Ground System Architectures Workshop

Session 11C

# The Trajectory of the GSAW Cloud Computing Working Group: 10 Years and Counting

*Ramesh Rangachar and Craig Lee*

*The Aerospace Corporation*

# The use of diagrams from NIST documents on Slides 7, 8, and 10 is permitted with the following notice:

This data/work was created by employees of the National Institute of Standards and Technology (NIST), an agency of the Federal Government. Pursuant to title 17 United States Code Section 105, works of NIST employees are not subject to copyright protection in the United States. This data/work may be subject to foreign copyright.

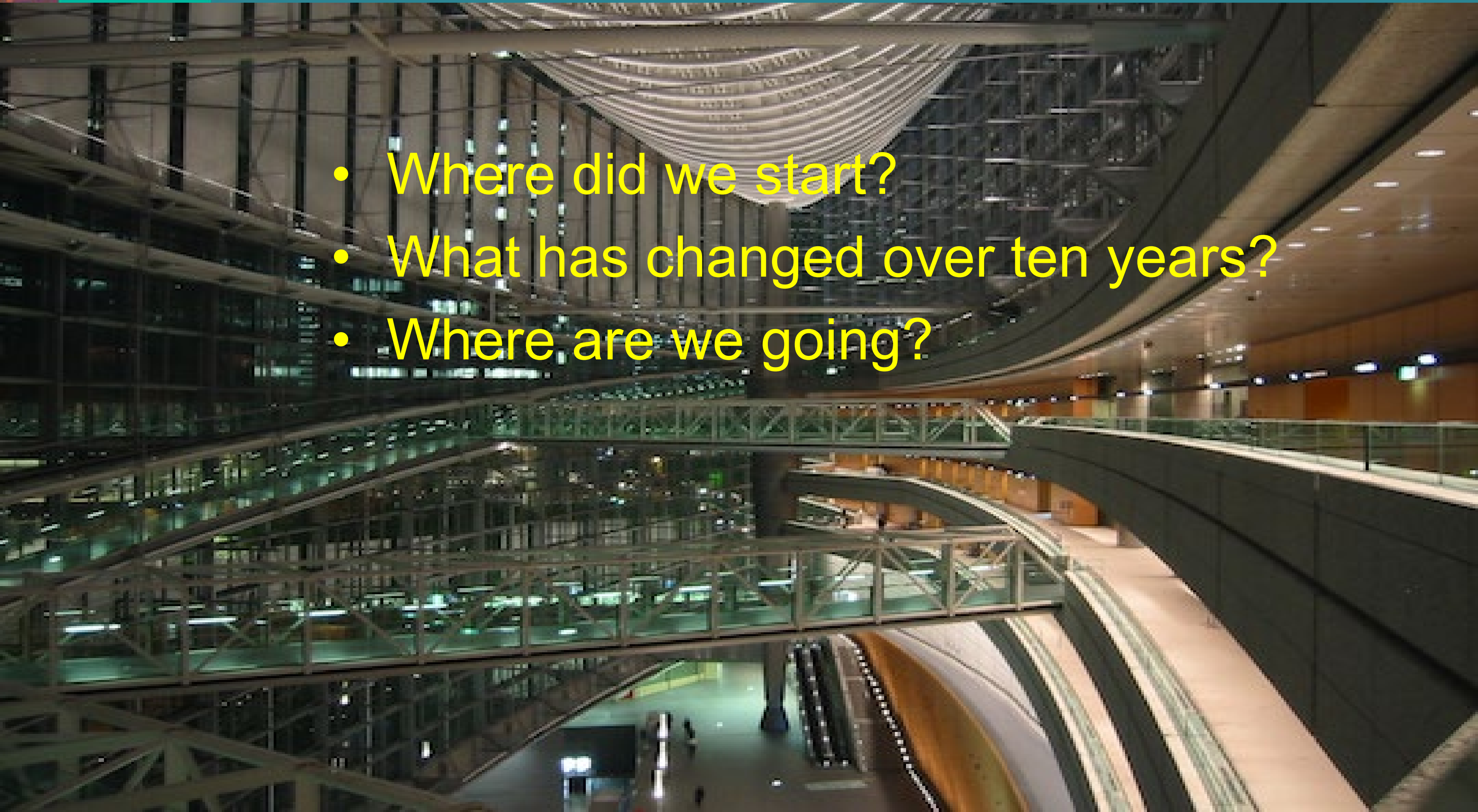
The data/work is provided by NIST as a public service and is expressly provided "AS IS." NIST MAKES NO WARRANTY OF ANY KIND, EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT AND DATA ACCURACY. NIST does not warrant or make any representations regarding the use of the data or the results thereof, including but not limited to the correctness, accuracy, reliability or usefulness of the data. NIST SHALL NOT BE LIABLE AND YOU HEREBY RELEASE NIST FROM LIABILITY FOR ANY INDIRECT, CONSEQUENTIAL, SPECIAL, OR INCIDENTAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, AND THE LIKE), WHETHER ARISING IN TORT, CONTRACT, OR OTHERWISE, ARISING FROM OR RELATING TO THE DATA (OR THE USE OF OR INABILITY TO USE THIS DATA), EVEN IF NIST HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

