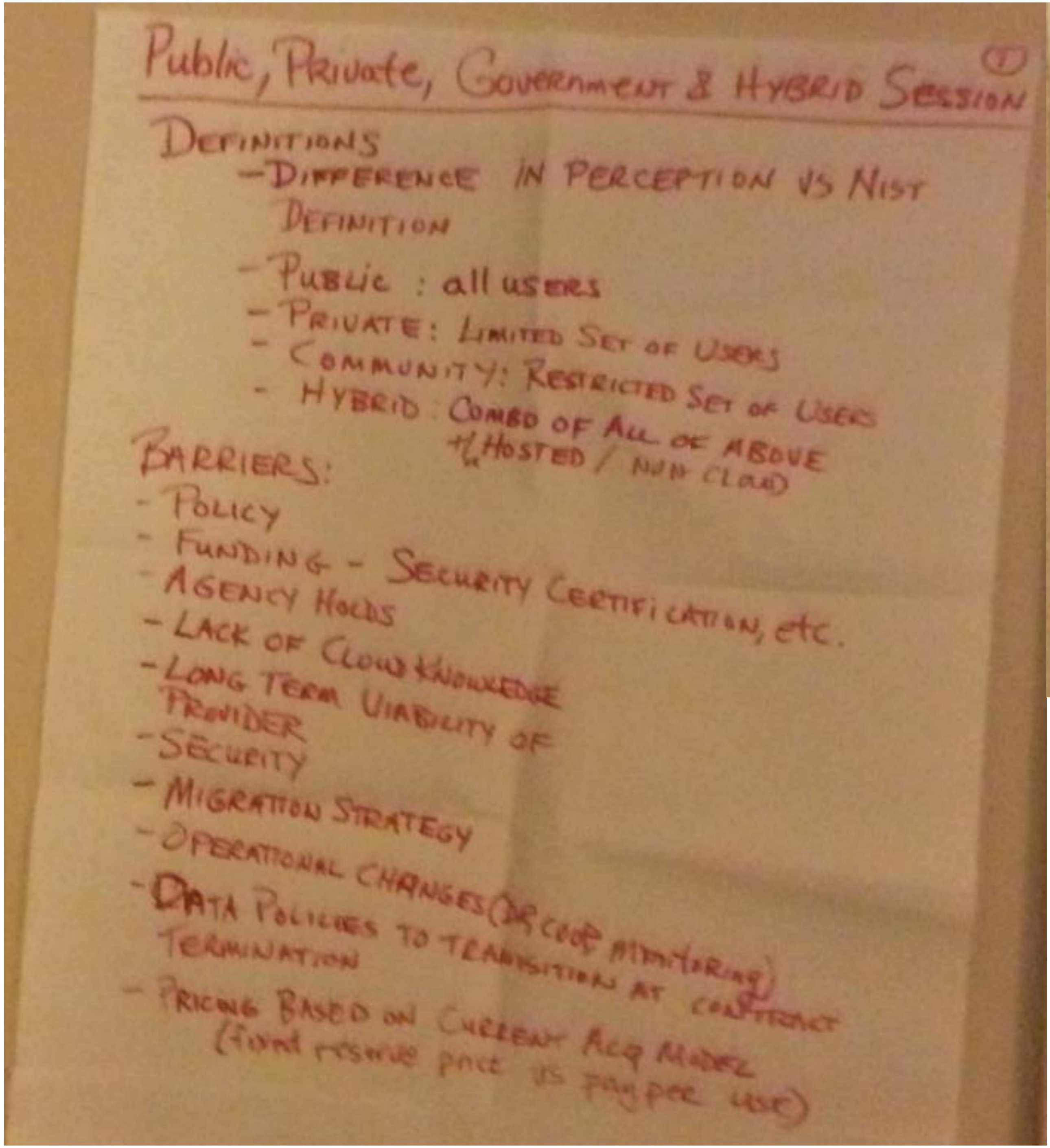
Session Notepads from the January 2015 MITRE-ATARC Collaboration Sessions

Public, Private, Government, or Hybrid clouds?



1

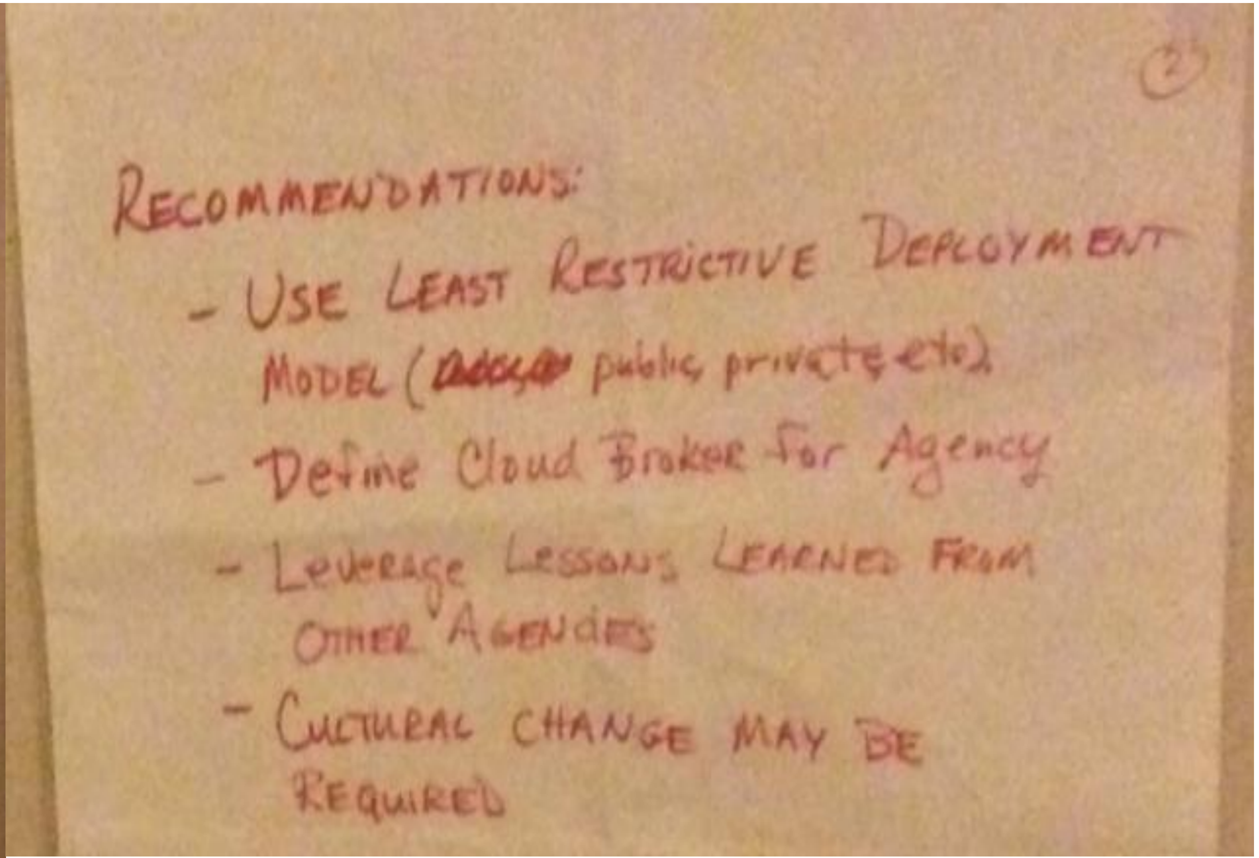
Public, Private, Government & Hybrid Session

