

# Microsoft Azure Government

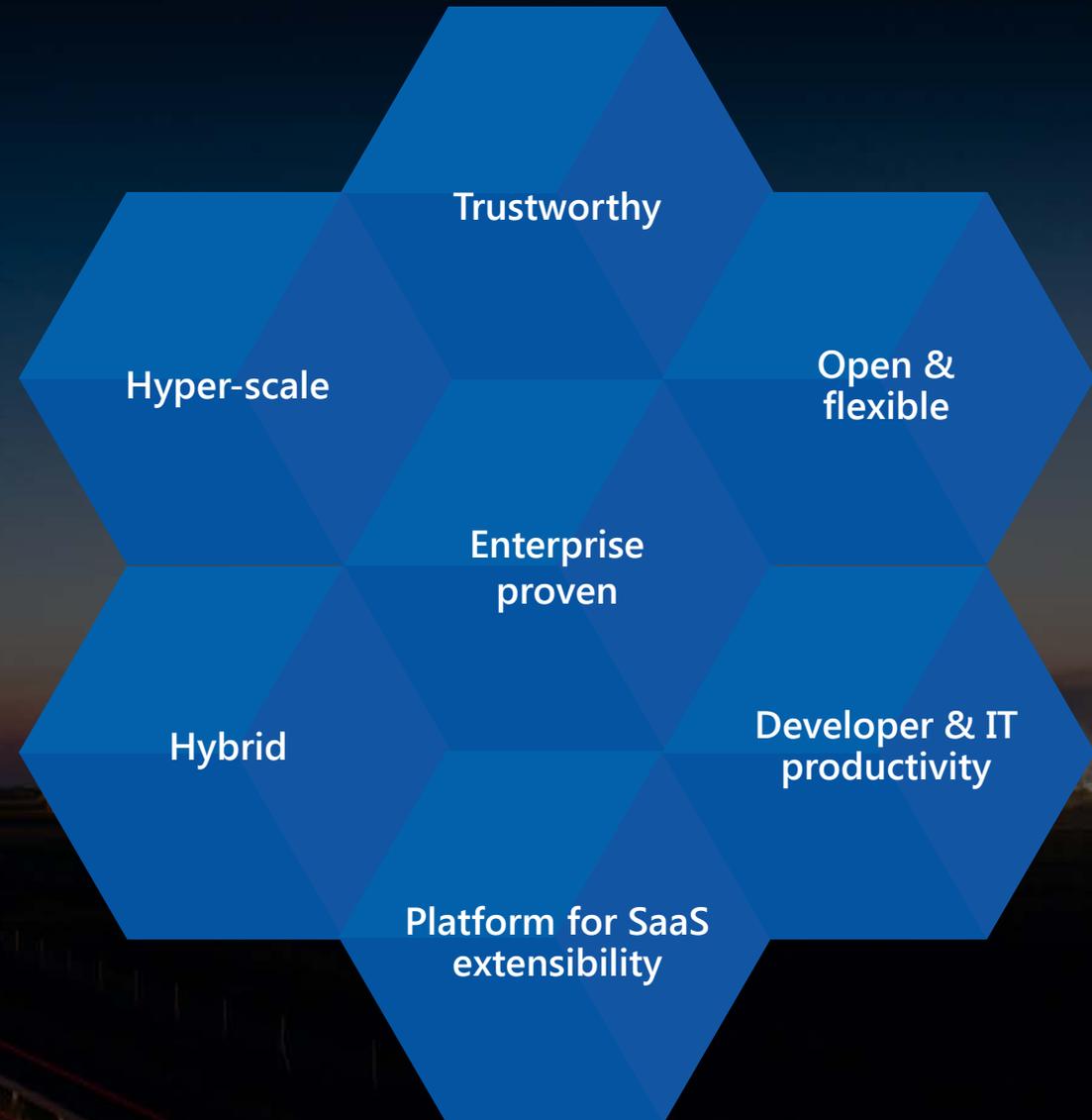
June 29, 2016

Presented by:

Matt Rathbun, Cloud Security Director

Cloud Health & Security Engineering

[matrath@microsoft.com](mailto:matrath@microsoft.com), [CHSE@Microsoft.com](mailto:CHSE@Microsoft.com)



# Azure Team Members

**Rathbun, Matt** – Cloud Security Director

**Adams, Susie** – CTO

**Soh, Adam** – Program Manager

**Chiou, Roger** – Program Manager

**Johnson, Nathan** – Program Manager

**Oppie, Tyler** – Program Manager



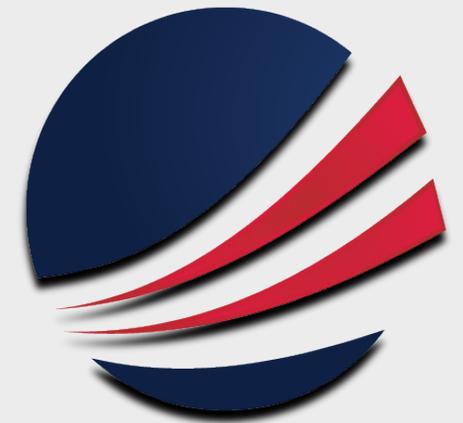
# Azure Government

**Dedicated Government Cloud:** The Azure Government cloud is dedicated to our United States based government customers.

**Restricted Customer Base:** Azure Government is restricted to Federal, State, Local, and Tribal government entities. ISVs are allowed when building first party solutions for the government. Limited commercial entities are allowed when they manage government regulated data such as: ITAR.