To the extent that NIST may hold copyright in countries other than the United States, you are hereby granted the non-exclusive irrevocable and unconditional right to print, publish, prepare derivative works and distribute the NIST data, in any medium, or authorize others to do so on your behalf, on a royalty-free basis throughout the world.

You may improve, modify, and create derivative works of the data or any portion of the data, and you may copy and distribute such modifications or works. Modified works should carry a notice stating that you changed the data and should note the date and nature of any such change. Please explicitly acknowledge the National Institute of Standards and Technology as the source of the data: Data citation recommendations are provided at https://www.nist.gov/open/license.

Permission to use this data is contingent upon your acceptance of the terms of this agreement and upon your providing appropriate acknowledgments of NIST's creation of the data/work.

# We’ve Been at It for Ten Years!



- Where did we start?
- What has changed over ten years?
- Where are we going?

# A Very Short History

2011 (I)
- Business Case and strategy needs to be refined
- Cloud standards are needed

2012 (II)
- Private Clouds
- Distributed Clouds
- Crossing Trust Boundaries -- Inter-Clouds

2013 (III)
- Security and Trust
- Technology is not the only problem

2014 (IV)
- SLAs for cloud
- Distinction between Public and Private cloud

2015 (V)
- Use cloud where it make sense: cost, reliability, performance
- Issues: data security, governance, org. barriers

2016 (VI)
- Containers and Microservices
- Config. Management: Chef, Puppet, Ansible
- Service Migration: re-host, re-factor, re-build

2017 (VII)
- Big Data, Containers, Microservice Architectures
- Cloud Adoption/Migration

2018 (VIII)
- Ground systems will no longer be monolithic
- They will be conglomerates of open source tools, containers, micro-services, etc.
- Mission and organizational boundaries will software-defined

2019 (IX)
- First time "Big Data" officially in the title
- Expands workshop scope to data-centricity
- Established processes and policies can be impediments

# So Where Are We Going?

***Can We Identify Some Destinations?***

# Trends

- Diversification up the stack
  - Everything is on-demand -- even *Ground System-as-a-Service*
    - CSPs provide back-haul!
    - CSPs are already operating global Content Distribution Networks (CDNs) with huge back-bone networks connecting their data centers
- Cloud Migration should involve a refactoring of the system arch
  - Migration Approaches: Lift-n-Shift, Green Field, Re-factoring
  - Service Identification
  - Enable more of a uService approach
- System design is much more than just the plumbing
  - *Security Architecture* must be a first-class citizen in the design process
- Cloud Design Patterns
  - Many are *data-access-oriented*
  - Many depend on some type of *API Gateway* or *Policy Enforcement Point*