Definitions

- Difference in perception vs NIST Definition
- Public : all users
- Private: Limited set of users
- Community: Restricted set of users
- Hybrid: Combo of all of above + hosted / non cloud

Barriers:

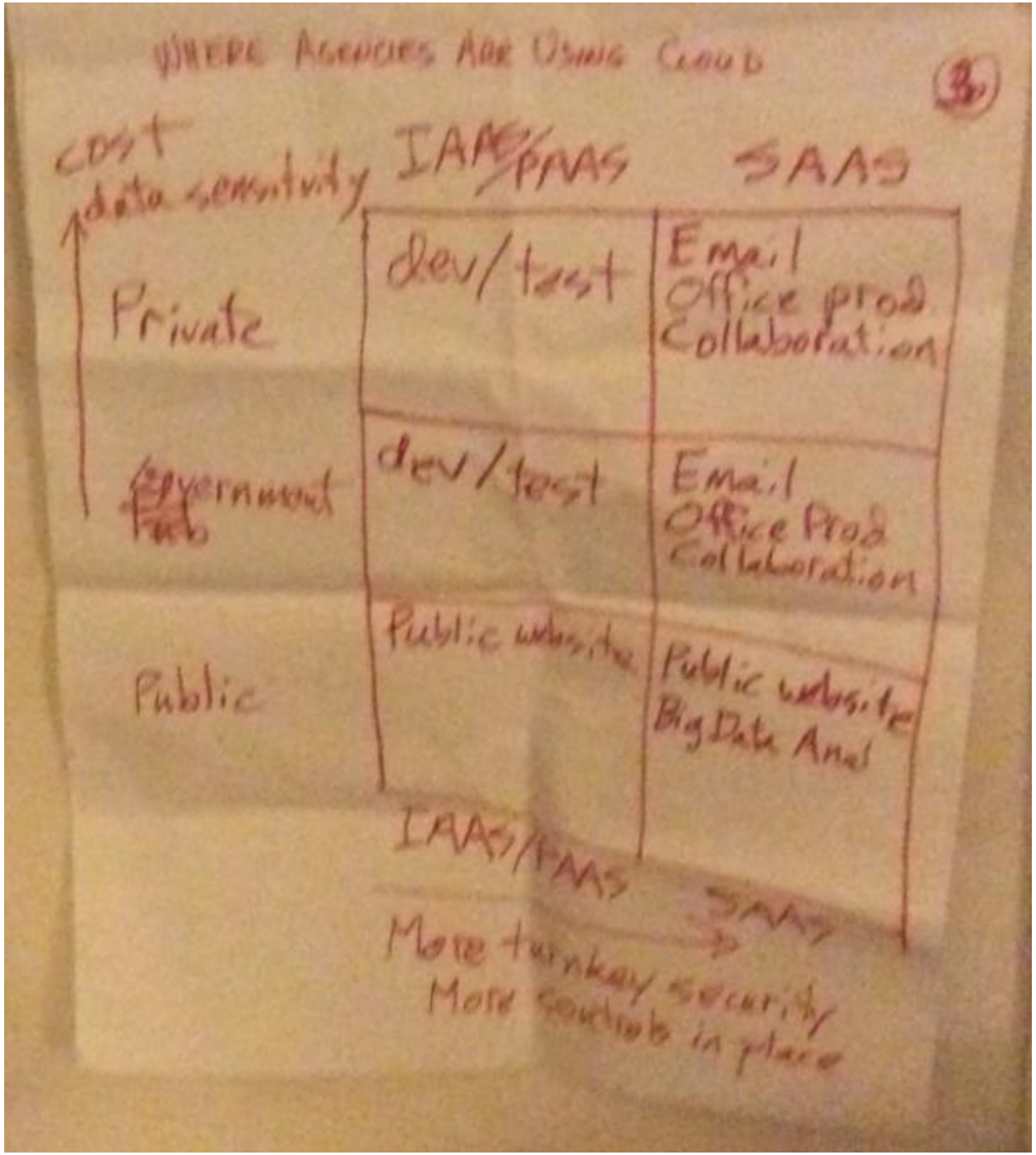
- Policy
- Funding - Security Certification, etc.
- Agency Holds
- Lack of Cloud Knowledge
- Long Term Viability of Provider
- Security
- Migration Strategy
- Operational Changes (DR, COOP Monitoring)
- Data Policies to transition at contract termination
- Pricing Based on Current Acq Model (fixed reserve price vs pay per use)



2

Recommendations:

- Use Least Restrictive Deployment Model (public private & etc)
- Define Cloud Broker for Agency
- Leverage Lessons Learned from Other Agencies
- Cultural change may be required



