Air Force MINSAV Industry Day Cloud Features

P. Len Orlando III

AF HwA Lead T&AM and MINSEC

AFRL/RYDT

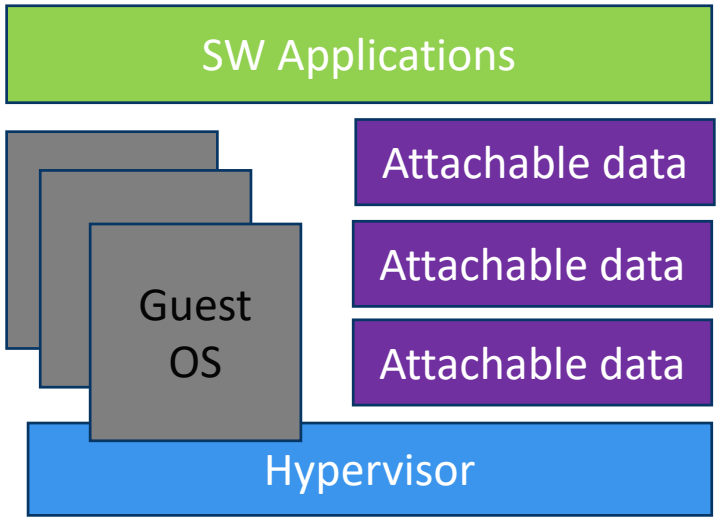
DISTRIBUTION A. Approved for public release: distribution unlimited.

Introduction

- Cloud 101
- Collaboration
- Traceability and Provenance
- Data Management
- Dynamics
- Storefronts
- Cloud Portability
- DoD Participation

DISTRIBUTION A. Approved for public release: distribution unlimited.