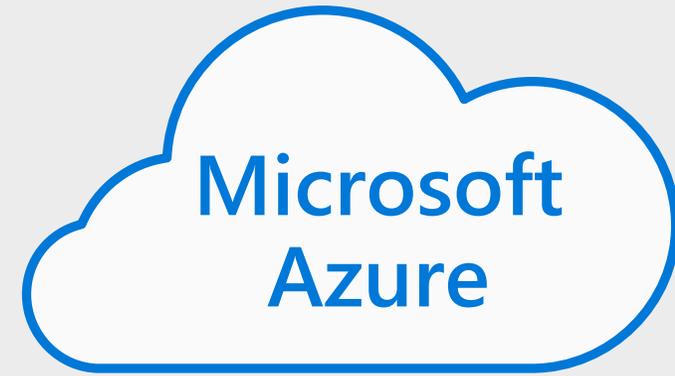
**Elevated Security Measures:** Azure Government has been architected to meet the highest available security bars among FedRAMP High, DISA L4, and DISA L5.

**IaaS/PaaS:** Azure Government provides both Infrastructure and Platform as a service



- Azure Government currently consists of two, geographically separated regions, US East and US West. All data within Azure Government resides solely within the United States.
- The trial subscription sign-up process for Azure Government determines the eligibility of customers to use the Government environment.
- All personnel managing Azure Government are United States citizens and have been screened to additional levels that go beyond our public screening process in order to comply with DISA and CJIS regulations.

# Security Benefits of the Cloud



**High Availability:** Geo-redundant datacenters, hybrid deployments, availability zones, and high availability configurations.

**Advanced Monitoring:** Application layer heuristic monitoring and big data analysis.

**Limited Human Interaction:** Administration is managed via approved pieces of code called workflows.

**Just In Time Access:** 'Two-key' solution for access to sensitive functions, requiring interaction and approval by multiple administrators.

**Federated Authentication & Cloud MFA:** HSPD-12 support, customer isolation.

**Platform as a Service:** Microsoft can handle patching and maintenance of your operating system on your behalf.

- Azure Government was designed with redundancy and availability in mind.
- Microsoft has reduced human interaction for repeatable tasks, freeing people to focus on areas where they add the most value.
- Just In Time Access addresses the number one threat to a system – malicious insiders.
- Advanced customer isolation capabilities built for a multi-tenant platform.
- Moving monitoring up the stack to application specific notifications and away from divining out of network traffic and protocols analysis.

# Why FedRAMP High

**Mission Critical Data:** Mission critical systems for many Federal agencies contain High impact data. This is especially true for security focused agencies where the need to protect human life elevates many systems to the High bar.

**One Platform Solution:** Azure Government is designed to handle all unclassified data, allowing agencies to utilize our platform for all unclassified data and to use software defined networking to safely communicate among their applications.

**Advantages of Hyper-scale:** The requirements of managing a hyper-scale, multi-tenant cloud already aligned Azure Government with the needs of FedRAMP High.



- High impact systems process information that if disclosed, modified, or denied access could have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
- These new enhancements generally increase the level of rigor, tighten timeframes, or increase scope of control applicability.

# E-Auth Level 4



**In Person Identity Proofing:** Microsoft initially distributed FIPS 140-2 validated smartcards, to support multifactor authentication for Microsoft administrators, to remote administrators via registered mail and using virtual in-person proofing to validate the identity of the recipient.

Microsoft is reissuing the certificates for these cards using an in person identity proofing process consistent with E-Auth Level 4 requirements. All Microsoft administrative personnel are scheduled to have been in-person proofed, with credentials reissued where necessary, by **July 19, 2016**.

Microsoft will have these implementations tested and verified by a 3PAO by **August 19, 2016**.

- Microsoft issued smartcards meet FIPS 140-2 requirements.
- Remote cards were distributed in a blocked state, and could only be unblocked after the recipient proved their identity, and possession of the credential.
- Personnel local to Microsoft Headquarters were issued cards by checking Government Issued, Photo ID, and the employee's Microsoft Badge. Microsoft badges are themselves issued consistent with I-9 requirements, checking two forms of ID at that time as well.
- A trained RA will fly to all remote administrators – such as administrators in datacenters – to perform the in-person identity proofing.