# Data-Centric Architectures: The NIST Big Data Reference Architecture

- Data does not "live in" any one application
- Data is available to all applications

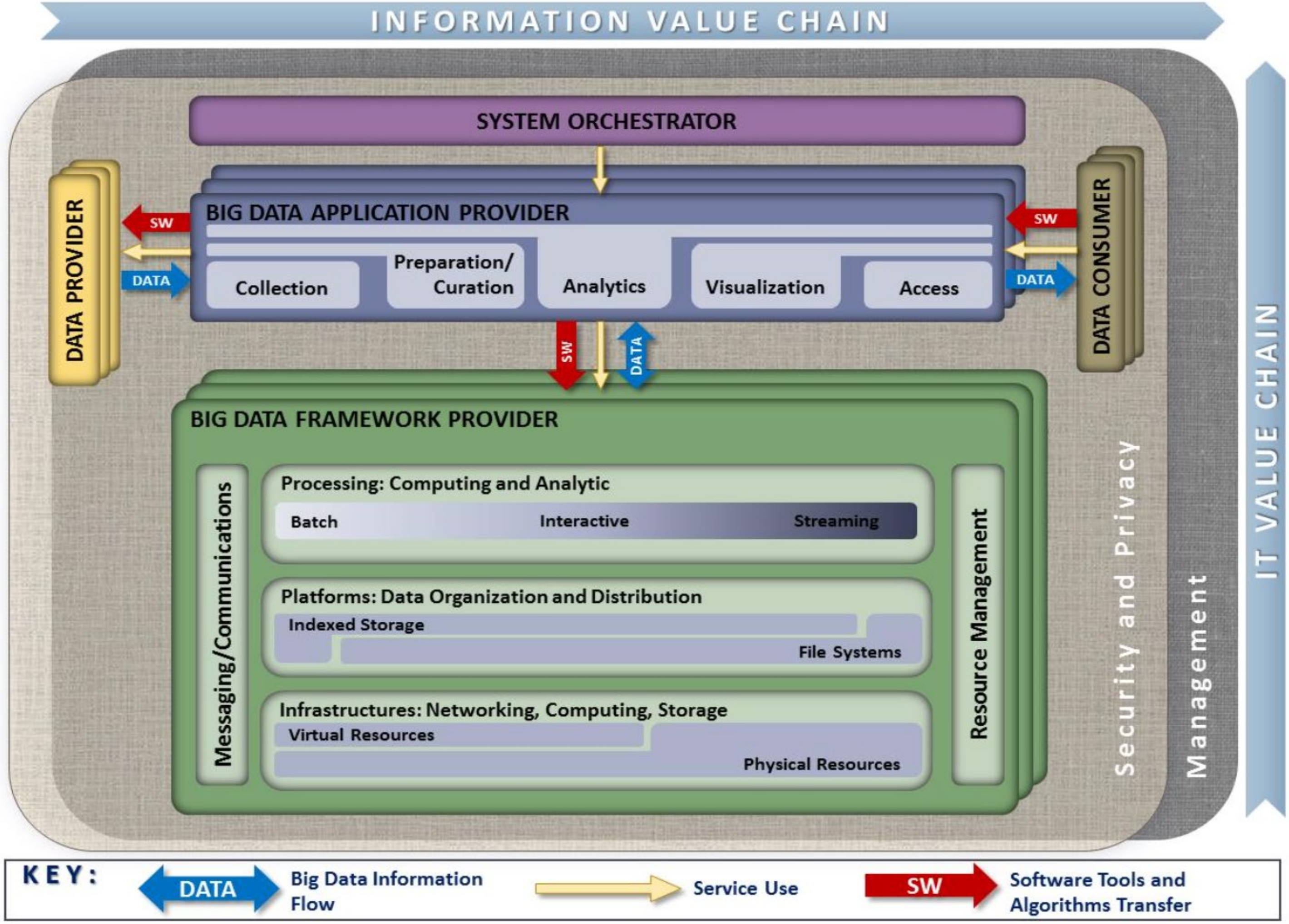


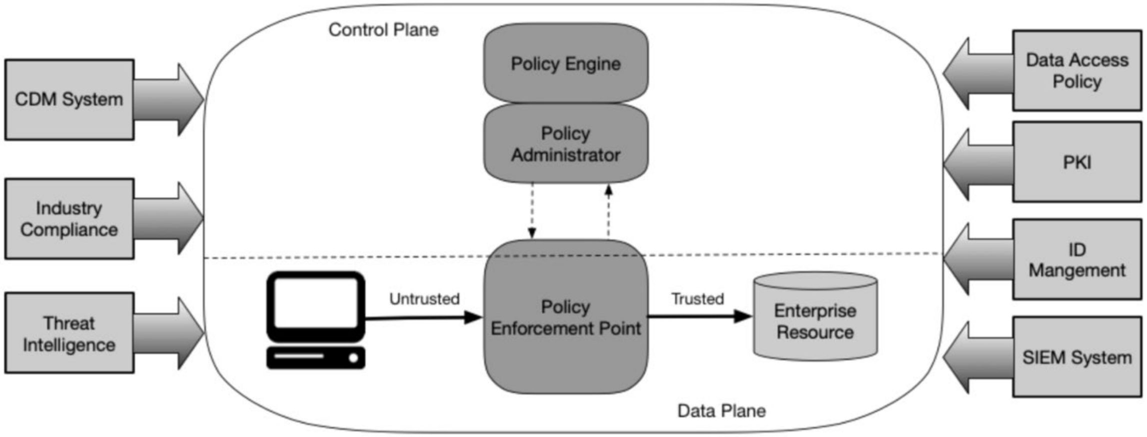
Figure 2 from *NIST Big Data Interoperability Framework*, NIST SP 1500, Version 2, Volume 6r1 (of nine volumes).