WHERE AGENCIES ARE USING CLOUD

3

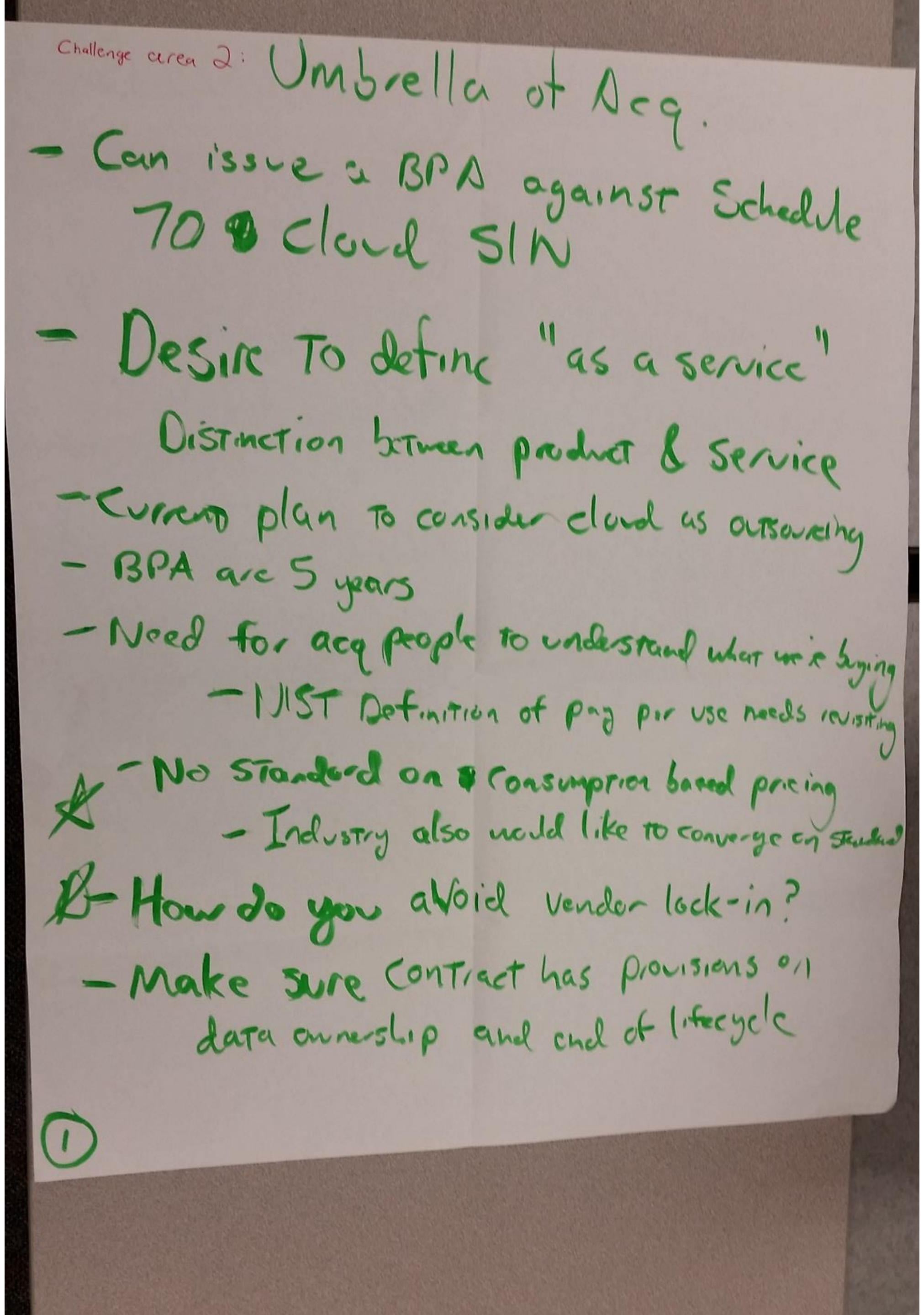
cost
data sensitivity ↑

	IAAS/PAAS	SAAS
Private	dev/test	Email Office prod Collaboration
Government Fed	dev/test	Email Office Prod Collaboration
Public	Public website	Public website Big Data Anal