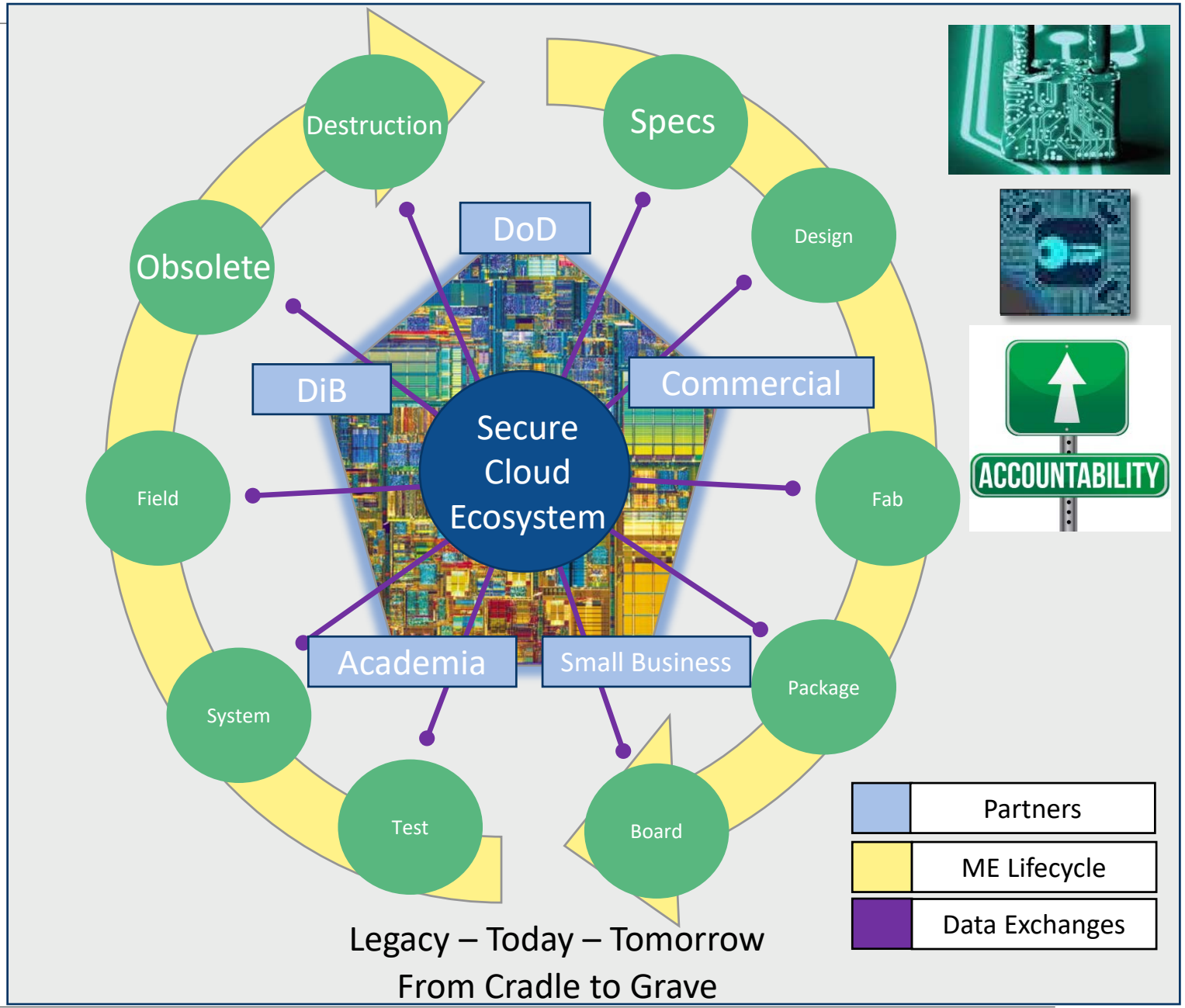
Cloud 101



Aggregated Hardware

High Availability

Physical Security – Common Compute – Storage
Database – Network – Configurable SW Security

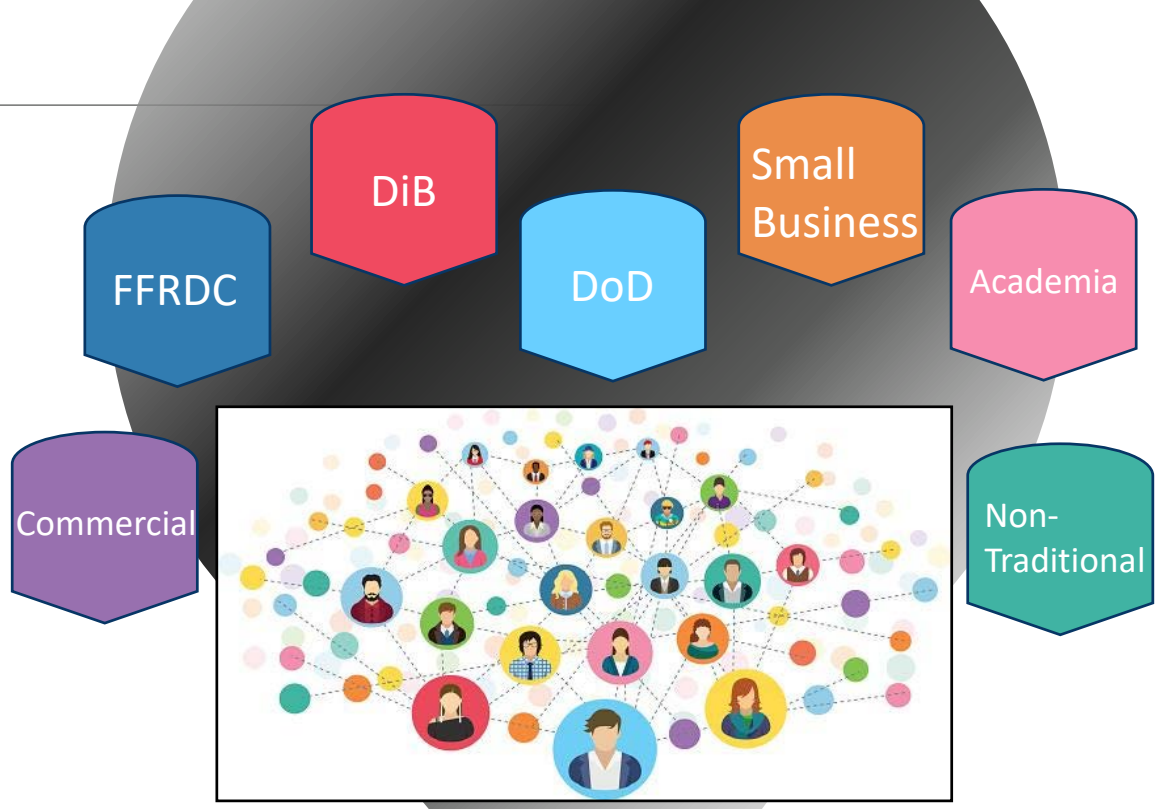


Legacy – Today – Tomorrow
From Cradle to Grave

DISTRIBUTION A. Approved for public release: distribution unlimited.