http://bigdataws.nist.gov

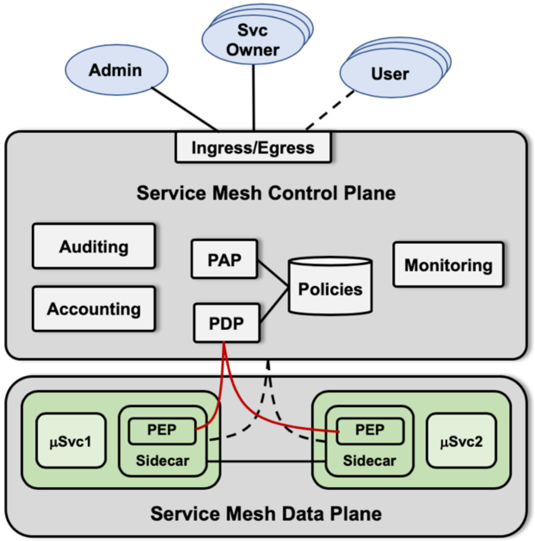
# Zero Trust Architectures and Microservice Mesh Architectures

- ZTAs based on minimizing *Trust Zones*
  - A Trust Zone is a zone of *implicit trust*

- uService Mesh Architecture is a promising ZTA approach
  - uServices are deployed in *side-cars* that include a PEP



