DOD JEDI Contract – It doesn't care about Cybersecurity!

The Department of Defense's (DoD) request for proposal (RFP) for the Joint Enterprise Defense Infrastructure (JEDI) does NOT care about Cybersecurity! How can I justify that statement? Read further.

July 26th 2018, the DoD released its highly contentious JEDI contract. This contract has garnered immense scrutiny from the industry for various reasons. One of the key themes proponents have used to justify this contract is the speed to market of capabilities that JEDI will enable (presumably through Cloud and "Industry Best Practice"). Since industry is great at speed to market (economics) and terrible at security (one could argue because of the acceptance of Cybersecurity risk for speed), how is JEDI going to be successful following that recipe? (I make this claim [terrible at security] based on the number of breaches we continually see in the news [both on-prem and cloud) on a continual basis]). I am shocked at how terrible this RFP was written. It does NOT outline Cybersecurity protections well at all. I find that fascinating.

I decided to read through the entire RFP (three times actually) to look for Cybersecurity impacts and requirements of this unprecedented Request for Proposal (RFP). I wanted to see how the contract defines Cybersecurity. What are the requirements and/or standards required from JEDI? How will the RFP process assess offerors' responses and against what Cybersecurity criteria? Can we surmise from what is provided in the RFP just HOW JEDI will address Cybersecurity?

Let's begin with the RFP document itself….

The first we begin to see Cybersecurity as a component of the RFP is in Section C1: Performance Work Statement.

The Offeror shall meet all requirements of Attachment J-6, JEDI
63 Cloud Cyber Security Plan. In the event of a conflict between the JEDI Cloud Cyber Security Plan
64 and the PWS, the JEDI Cloud Cyber Security Plan takes precedence over the PWS. For
65 administration purposes both the PWS and the JEDI Cloud Cyber Security Plan are listed as
66 attachments in Section J. However, for the purpose of FAR 52.212-4(s), they shall be deemed
67 incorporated into Section C1.

Here we can see the reference to Attachment J-6, JEDI Cloud Cyber Security Plan. Additionally, it cites data destruction according to Attachment J-6, JEDI Cloud Cyber Security Plan. Then there is reference to Classified work that will have specific information and requirements within the Task Order (TO) for classified work. So, for this document, I'll focus only on *the unclassified work*.

DOD JEDI Contract – It doesn't care about Cybersecurity!

Buried in section C4 are some security implications:

Section C4: Contractor Control of Certain Parts of JEDI Cloud

1. The legally enforceable ability for the prime contractor to maintain control over certain parts of JEDI Cloud is critical to meeting the security requirements of this contract. The Government expects that it will need to direct the Contractor to affect alterations or configuration changes to JEDI Cloud for purposes of addressing critical security vulnerabilities. The Contractor must be able to decisively and rapidly respond in the interests of national defense. For the purpose of this section, the direction concerning critical security vulnerabilities may come from the DoD CIO in coordination with the JEDI Cloud Contracting Officer and CCPO PM.

2. For purpose of this section, "rapidly" means in 8 hours or less from Government notification. All Government-directed alterations or configurations changes will be agreed upon by both the Government and the Contractor prior to implementation.

3. Depending on the urgency of the circumstances, the agreed-to alteration or configuration change may initially be achieved by oral direction from the JEDI Cloud Contracting Officer, but to the extent it is deemed a "change" as defined by FAR clause 52.212-4(c), the change will be subsequently reflected in a written agreement of the parties as soon as practicable.

4. Throughout the entire period of performance, the Contractor shall maintain control, as defined in this section, over the following parts of JEDI Cloud for both the unclassified and classified environments:

a. Underlying hardware infrastructure, including networking components within the data centers;

b. Underlying software layer, including the hypervisor and networking components;

c. Software platform offerings (excluding third-party marketplace offerings); and

d. Hardware and software components of all points of presence.

5. "Control" means that, for the part of JEDI Cloud in paragraph 1 above, the prime contractor either:

a. Is the owner, as defined in this section, paragraph 6, as evidenced by self-certification. The Government may request additional documentation to prove ownership at any time and with any frequency throughout the period of performance; or

b. Has a bilaterally signed agreement (Control Agreement) that is binding for at least 11 years with the owner granting the prime contractor the following rights:

i. Unrestricted physical access; and

ii. An ability to rapidly affect changes to the owned parts.

This Control Agreement must state that it may not be terminated by the Owner without at least 120 days notice to the Government. The JEDI Cloud Contracting Officer may request confirmation that the Control Agreement has not been altered or terminated at any time.

6. "Owner" means that, for the parts listed in paragraph 1, the entity has a legally enforceable claim or title, which includes the rights listed in sub-paragraphs 5.b.i and 5.b.ii. The owner must have a legally binding and recorded document evidencing ownership.

DOD JEDI Contract – It doesn't care about Cybersecurity!

