T READY?
- IF STRUCTURED STG THEN APP + DATA SHOULD BE DEPLOYED TOGETHER (SAME INFRASTRUCTURE)


8
- THE DECISION TREE SHOULD INCLUDE FUNCTIONALITIES
- RE-ARCHITECTING APPS.
→ MICRO-SERVICES
- DATA OWNERSHIP / VALIDATION ?
- DO MORE ABOUT PROTECTING THE DATA SIDE (SLICING UNIQUE KEYS, ...)
atarc
FEDERA
CLOUD
SUMMI