ENDURING VALUES. INSPIRED PERFORMANCE.®

ARC-P
FedRAMP HIGH Baseline

James Bowman
Government Cloud Solutions ISSM

June, 2016

Team Members

- John Keese, Director, CSRA Government Cloud Solutions
- Rachel Askew, Senior Program Manager, CSRA Government Cloud Solutions
- James Bowman, ISSM, CSRA Government Cloud Solutions

ARC-P Overview

- Federal Government Infrastructure as a Service (IaaS)
  - ARC-P Government Community Cloud (GCC)
  - Government Private Cloud (GPC)
  - ARC-P Secure Data Center (SDC)

- Focus on OPEN standards assures interoperability and prevents vendor/CSP lock in

ARC-P Features

- Entire ARC-P Security Authorization Boundary upgraded to the FedRAMP HBL and includes ARC-P GCC, GPC, and SDC offerings
- GCC Customer Virtual Network (CVN) separation at Layer 2

- ARC-P GPC is a true Private Cloud offering with dedicated hardware
  - Customized and sized to client requirements
  - Deployed in ARC-P data centers or on-premise for agency/mission as a managed service bringing our full security compliance

CSRA Cloud Benefits

- CSRA provides for direct CSP contractual relationships – no middle-man/resellers

- Security Consulting and Engineering support for applications/environments
  - Dedicated support personnel to each customer
  - Customized SSP templates for authorizing solutions/applications atop IaaS or PaaS provides accelerated ATO path
  - Cost effective managed services above the hypervisor. CSRA is both the CSP and SI – Contract from one source

ARC-P eAuth Level 4

- ARC-P accepts PIV/CAC authentication for customer access at the ARC-P Portal currently

- ARC-P underlying infrastructure VPN access for GCS internal Engineering and Security Team access currently utilizes RSA SecurID multifactor authentication w/ hardware tokens
  - eAuth Level 4 utilizing PIV is in testing in the ARC-P development environment
    - Scheduled production implementation by August 19, 2016
    - Scheduled FedRAMP accredited 3PAO verification by September 19, 2016

Thank you