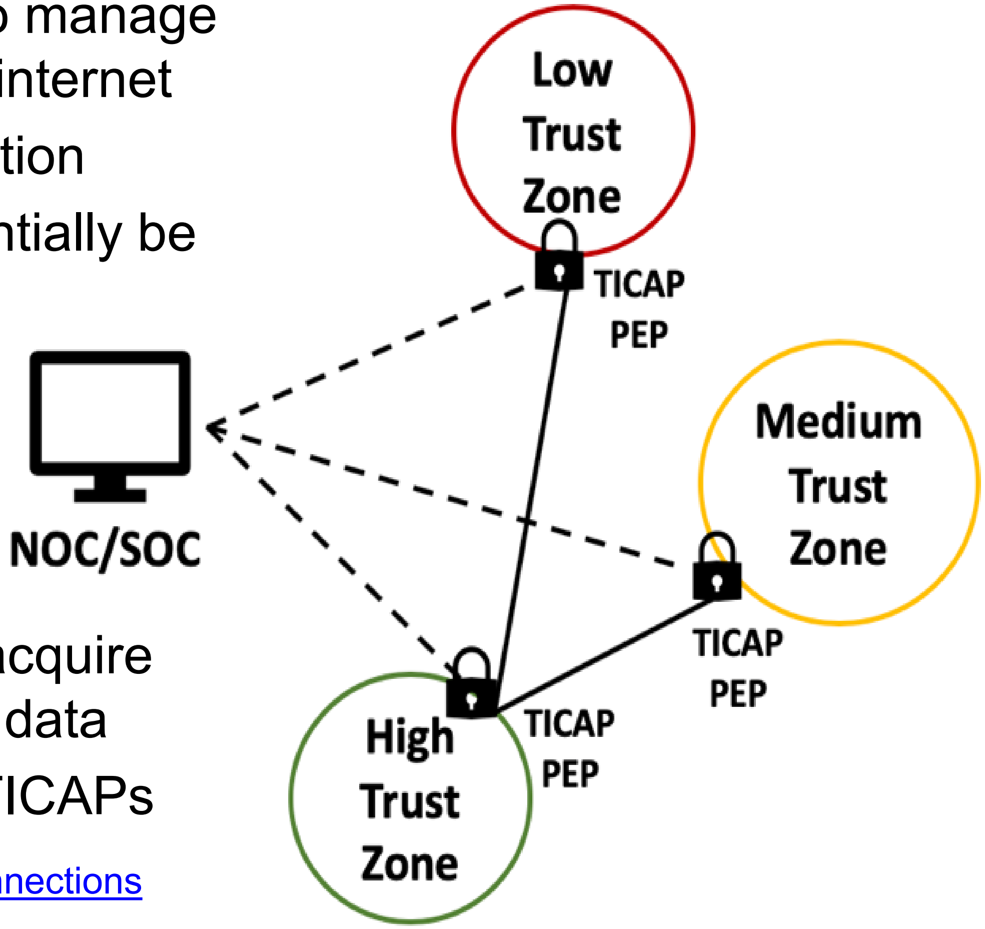
Rose, et al., *Zero Trust Architecture*, NIST SP 800-207, September 2019.



Chandramouli and Butcher, *Building Secure Microservice-Based Applications Using Service-Mesh Architecture*, Draft NIST SP 800-204A, January 2020.