This section discusses ownership and operational control. It is foundationally about accountability. The Cybersecurity aspect is about accountability of vulnerability management and ownership of asset management.

Then we get to the only real security section within the RFP.

Section H4: 535 **Additional Security**
536
537 1. Security requirements is one material condition of this contract. This contract and any
538 resulting TOs shall be subject to immediate termination for cause, without the requirement for a cure
539 notice, when it has been determined by the JEDI Cloud Contracting Officer that a failure to fully
540 comply with the security requirements of this contract resulted from the willful misconduct or lack of
541 good faith on the part of any one of the Contractor's directors or officers, or on the part of any of the
542 managers, superintendents, or equivalent representatives of the Contractor who have supervision or
543 direction of:
544
545 a. All or substantially all of the Contractor's Cloud business, or
546 b. All or substantially all of the Contractor's operations at any one plant or separate
547 location in which this contract is being performed, or
548 c. A separate and complete major industrial operation in connection with the
549 performance of this contract.
550
551 2. The legally enforceable ability for the prime contractor to maintain control over certain parts
552 of JEDI Cloud is another material condition of this contract. This contract and any resulting TOs shall
553 be subject to immediate termination for cause, without the requirement for a cure notice, when it has
554 been determined by the JEDI Cloud Contracting Officer that a failure to fully comply with the
555 security requirements of this contract resulted from the lack of control required by Section C4.

Note this section assigns responsibility for the security of this contract but does not define what is that security. It also defines that the prime contractor is responsible for the supply chain. It also sets the stage that the contract can be immediately terminated for cause (related to security).

That's it. Hmmm. Can that really be all there is for the unclassified portion of JEDI? Well, as you well know if you do business with the US Government, you get an entire list of Federal Acquisition Regulations (FAR) thrown at you as terms and conditions of the contract. Additionally, as DoD, you also get Defense Federal Acquisition Regulations Supplement (DFARS) clauses. So, what is in the RFP as FAR or DFARS clauses that are Cybersecurity relevant?

1. **52.204.2 Security Requirements (AUG 1996)**

DOD JEDI Contract – It doesn't care about Cybersecurity!

2. **52.204.21 Basic Safeguarding of Covered Contractor Information Systems (JUN 2016)**
3. **52.239-1 Privacy or Security Safeguards (AUG 1996)**
4. **252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting (OCT 2016)**
5. **252.239-7010 Cloud Computing Services (OCT 2016)**
6. **252.239-7018 Supply Chain Risk (OCT 2015)**

What does these 6 things refer to? Three of them (first, third and sixth) are exclusively focused on requirements associated with classified systems. Since not in scope for this paper, that leaves three (second, fourth and fifth). The fourth and fifth are associated with ensuring authorized personnel is allowed access (though it doesn't prescribe how) and of course, requiring compliance with the DoD Security Requirements Guide (SRG). That leaves the second FAR clause. On the surface it has 15 basic requirements for all Federal contracts. Is there anything else in the RFP not in the clauses? There is mention of not being relieved of other requirements such as Controlled Unclassified Information (CUI). That now adds the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 as a requirement. There is no mention of other standards that are required like OMB requirements, Cybersecurity Framework requirements, Cybersecurity Workforce Framework requirements, Insider Threat requirements, Advanced Persistent Threat requirements, Controlled Unclassified Information, Cybersecurity Resiliency Review, NIST and/or DOD Risk Management Framework (RMF) approaches, Engineering Resilience requirements, etc.

In the instructions for the proposal volumes, there are some other requirements identified as well. In the proposal volume instructions there is one mention of a requirement in section 1, sub-factor 2. The requirement states:

No fewer than three physical existing unclassified CCO data centers within the Customs Territory of the United States, as defined in FAR 2.101, that are all supporting at least one IaaS offering and at least one PaaS offering that are FedRAMP Moderate "Authorized" by the Joint Authorization Board (JAB) as demonstrated by documented evidence.

So, FedRAMP Moderate authorization is required (although FedRAMP is not a Cybersecurity specific requirement).

Next, in factor 4, there are more requirements laid out in an objective format. They are:

In Volume II, Factor IV (Tab D), it states:

Factor 4 - Information Security and Access Controls (TAB D)

1. The Offeror shall provide its proposed approach for information security, specifically:

DOD JEDI Contract – It doesn't care about Cybersecurity!

2819 a. Patching and vulnerability management of hardware, software, and other system components
2820 that comprise or are provided by the Offeror's proposed solution, and the ability to control
2821 enforcement of patching based on vulnerability criticality.
2822 b. Managing supply chain risk for hardware, software, and other system components.