IAAS/PAAS → SAAS

More turnkey security
More controls in place

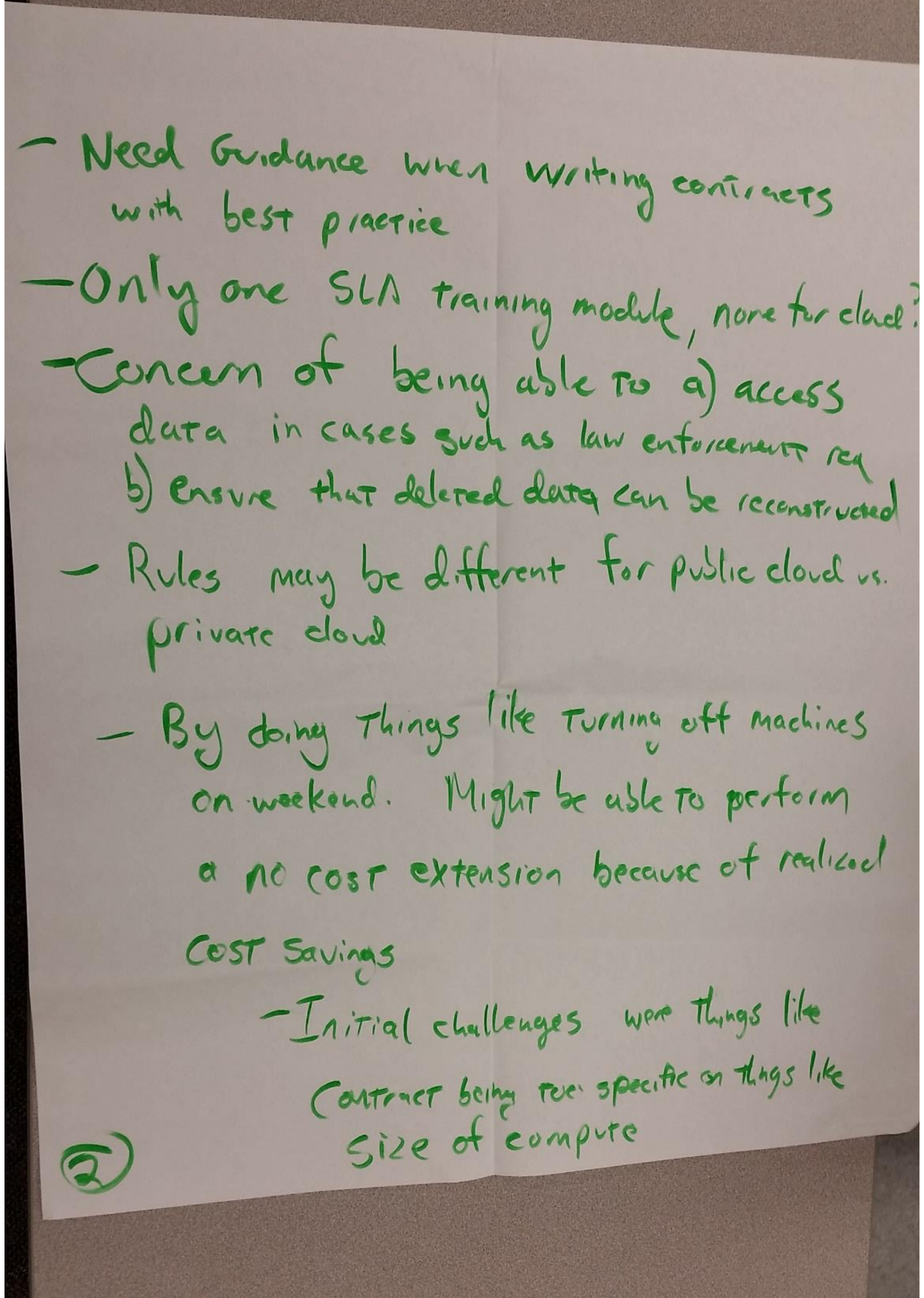
The Umbrella of Acquisition



Challenge area 2: Umbrella of Acq.

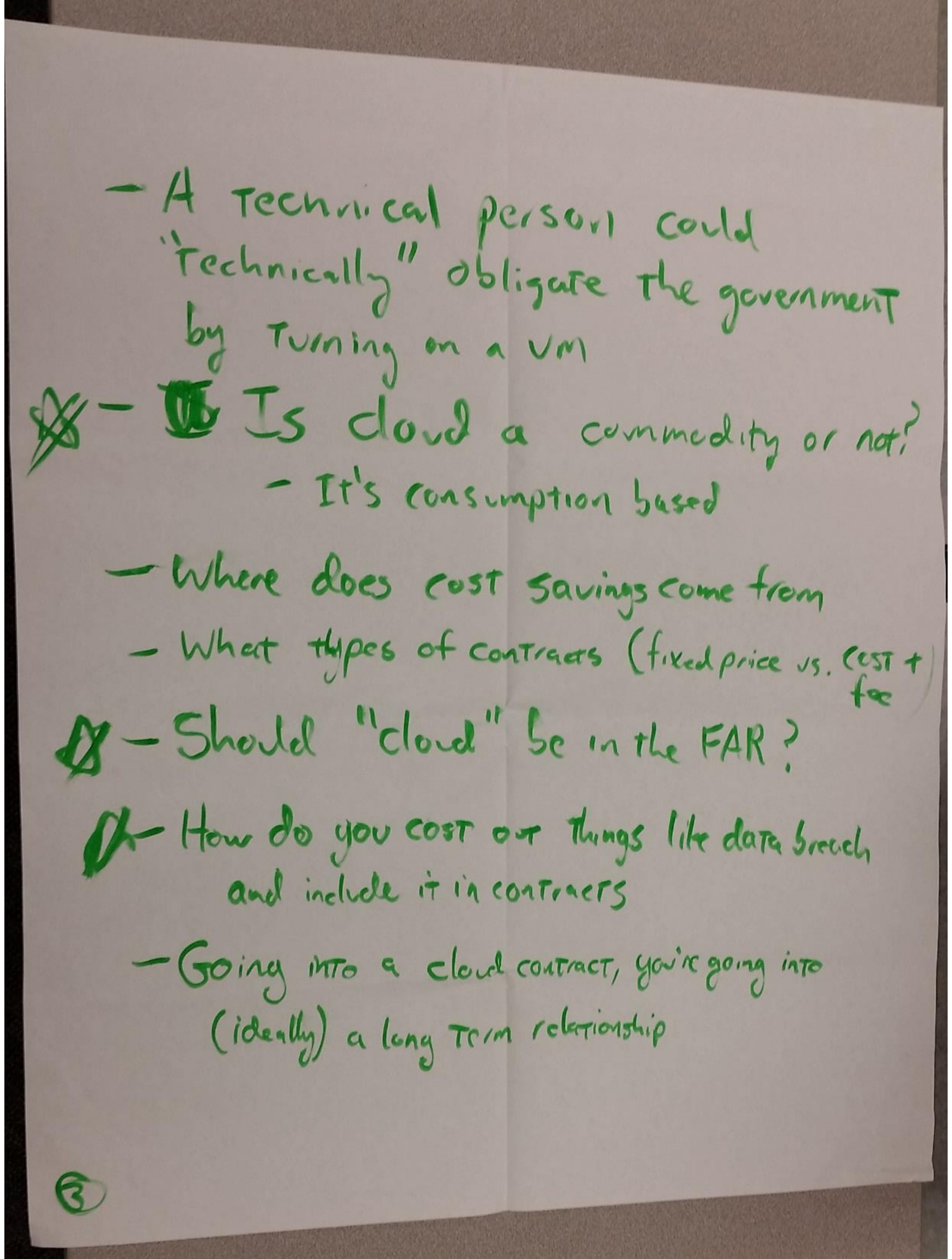
- Can issue a BPA against Schedule 70 Cloud SIN
- Desire To define "as a service"
  Distinction between product & service
- Current plan To consider cloud as outsourcing
- BPA are 5 years
- Need for acq people to understand what we're buying
  - NIST Definition of pay per use needs revisiting
- ★ No standard on consumption based pricing
  - Industry also would like to converge on standard
- ★ How do you avoid vendor lock-in?
  - Make sure contract has provisions on data ownership and end of lifecycle