Collaboration

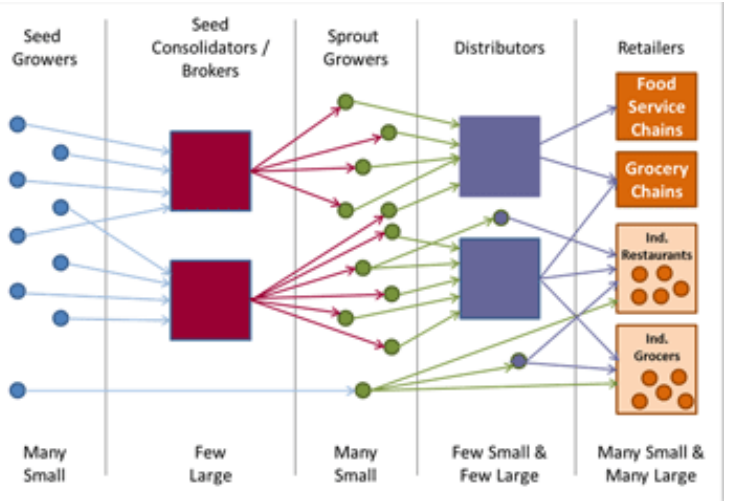
- Traditionally DoD communities are isolated silos of deep knowledge
  - Geographically and organizationally isolated
  - Beneficial when problems can be solved within a site
- Today, problems are challenging enough that multidisciplinary skills are necessary to provide solutions
- Technology pace is rapid and dynamic
- Cloud as an enabler:
  - Integrate geographically desperate communities to solve problems interactively
  - Leverage economies of scale utilizing reproducible cloud methods
  - Granularity of controlled access: user, project, community, organization, periods of time
  - Persistent information capture
  - Multi-org consistency
  - Secure infrastructure



DISTRIBUTION A. Approved for public release: distribution unlimited.

Traceability and Provenance

- The objective is to provide mechanisms to determine who created what, who did what and when was it done.



- How is traceability and provenance achieved?
  - Cloud Technology i.e AWS CloudTrail/CloudWatch
  - Blockchain (Capture every click, data sources, etc.)
  - Or is it a mix? Or new technology?

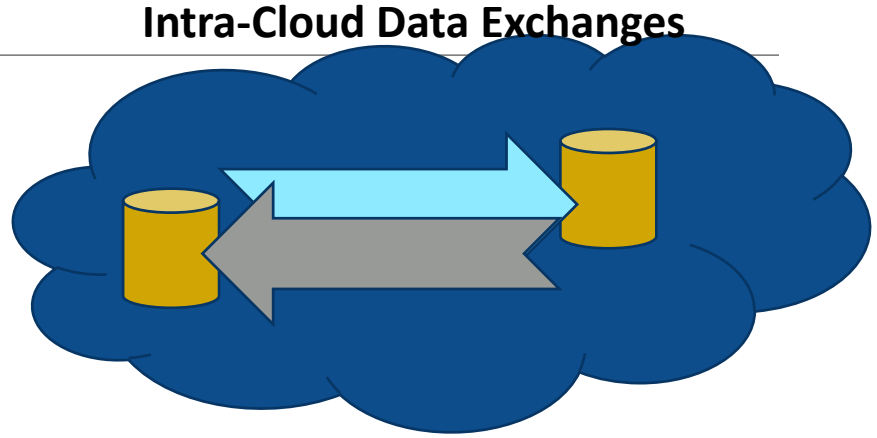
- How will you authenticate?
  - 2 factor authentication i.e google authenticate
  - Specific hardware requirements