# Trusted Internet Connections (TIC) TIC Access Points (TICAPs)

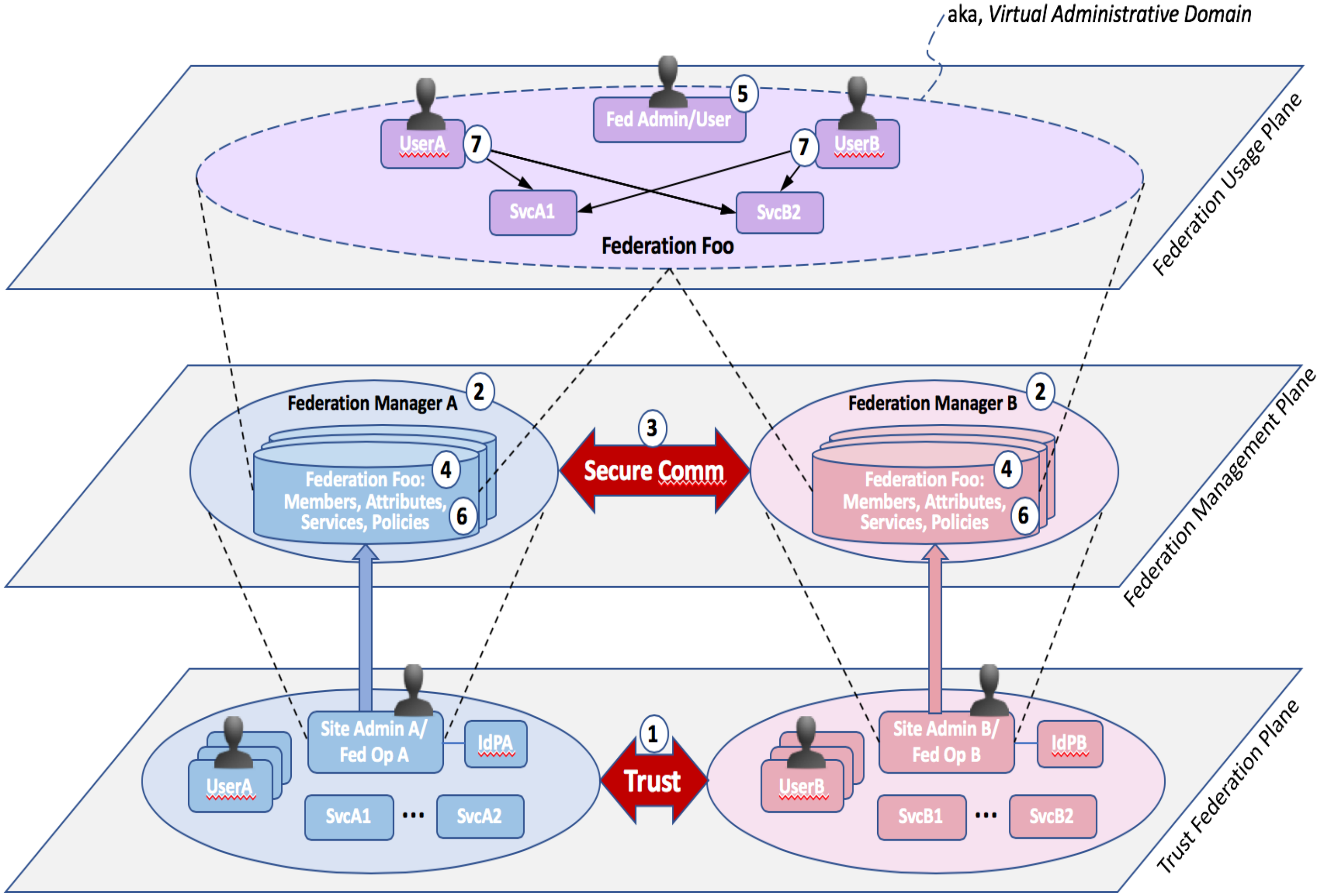
- TIC developed in pre-cloud era to manage how USG system connect to the internet
  - Based on hardware configuration
- TIC 3.0 being developed to essentially be *cloud-native*
  - TICAP *Policy Enforcement Points (PEPs)* will manage distributed *trust zones*
- Example: NOAA N-Wave
  - Global backbone network to acquire massive weather and climate data
  - Enters through five CONUS TICAPs



https://www.cisa.gov/trusted-internet-connections

# The NIST Cloud Federation Reference Architecture

- CFRA explicitly addresses managing *system boundaries*
- Central Concept: *Virtual Administrative Domains*
- Implementations can use *API Gateways*
- CFRA organizes the entire federation design space
- Identifies range of deployment and governance models



https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-332.pdf
Digital Object Identifier: https://doi.org/10.6028/NIST.SP.500-332

# Final Observations

As systems move to the cloud, all management and security boundaries will have to be *software-defined*

These boundaries will all be defined by how identity, credentials, roles, attributes, resource discovery and access policies are managed

These requirements are shared by many system design approaches

The organizational and economic issues will be more difficult than the technical issues

It's not a question of if -- but when and how