①



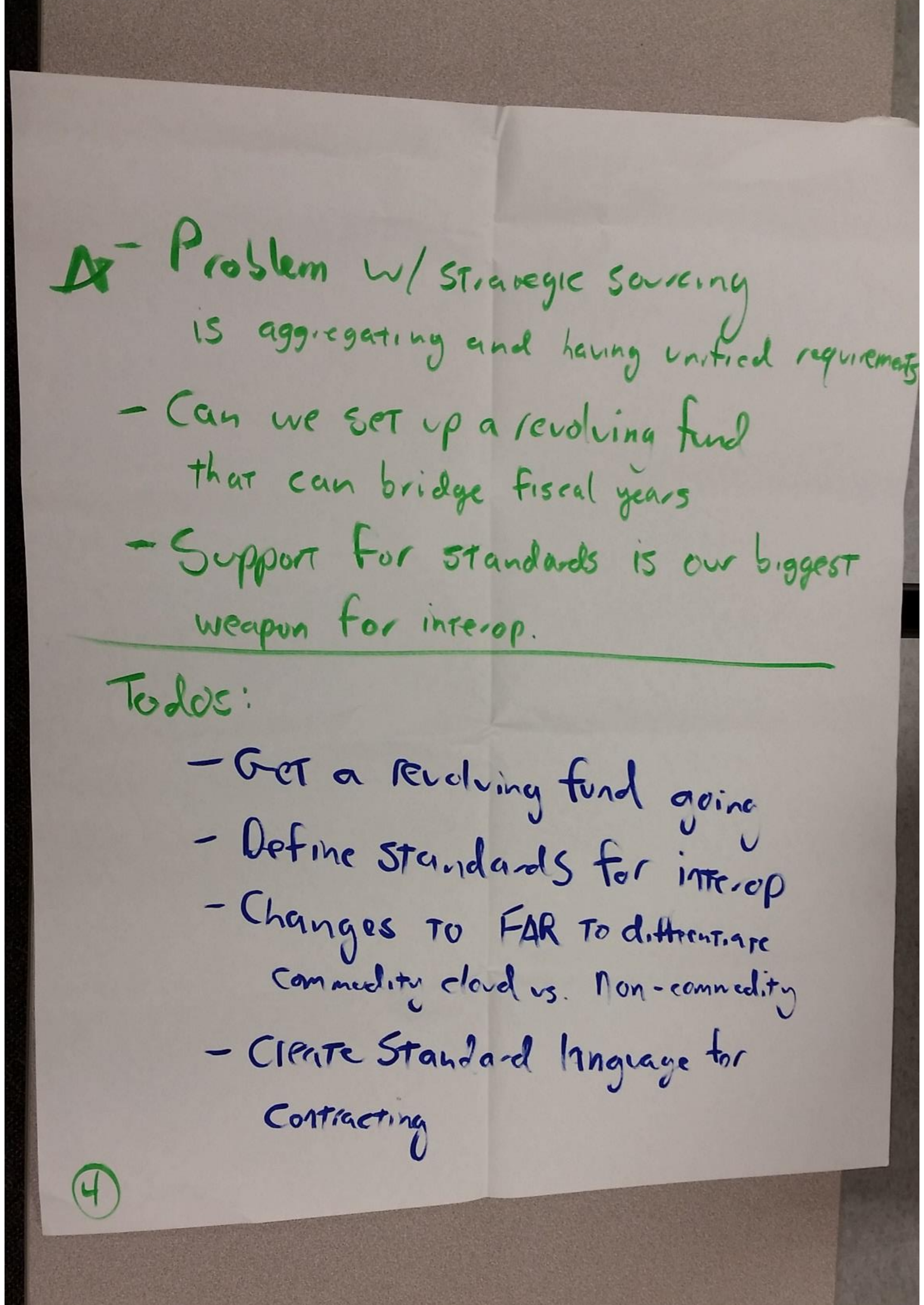
- Need Guidance when writing contracts with best practice
- Only one SLA training module, none for cloud?
- Concern of being able to a) access data in cases such as law enforcement req b) ensure that deleted data can be reconstructed
- Rules may be different for public cloud vs. private cloud
- By doing Things like Turning off machines on weekend. Might be able to perform a no cost extension because of realized cost savings
  - Initial challenges were things like contract being too specific on things like size of compute

②



- A technical person could "technically" obligate the government by Turning on a VM
- ☆ - Is cloud a commodity or not?
  - It's consumption based
- Where does cost savings come from
  - What types of contracts (fixed price vs. cost + fee)
- ☆ - Should "cloud" be in the FAR?
- ☆ - How do you cost out things like data breach and include it in contracts
- Going into a cloud contract, you're going into (ideally) a long term relationship