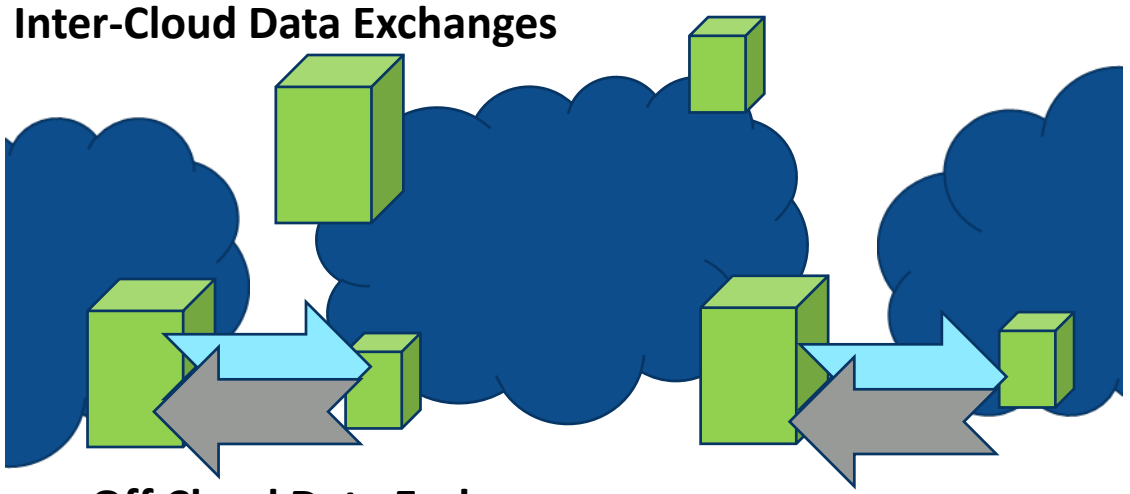
- What data is captured and granularity?

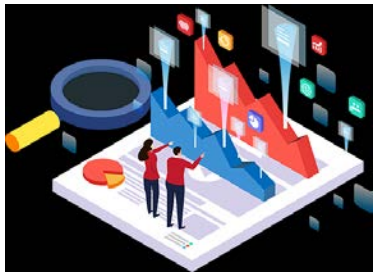
DISTRIBUTION A. Approved for public release: distribution unlimited.

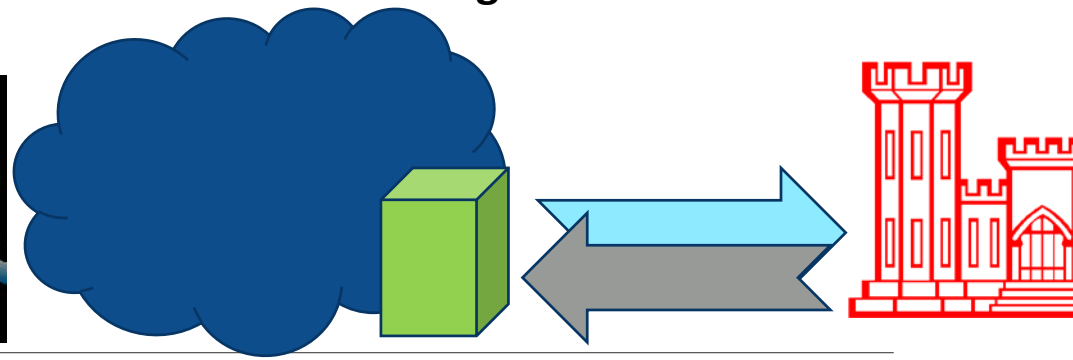
Data Management

- How is data managed and monitored while in-motion or at-rest?
  - Data Exchanges: commercial-defense-university
  - Data Generated: IP repository
  - Data Ingested: 3rd Party IP, Commercial IP and Software
  - Data Validation
  - Data Archived: Persistent long-term data storage (i.e. AWS Glacier)
  - Data Resurrection: Bring data back into the system for analysis
  - Data Protection: Encryption
  - Data Access: Levels of access User, Group, Org, etc.
  - U.S. citizen vs. greencard vs. non-U.S.





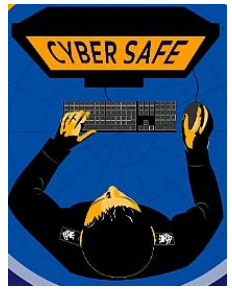




DISTRIBUTION A. Approved for public release: distribution unlimited.

