

Creating Isolation in the Cloud

Nabil Schear
nabil@ll.mit.edu

Massachusetts Open Cloud Workshop

30 October 2018



Office of the Director of National Intelligence

I A R P A
BE THE FUTURE

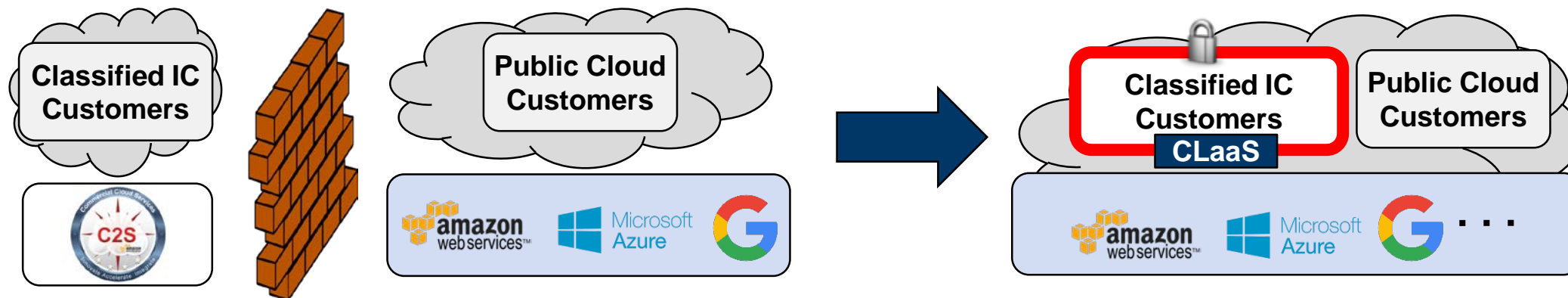
DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.
This material is based upon work supported under Air Force Contract No. FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the U.S. Air Force.
© 2018 Massachusetts Institute of Technology.

Delivered to the U.S. Government with Unlimited Rights, as defined in DFARS Part 252.227-7013 or 7014 (Feb 2014). Notwithstanding any copyright notice, U.S. Government rights in this work are defined by DFARS 252.227-7013 or DFARS 252.227-7014 as detailed above. Use of this work other than as specifically authorized by the U.S. Government may violate any copyrights that exist in this work.





Classified-as-a-Service (CLaaS) Concept



- **Current: classified workloads in physically isolated copies of commercial clouds**
 - **Sacrifice: scalability, flexibility, cost, latest technology advances**

- **Alternative: strongly *isolate* classified workloads in the public cloud**
 - **Need secure integrated hardware and software implemented by cloud providers and IC customers**

The IC needs flexible and substantial cloud resources to maintain US intelligence advantage



How do We Protect Classified Clouds Today?