③

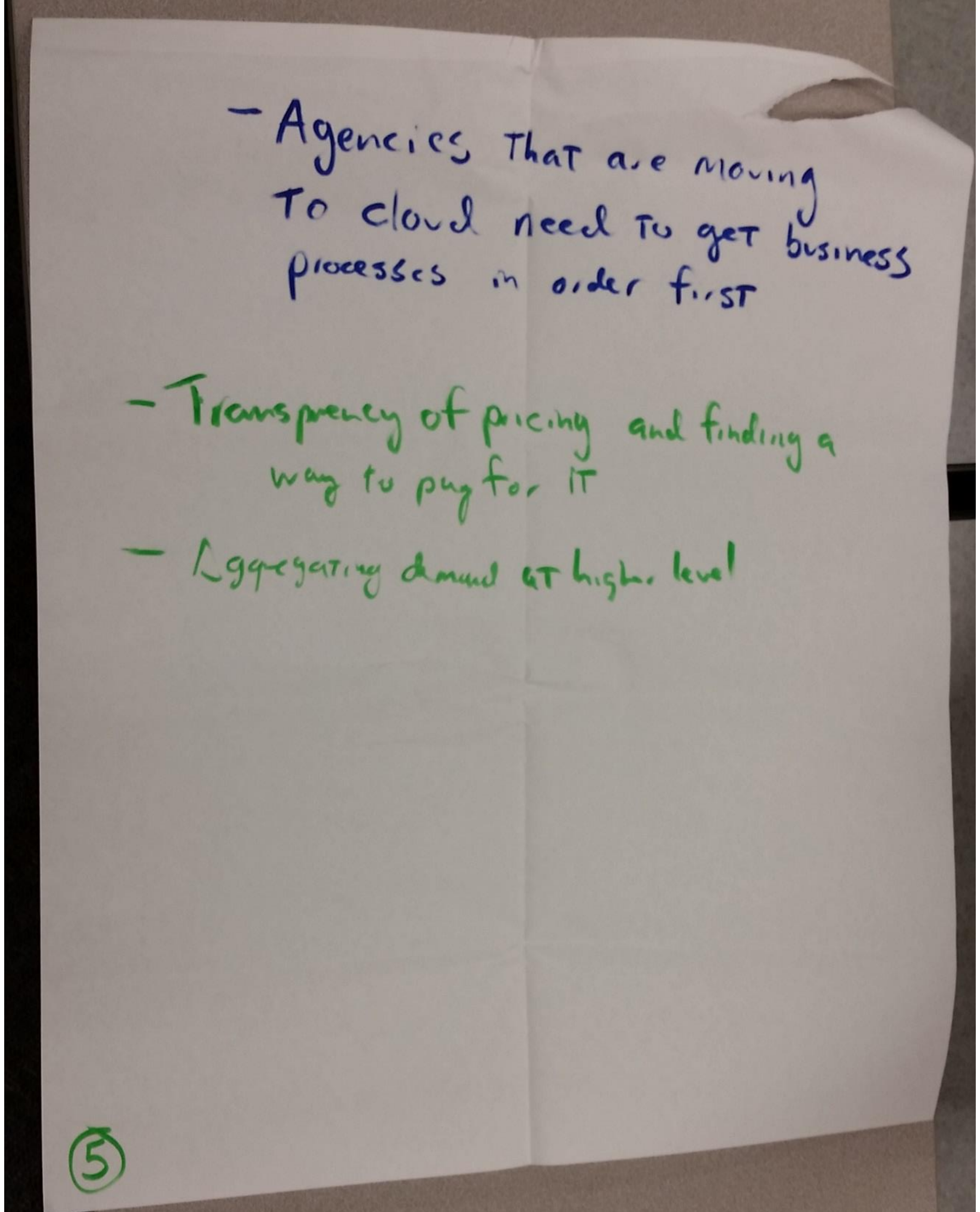


- ☆ - Problem w/ strategic sourcing is aggregating and having unified requirements
- Can we set up a revolving fund that can bridge fiscal years
- Support for standards is our biggest weapon for interop.

Todos:

- Get a revolving fund going
- Define standards for interop
- Changes to FAR to differentiate commodity cloud vs. non-commodity
- Create Standard language for contracting

④



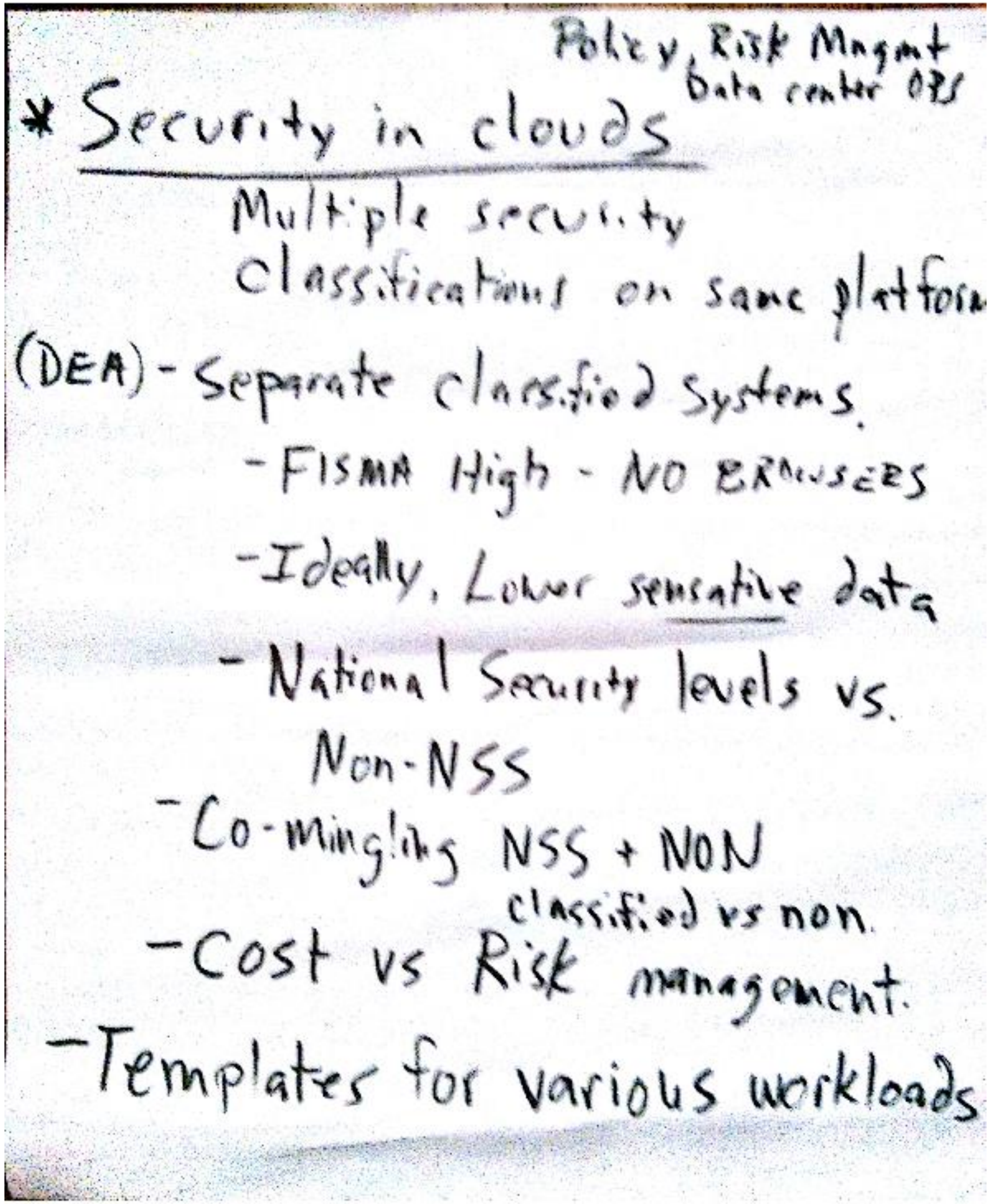
- Agencies That are moving To cloud need To get business processes in order first