Dynamics

- Cloud environment is constantly changing with new hardware, security threats, software, vulnerabilities, and users.
- Scalable system
- Automated deployment
- Cloud independence
- Transferrable
- Persistent Data availability for 10’s of years
- Uptime
  - System needs to be operational 24/7
  - Red-Blue Deployment
  - Scheduled outages when needed



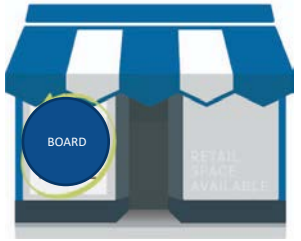
DISTRIBUTION A. Approved for public release: distribution unlimited.

Virtual Store Fronts

- Private cloud enclaves operated by 3rd party technology providers who determine what information is shared, who it is shared with, and when it is shared
- Leverage common distribution mechanisms within the cloud
- Centralized Terms and Conditions (T&C's) and Non-disclosure agreements (NDA's)
- Key enabled access
  - Different levels of access based on need
- Solutions can be made available to all
- Configuration control

Virtual Microelectronics Community

Data Repo

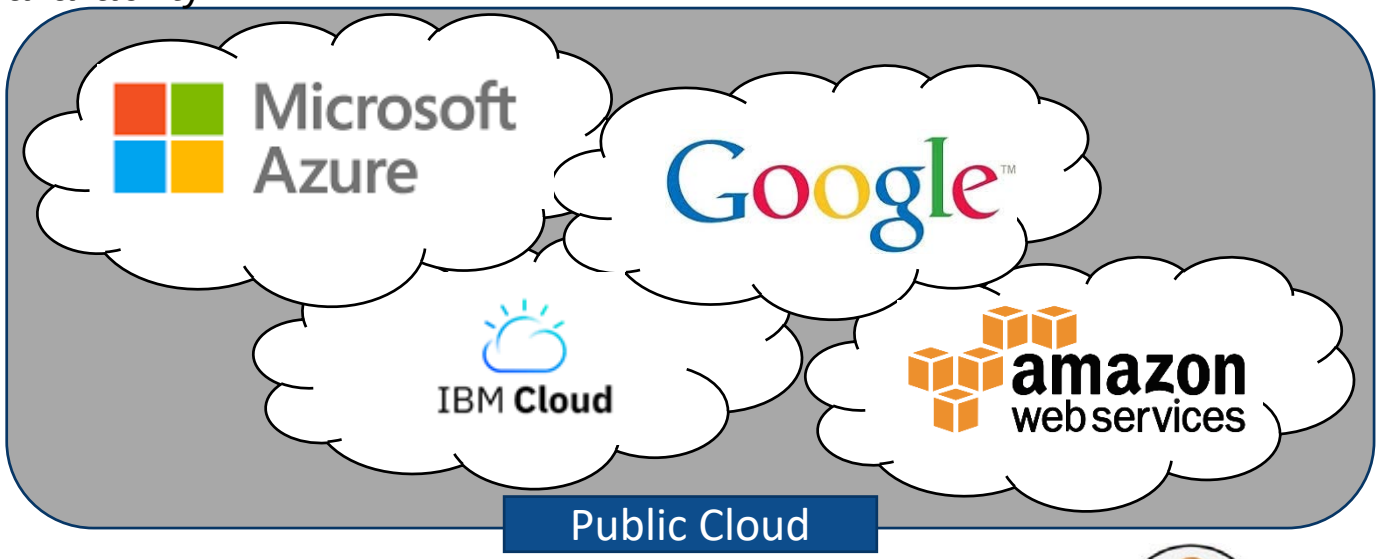


SW Repo

DISTRIBUTION A. Approved for public release: distribution unlimited.