Physical Isolation



NSA Certified Network Encryption

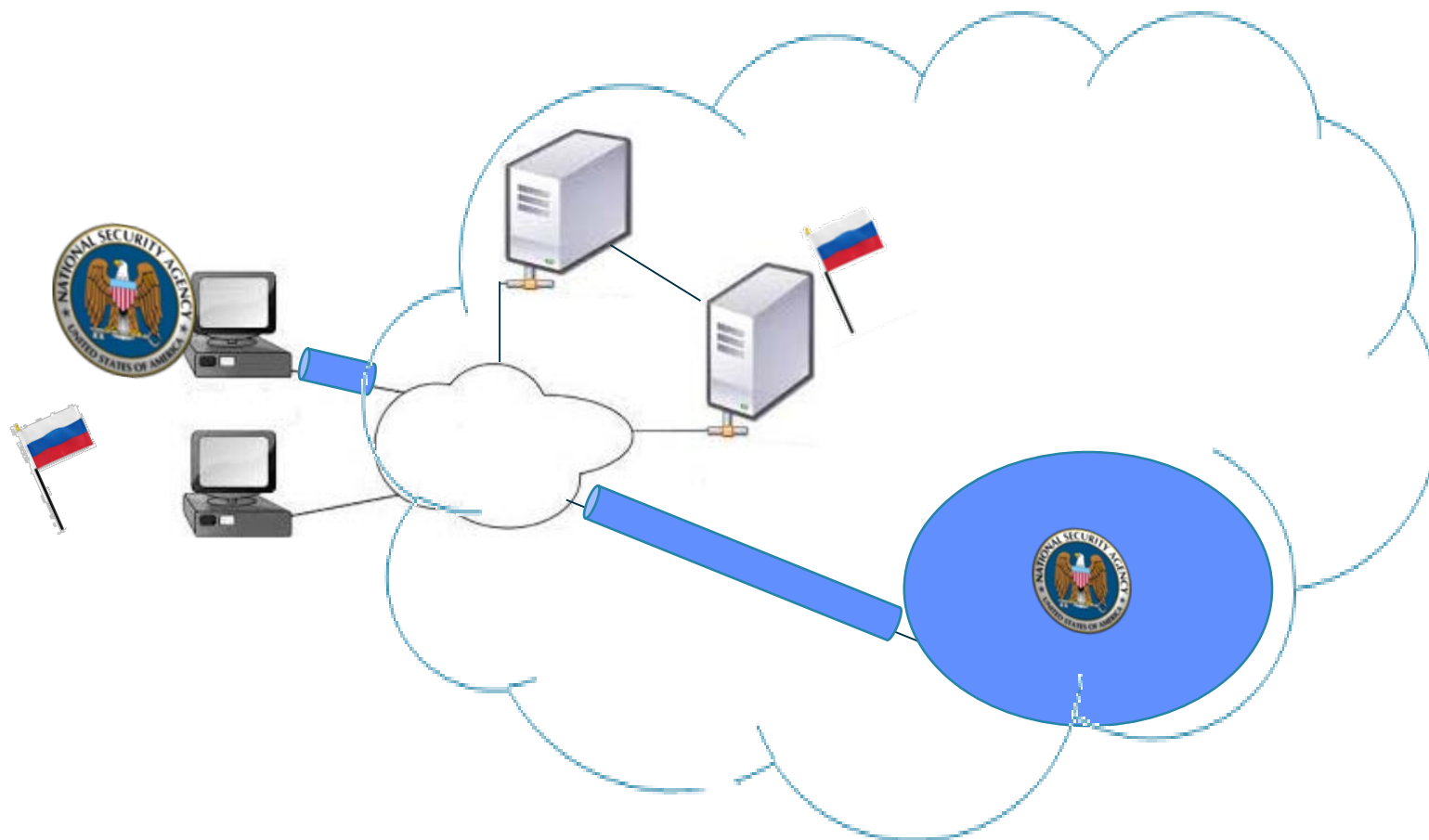


Policy and Certification



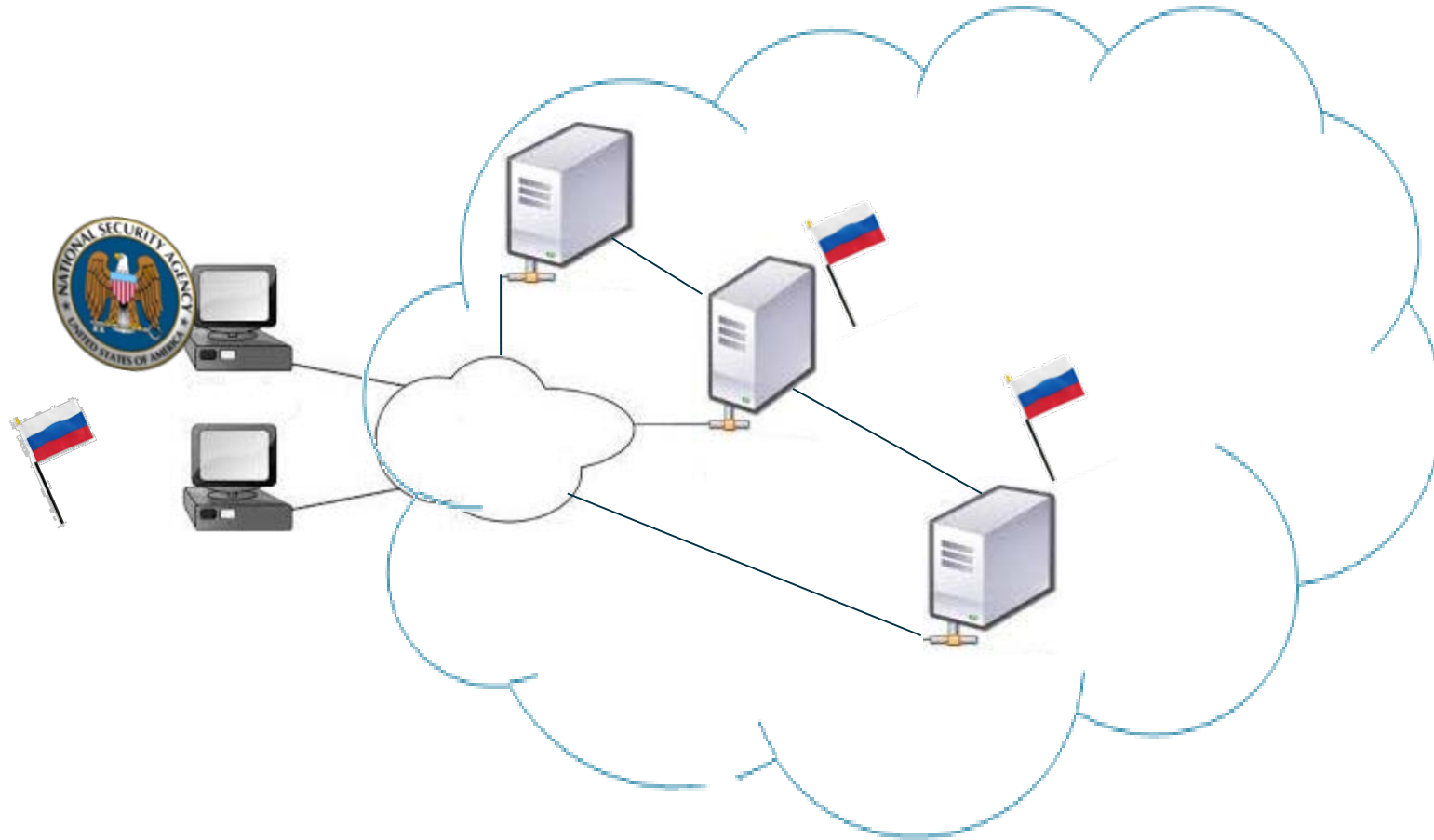


What We Want to Enable





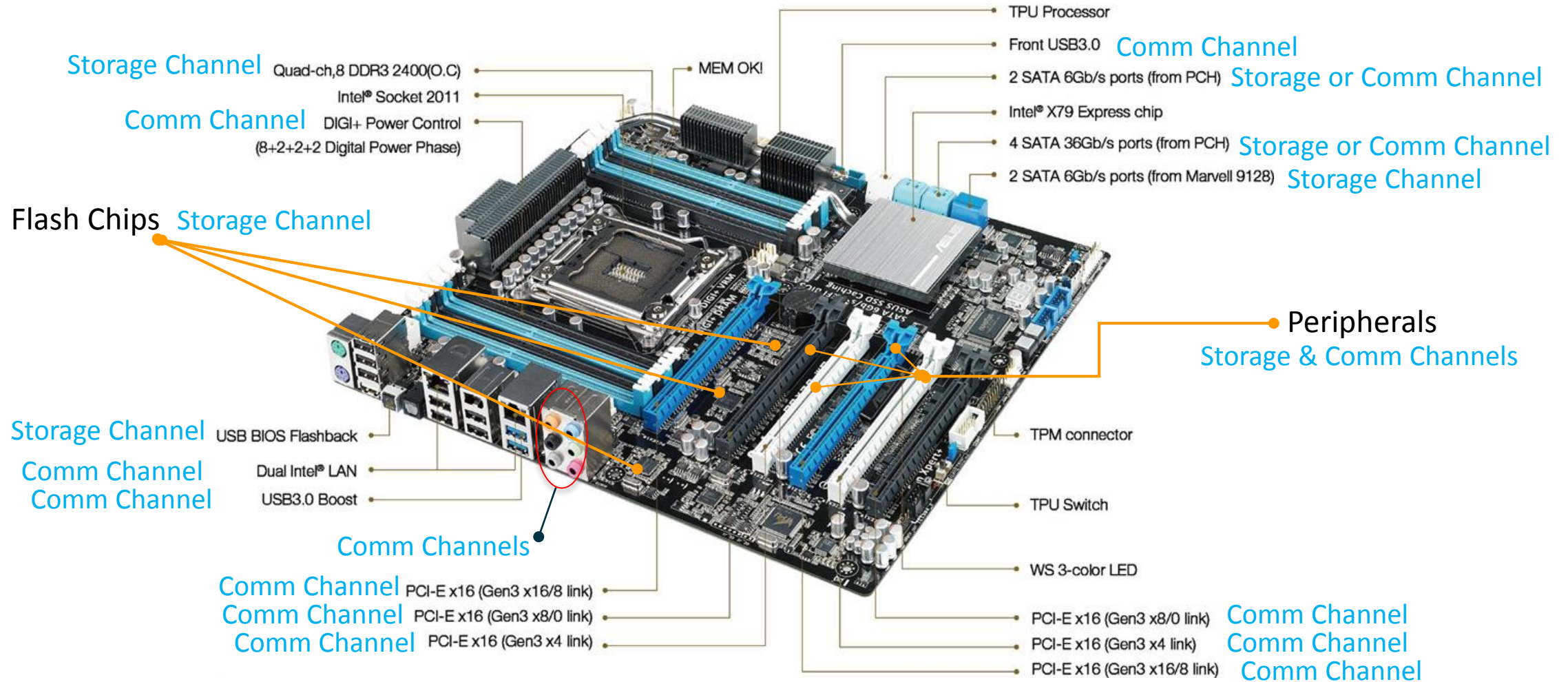
What We Want to Enable





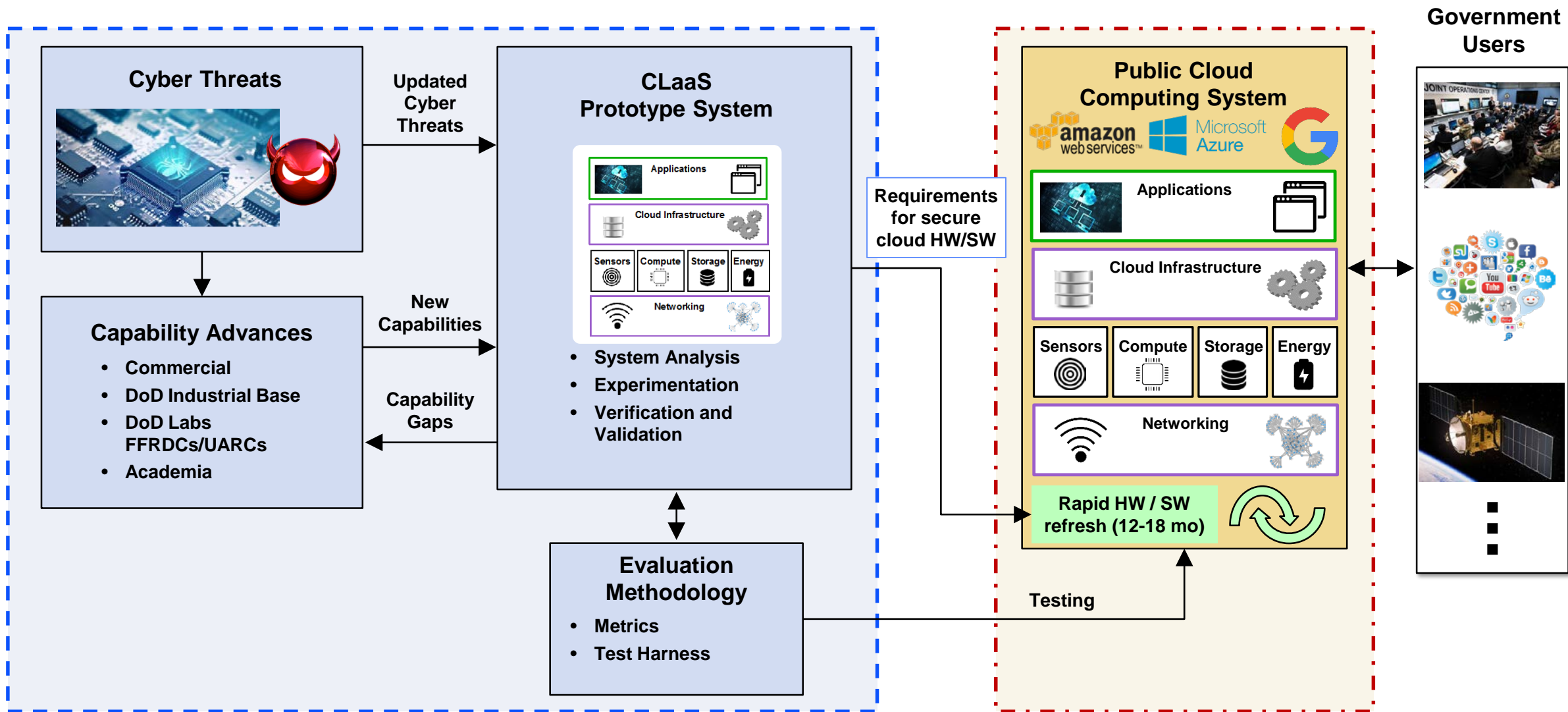
Why Isolation is So Hard

Server Motherboard





CLaaS Development and Transition Model





Summary



- **CLaaS has the potential to revolutionize secure cloud in the 2020s**
 - Commercial cloud providers interested
 - Technology to implement CLaaS is maturing: bare metal clouds are a reality
 - Assessment based on:
 - Isolation mechanism assurance
 - Bandwidth of covert storage and communication channels
- **Current status:**
 - Beginning initial study to flesh out initial design for prototype and assessment methodology
 - Building a community of interested partners including
 - Major cloud providers
 - Massachusetts Open Cloud partners

We are seeking your ideas for technical solutions to strong isolation in the cloud