- Transprency of pricing and finding a way to pay for IT

- Aggregating demand at higher level

5

Tiered Architectures



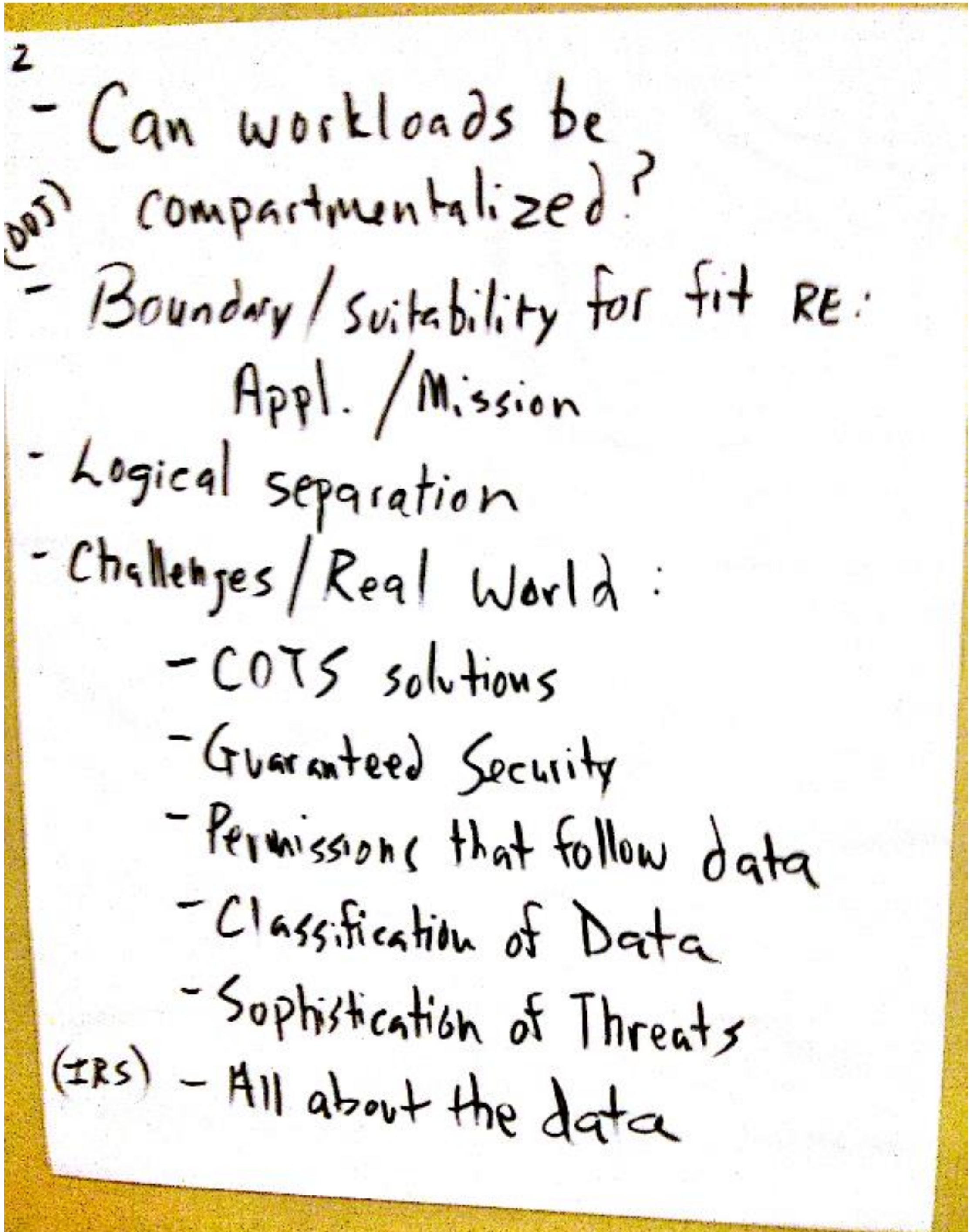
Policy, Risk Mngmt
Data center OPS

* Security in clouds

Multiple security
classifications on same platform

(DEA) - Separate classified systems.

- FISMA High - NO BROWSERS
- Ideally, Lower sencative data
- National Security levels vs.
Non-NSS
- Co-mingling NSS + NON
classified vs non.
- Cost vs Risk management.
- Templates for various workloads



2

- Can workloads be
(DOT) compartmentalized?
- Boundary / Suitability for fit RE:
Appl. / Mission
- Logical separation
- Challenges / Real World:
  - COTS solutions
  - Guaranteed Security
  - Permissions that follow data
  - Classification of Data
  - Sophistication of Threats

(IRS) - All about the data

3 Real World Constructs cont'd

(Va) * Cost vs Risk

- Identity + Access Control
- Encryption at Storage level
- PIV /CAC / credentials
- Middleware
- HIPAA
- Attestation
- Inter-Agency sharing
- SLA
- CAPEX vs OPEX [illegible]
- Data Loss
- Compromize

[illegible] - SEPARATION BTW/ CISO + CIO

4

~~Substitute cottage cheese for Rigotta.~~ ✓

- SSP - controls vs SLA
- Multiple levels on the same resources
- Geography
- Security personnel

