Department of Defense
Joint Enterprise Defense Infrastructure (JEDI) Cloud Program

Cyber Security Plan

Cloud Computing Program Office

Version: 1.0
Date: 11 April 2018

DRAFT

Submitted By:

____

Program Manager
Cloud Computing Program Office

Concurrence By:

____

Commander, United States Cyber Command
and Director of the National Security Agency
Department of Defense

Approval:

____

Chief Information Officer
Department of Defense

DRAFT JEDI Cyber Security Plan

Updated 10 April 2018

0 Purpose

Security threats are the primary source of risk for any cloud solution. The Joint Enterprise Defense Infrastructure (JEDI) cloud initiative meets this challenge through robustness against known threats and an antifragile posture against future ones. The volatility of technology is not a weakness; it is an opportunity for growth. To that end, this document sets an onerous bar for outcomes but refrains from specificity in implementation. JEDI taps into the rapid adaptation and innovation of the commercial sector to relentlessly improve Department of Defense's services and security.

1 Compliance

1.0 The Contractor is responsible for meeting the requirements specified.

1.1 The Contractor is responsible for following the DoD Cloud Computing Security Requirement Guidelines, with the following exceptions:

1.1.0 Unclassified infrastructure must be logically separated with cryptographic certainty, but need not be physically separated, from other Contractor infrastructure.

1.1.1 Classified infrastructure must be logically separated with cryptographic certainty from other classified infrastructure. Classified infrastructure does not need to be physically separated from other classified infrastructure.

1.1.2 Classified infrastructure must be physically separated from unclassified infrastructure.

1.1.3 Positions without classified infrastructure access may be filled by non-US persons.

1.1.4 Infrastructure is part of the greater Department Of Defense Information Network (DODIN).

1.2 The Contractor must follow the National Industrial Security Program [D.0].

1.3 The internal operators, internal auditors, and external auditors verify compliance.

1.4 The contract defines timelines and metrics, as well as consequences for falling short of them.

1.5 Compliance evaluation takes only recorded communication into consideration.

1.6 In the event of a conflict, the requirements in this document supersede any referenced policy.

2 Operation

2.0 The Contractor, internal auditors, and external auditors report directly to the CIO. The internal operators and CIO do not report to each other. This is to encourage unbiased evaluation.

2.1 The CIO empowers internal operators to conduct missions and testing using infrastructure.

2.2 The CIO may exempt any requirements on a case-by-case basis.

3 Modernization

3.0 Capabilities used to meet requirements evolve at or beyond the speed of commercial offerings.

4 Requirements

4.0 Geographic redundancy enables applications to quickly recover from disaster.

4.0.0 Data centers sufficiently dispersed within US customs territory [D.1] such that applications can support the same overall load in the event of one or more natural or human-made disasters.

4.0.1 High availability unclassified and classified infrastructure in three or more data centers.

4.0.2 Tools that enable applications to harness geographic redundancy and support failover.

4.0.3 Network availability through redundant, globally distributed points of presence controlled by the Contractor and available on all continents (except Antarctica).