Cloud Portability

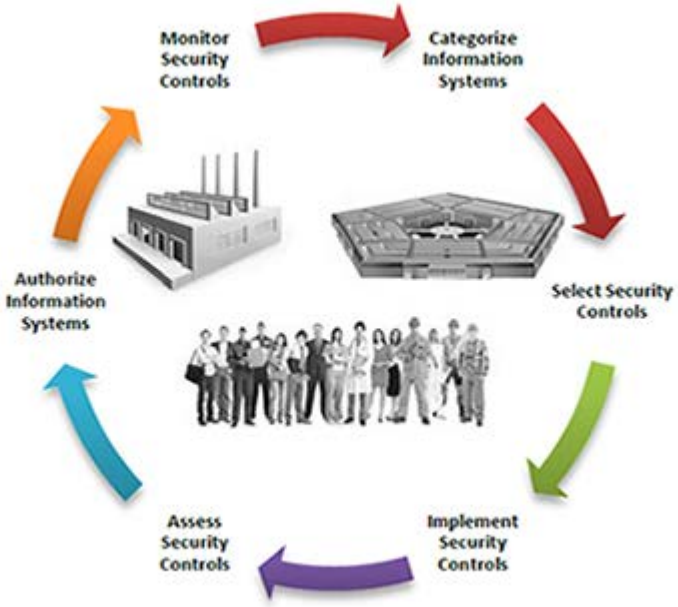
- Ability to encapsulate the entire cloud environment used to design a microelectronics system and transfer to another cloud or to a standalone environment
- Provides a path for cloud independence
- Orchestration of independent cloud environments to achieve best capability to achieve mission objectives
- Mechanism to achieve maximum uptime and availability



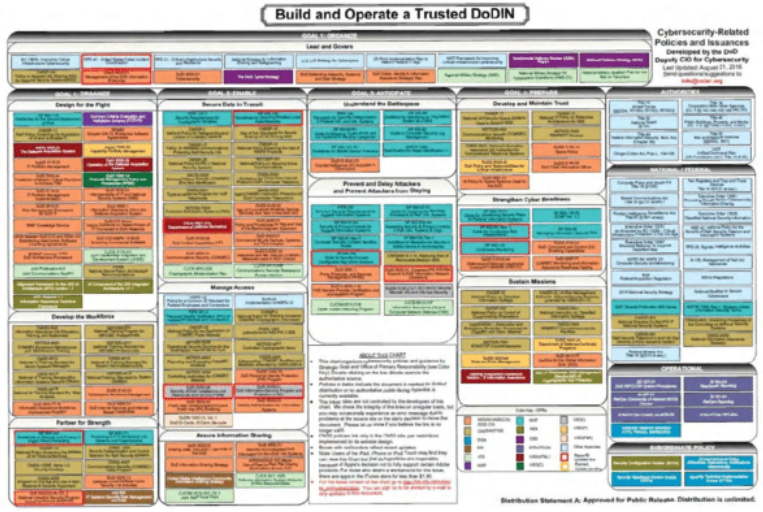
DISTRIBUTION A. Approved for public release: distribution unlimited.

DoD Participation

- DoD is an active participant within the cloud environment
- Pathway to accreditation
  - FEDRAMP approved
  - Authorization to operate
  - Authorization to use
  - Risk Management Framework
    - Requires additional processes and reports
- Operating System STIG compliance
- Routine Static and Dynamic Scans
- Penetration Testing



Item	Primary OV-5 Type	Feature	Tool	Description	Users	Totals Per Category D	O	T	ML	P	F	Avg	Action	Migrate Vital Features To
1	Infrastructure Mgmt.	Asset Mgmt	CM Extraordinaire	Does really cool stuff	Remote Office of 1	3	2	1	2	1	1	1.7	Turn Off	Centralized Solution
2	Security Monitoring and Mgmt.	SA/COP Network Status	Logs and Frogs	Log aggregation, script generation, Track IP Hopping	Data Center Sys. Admin	3	2	1	2	1	1	1.6	Keep	
3	System Access	Unnecessary Step	NeverTell	Keep my brother in-law employed	COOP users	2	2	2	5	1	5	1.9	Turn Off	Nowhere
4	Decision Support	Dashboard	MyBigBrain	Has always been a pet project	At a great TDY location	2	2	1	2	1	1	1.3	Turn Off	Cloud



DISTRIBUTION A. Approved for public release: distribution unlimited.

Summary

Utilize best cloud services possible to achieve microelectronics mission

- **Leverage commercial existing capability**
- **Enable collaboration within the ecosystem and partnerships external to the ecosystem**
- **Maintain high levels of assurance, traceability and provenance, and security**
- **Automated, dynamic, and extendable to cover the full lifecycle**

DISTRIBUTION A. Approved for public release: distribution unlimited.

Questions?

DISTRIBUTION A. Approved for public release: distribution unlimited.