*Is there a concern about WHERE cloud is located

- Bandwidth
- Latency.
- VDI Solutions

5

Where the Cloud is located (contd)

- Protection from end to end
- NOC, Backup, Support in different locations.
- Put everything in the contract.
- ITAR
- Supply Chain / Equipment Integrity
- Data encryption
- Key Management System / Key Esrow
- Performance is Key
- Noisy Neighbors
- Over-subscription
- Guaranteed IOPS
- TIC - Not cloud-friendly

6 Geography

- COOP
- Flood zone DR / Primary
- DR / COOP / Hot DR / Elasticity
- Using the Cloud for elastic requirements.
- Hybrid Solutions
- Load Balancing

*OPERATIONS CONCERNS

- Application upgrades / OS Changes / patches
- Change Management
- Control over Supply Chain.
- Partitioning, based on cust. requirements

7

Operations Concerns

- Backups
  - Where do they go
  - Visibility / Access
  - Log file Analytics.
  - Disk Drive release /reclamation
  - One version ?
  - CO-mingling of companion services
- Cyber Defense
  - Reporting
  - Additional Monitoring
  - Incident Reporting
- Break/Fix coordination
- Financial Stability of CSP
- Data Rights
- Security DATA / SOC

8

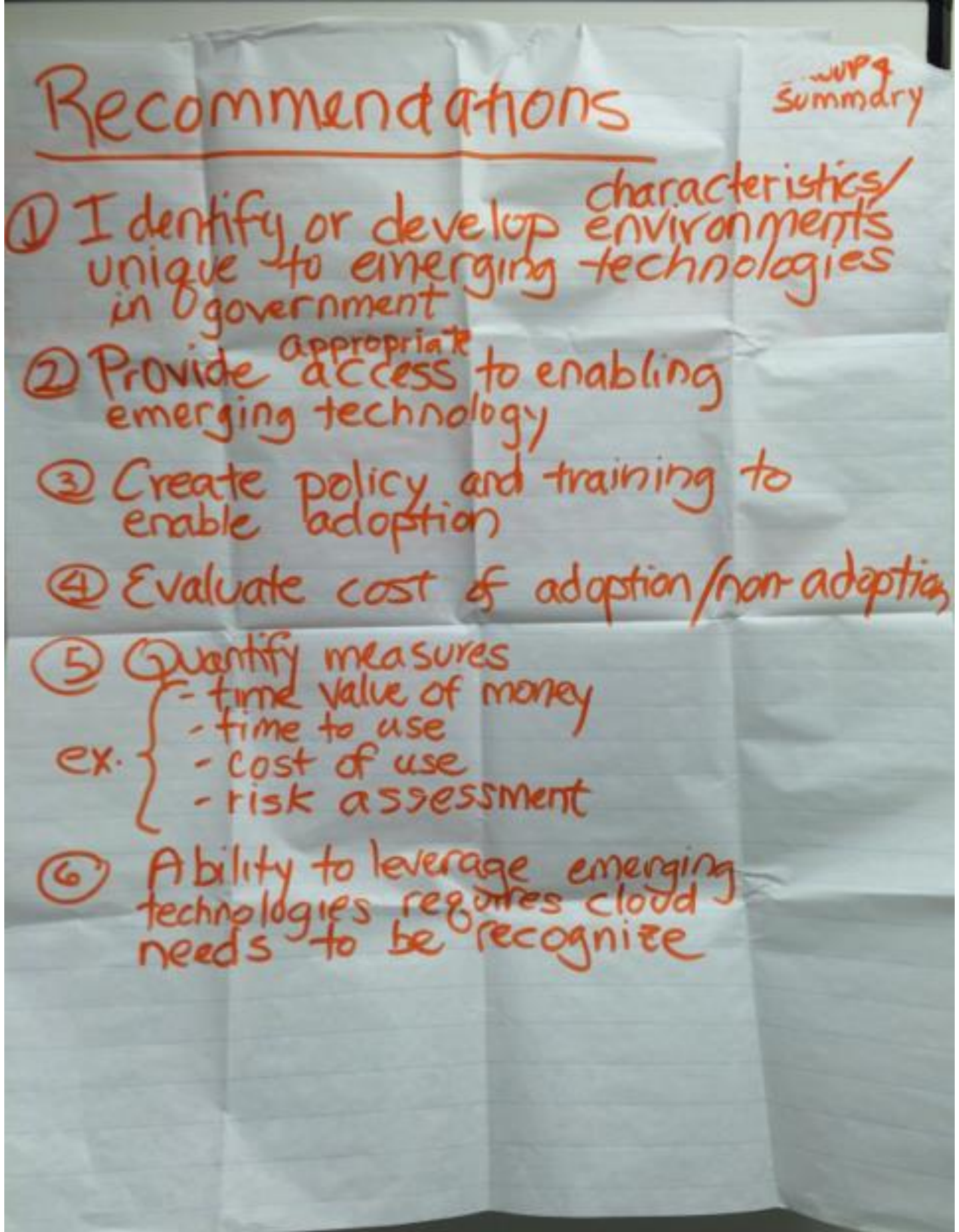
Recommendations

- Contract. Put it in the agreement.
  - Consistency
  - Templates
- Shared RFP Templates
- TIC - Fix TIC Problem
  Architected for Cloud ? S ?
- Data Rights / Data Ownership
  - In Contract.
- COOP / DR
  - CONUS + CLEARANCE
- VISIBILITY
  - How broad is the scope of things like vulnerabilities.
- Trusted Relationship
  CYBER Incident Reporting

9 Recommendations

- Change Management
- FedRAMP contract clauses being expanded. / Best Practice sharing
- Business + Technical requirements inside Contract.

The Roles of Cloud Computing in Emerging Technologies



Recommendations

Group 4 Summary

1. Identify or develop characteristics/ environments unique to emerging technologies in government
2. Provide appropriate access to enabling emerging technology
3. Create policy and training to enable adoption
4. Evaluate cost of adoption/non-adoption
5. Quantify measures
   ex.
   - time value of money
   - time to use
   - cost of use
   - risk assessment
6. Ability to leverage emerging technologies requires cloud needs to be recognize