4.1 Physical access to infrastructure without authorization is considered logical root access.

4.1.0 Handle classified and unclassified server destruction pursuant to DoD 5220.22-M [D.2].

4.1.1 Classified infrastructure is physically isolated from all other Contractor infrastructure.

4.1.2 Unclassified infrastructure is mixed with public Contractor infrastructure.

4.1.3 Access restriction policies apply to infrastructure pursuant to the DD Form 254 [D.0].

4.1.4 Non-network infrastructure must be in US customs territory or military installations [D.1].

4.1.5 No individual may have both physical and logical access.

4.2 Logical administration and separation enable resource pooling, a key cloud advantage.

4.2.0 Logical separation with cryptographic certainty of isolation pursuant to CNSSP 15 [D.3].

4.2.1 Data at rest and in transit encrypted pursuant to CNSSP 15 [D.3].

4.2.2 Management of encryption keys supported by either the government or Contractor.

4.2.3 Authentication requires MFA such as DoD PKI [D.4].

4.2.4 Authentication to classified infrastructure requires DoD PKI [D.4].

4.2.5 Highly granular access control configuration for compliance with technical policies [D.5].

4.2.6 Regular software lifecycle and upgrades.

4.3 Servers must be hardened against future hardware vulnerabilities.

4.3.0 JEDI allocation cannot exceed a significant portion of Contractor allocation.

4.3.1 Regular hardware lifecycle and upgrades.

4.4 Network security achieved through border control and blending with non-JEDI traffic.

4.4.0 Intra-application traffic encrypted with cryptographic certainty.

4.4.1 Inter-application traffic requires CIO approval and cryptographic certainty of encryption.

4.4.2 Applications globally available and responsive.

4.4.3 JEDI traffic cannot exceed a significant portion of total Contractor traffic.

4.4.4 Establishing direct fiber links to DoD Meet-Me-Points for unclassified connections.

4.4.5 Establishing direct fiber links for classified connections.

4.4.6 Internet addressing of JEDI traffic cannot be distinct from other Contractor traffic.

4.5 Defense requires the Contractor, CIO, and internal operators to work closely together.

4.5.0 The CIO may require specific physical and logical component supply chains.

4.5.1 The CIO may require specific traffic profiles be intercepted, modified, or stored.

4.5.2 Internal and boundary security capabilities able to protect applications.

4.5.3 The CIO may require specific hardware, software, or allocation profiles be blocked.

4.5.4 Contractor personnel attain training and clearances pursuant to the DD Form 254 [D.0].

4.5.5 Regular testing of infrastructure, DoD testing allowed on request of CIO.

4.5.6 Vulnerabilities known to the public, Contractor, or government mitigated.

4.5.7 Investigations of vulnerability exploitation conducted.

4.5.8 Activity which reveals DoD usage information is considered an investigation.

4.5.9 The CIO determines priority between mitigations, then investigations, then testing.

4.5.10 All information yielded from mitigation, investigation, and testing shared with the CIO.

4.5.11 Marketplace services rapidly reviewed for compliance by a documented process.

4.5.12 The Offeror's marketplace must support security scanning of new and existing services being offered and also include a rapid method to notify customers using any marketplace service that a vulnerability has been discovered.

4.6 Audits to determine the extent of compromise from attack must be possible within reason.

4.6.0 Forensic and compliance audits pursuant to NISTIR 8006 [D.6] coordinated with the CIO.

4.6.1 Providing information on physical components, logical components, and risk management.

4.6.2 Providing physical and logical access and location records.

4.6.3 Providing allocation and traffic usage records.

4.6.4 Providing records of internal and boundary security incidents.

4.6.5 Providing mitigation, investigation, and testing records.

4.6.6 Providing infrastructure destruction records.

4.6.7 Records stored with the highest classification level of their source applications.

4.6.8 Records are available at the request of the CIO and other requiring officials [D.7].

4.7 Application level risk management [D.8] by DoD is enabled via the above requirements.

A Scenarios

These are examples of questions the Contractor must be able to answer, and the CIO must be able to verify through records available for audit.

A.0 Unauthorized Access: Who gained access and how did they do so?

A.1 Physical Misuse: What hardware is missing or modified and what devices were left behind?

A.2 Logical Misuse: Which affected accounts took what actions and accessed what data?

A.3 Unexpected Ingress: What behavior signatures did the traffic exhibit?

A.4 Unexpected Egress: What was exfiltrated and to whom was it sent?

A.5 Software Bug: Which applications were affected or exploited?

A.6 Hardware Bug: What infrastructure was affected or exploited and when was it discovered?

B Parties

B.0 Department of Defense (DoD) - Customer for cloud infrastructure.

B.1 Chief information officer (CIO) - The DoD CIO, or their designated authorizing officials.

B.2 Contractor - Contractor responsible for delivering JEDI.

B.3 Internal auditors - The agencies(s) appointed by CIO to audit JEDI (e.g., JFHQ-DODIN).

B.4 External auditors - The contractor(s) directed by CIO to audit JEDI.

B.5 Internal operators - Governmental groups tasked with security (e.g., USCYBERCOM).

C Definitions

C.0 Contract - Agreement between the Contractor and DoD for JEDI cloud.

C.1 Infrastructure - Physical and virtual components that comprise JEDI.

C.2 Account - Provisioned identity able to manage infrastructure and platform services.

C.3 Unclassified infrastructure - FedRAMP Moderate compliant for all unclassified levels.

C.4 Classified infrastructure - FedRAMP High compliant for all classification levels.

C.5 Server - Physical infrastructure related to transforming or storing data (e.g., database).

C.6 Allocation - Server resources dedicated to JEDI as measured by CPU and GPU capacity.

C.7 Network - Physical infrastructure related to packaging or transmitting data (e.g., router).

C.8 Traffic - Internal or external, ingress or egress related to JEDI as measured in bytes.

C.9 Addressing - Data used to route data (e.g., IPv6).

C.10 Data center - A physical site containing significant infrastructure.

C.11 Application - Infrastructure dedicated to and managed by a single account.

C.12 Failover - Unanticipated migration of application operation with minimal downtime.

C.13 Cryptographic certainty - Assurance unmediated data transfer does not occur [D.3].

C.14 Vulnerability - Weaknesses affecting data transfer, service availability, or code execution.

C.15 Testing - Assessments and attacks to verify security compliance and incident response.

D References

D.0 DoDM 5200.01, DoD 5220.22, DD Form 254, et al.

D.1 FAR 2.101, et al.

D.2 DoD 5220.22-M, NIST SP 800-88, et al.

D.3 CNSSP 15, DoDD 8100.02, FIPS 140, Circular A-130, et al.

D.4 NIST SP 800-63, et al.

D.5 NIST SP 800-53, et al.

D.6 NISTIR 8006, et al.

D.7 44 U.S. Code Chapter 21, et al.

D.8 NIST RMF, CSSP, et al.