NRC CLOUD INFRASTRUCTURE

PUSHPA JAYAPAL AND STEVE SCHRADER

CLOUD STRATEGY

- The Agency's objectives are:
  - Improve security, cost effectiveness, efficiency, agility, and scalability in delivering IT services;
  - Align with the OMB's "Cloud Smart" policy and the Federal Cloud Computing Strategy;
  - Accomplish appropriate system and application migrations to cloud services as part of compliance with Federal DCOI mandates;
  - Establish consistent cloud solution planning and migration practices; and
  - Reduce risks to IT delivery, availability, and performance through a more distributed and consistent infrastructure and platform environment.
- To maximize cloud services benefits, the NRC will use the following strategies:
  - Leverage Software-as-a-Service (SaaS) first to support a low-code deployment approach and optimize functional requirements to take full advantages of SaaS benefits.
  - Leverage Platform-as-a-Service (PaaS) to drive technology standardization for modernized systems and applications that require customization.
  - Plan to acquire and support standardized PaaS platforms.
  - Increase application refactoring activities to rearchitect applications from monolithic and tightly integrated applications to loosely-coupled, cloud-based microservices focused on activities and workflows.
  - Adopt Infrastructure-as-a-Service (IaaS) only by exception.

MAJOR COMPONENTS

- Azure Commercial (IaaS and PaaS)
- AWS, NRC RES-Managed
- Other SaaS

AZURE INFRASTRUCTURE

- ExpressRoute connected stub network
  - No direct Internet Access—All access through the NRC TIC connection
  - 2-Gbps Connection through Equinix
  - Equinix will be the TIC 3.0 connection for NRC
  - Supports Cloud EDTE, Production, and DMZ zones
- Currently supporting several systems using the following PaaS (not exhaustive):
  - Azure Web Apps
  - Azure SQL Database
  - Azure Functions
  - Azure Bot and QnA Maker
  - Azure Search
  - Azure Cognitive Speech Service

CLOUD SECURITY

- When possible, all cloud systems use Private IP Space
  - In Azure, SaaS and PaaS Services use PrivateLink to provide for Private IP usage
  - In Azure and AWS IaaS, no public IP addresses are assigned to VMs
- Cloud Access Security Broker (CASB)
  - Provides policy enforcement regardless of what sort of device is attempting to access cloud services
- Azure Defender
  - Currently monitors Azure SaaS and PaaS Configurations
  - Can be configured to remediate identified issues
- "Standard" Network Security approaches, e.g. Splunk, Firewalls, IDS, AV

CURRENT AND FUTURE PROJECTS

- Application Migration Efforts – EIE, ILDC, NITA, Data Warehouse, ADAMS, TTC ColdFusion, RPS, ALM, Azure VDI
- New Capabilities – ActiveNav
- PaaS Implementations – Containers, Azure Security Center, Site Recovery, Mobile Apps, Logic Apps
- 3WFN Data Center Consolidation
- Evaluating and Scheduling all NRC FISMA Systems Cloud Migrations
  - Goal is to migrate all systems which can be migrated to the cloud by Dec 2026

THANK YOU

JAYAPAL, PUSHPA
PUSHPARANI.JAYAPAL@NRC.GOV

STEVE SCHRADER
STEVEN.SCHRADER@NRC.GOV