2823 c. Auditability of both the physical location and logical isolation of any hosted service to ensure
2824 compliance with security policy.
2825 d. Automated breach identification and any processes for breach mitigation, isolation, and
2826 reporting.
2827 e. Self-service and automated tools for preventing and remediating data spills of classified or
2828 other controlled information, including the ability to locate and erase all related data.
2829 f. Ability to erase data and purge the associated media in both unclassified and classified
2830 environments.
2831 g. Self-service tools to access data and analysis generated by threat detection systems. The
2832 ability to provide notifications and findings to system owners. The ability to provide raw logs
2833 to the government for analysis.
2834 h. Ability to onboard new services into the Offeror's marketplace in a rapid and secure manner,
2835 and executing against a clearly documented process for reviewing existing marketplace
2836 offerings for security and other policy compliance. The Offeror shall provide three examples
2837 of previous new service rollouts and how each service was reviewed for security and policy
2838 compliance.
2839
2840 2. The Offeror shall provide its proposed approach for access controls, specifically:
2841 a. Managing technical policies from one account to all JEDI Cloud accounts, and the ability to
2842 control access to services and restrict configuration parameters.
2843 b. Highly granular attribute and role-based access control configuration, and the ability to assign
2844 permissions to roles IAW technical policies.
2845 c. Object and resource access control management, including data and resource tagging.
2846 d. Token-based and time-limited federated authentication allowing a user to assume a role
2847 within the cloud environment at all classification levels.
2848 e. Indicate which access control capabilities are available via the Offeror's web interface,
2849 command line interface (CLI) application, and/or API.

These certainly provide more details about Cybersecurity. But, this isn't comprehensive, nor compliant with today's Cybersecurity Guidance. As, I continued to read, there were more directions in the form of guidance on how to submit the volumes of proposal and the evaluation criteria.

With the addition of the DD254 and JEDI Security Plan, that is it. Nothing else is in the RFP about Cybersecurity. However, we do find something interesting in the evaluation criteria for the RFP. Phase I of the evaluations was Factor 1 only. And, there will be no further evaluation if Factor 1 is

DOD JEDI Contract – It doesn't care about Cybersecurity!

not rated "acceptable". The only perceived Cybersecurity component of Factor 1 is FedRAMP Moderate "authorized" cloud instance. That is, it.

If the offeror is rated "acceptable" for factor 1 (they have evidence of a FedRAMP Moderate authorization), then they will proceed to phase two. In phase 2, the evaluation of factor 4 (Information Security and Access Control) is:

3308 **Factor 4 - Information Security and Access Controls**
3309
3310 1. The Government will evaluate the quality of the Offeror's proposed information security
3311 approach and the degree to which the proposed solution meets the requirements in Section L, Factor
3312 4(1)(a-h). As part of this evaluation, the Government will consider the following:
3313 a. The frequency, accuracy, efficacy, and degree of automation of patching and vulnerability
3314 management of hardware, software, and other system components. The degree to which
3315 patching enforcement can be controlled based on vulnerability criticality.
3316 b. The quality of supply chain risk management for hardware, software, and other system
3317 components.
3318 c. The degree to which the physical location and logical isolation of hosted services is
3319 discoverable and auditable.
3320 d. The degree to which breach identification is automated, and efficacy of processes for
3321 mitigation, isolation, and reporting.
3322 e. The degree to which tools and automation can prevent and remediate data spills, including the
3323 efficacy of the process for locating and erasing all related data and purging all related media.
3324 f. The degree to which the Offeror is able to erase data in any environment.
3325 g. The degree to which data generated by all intrusion detection technology, network traffic
3326 analysis tools, or any other threat detection performed is captured. The efficacy of analysis on
3327 the data generated. The degree to which users can control the manner in which notifications
3328 are communicated, and the breadth of configuration options for alerts generated by threat
3329 detection systems. Whether the Offeror provides the ability to deliver raw logs to the
3330 Government for analysis.
3331 h. The efficacy and quality of the process for onboarding new services into the Offeror's
3332 marketplace in a rapid and secure manner. The degree to which the Offeror was able to
3333 rapidly and securely add offerings to the marketplace in the examples provided. 3334
3335 2. The Government will evaluate the quality of the Offeror's proposed access control approach
3336 and the degree to which the proposed solution meets the requirements in Section L, Factor 4(2)(a-f).
3337 As part of this evaluation, the Government will consider the following:
3338 a. The range of functionality for creating, applying, and managing technical policies for one
3339 account and across all JEDI Cloud accounts.
3340 b. The degree of granularity of the permissions available, and the ease of discovery and
3341 assignment to roles.
3342 c. The efficacy of the capability to tag data objects and resources for billing tracking, access
3343 control, and assignment of technical policy.

DOD JEDI Contract – It doesn't care about Cybersecurity!

3344 d. The range of capability, ease of implementation, and use of modern standards for federated,
3345 token-based, time-limited authentication and role assumption.
3346 e. The degree to which the Offeror has implemented modern standards for any API and CLI
3347 access and the degree to which these APIs or CLIs, if any, match or exceed the abilities of the
3348 Offeror's web interfaces for user, account, identity, and access management.

This is interesting in that introduces new objectives in the form of evaluation criteria. However, even with these new requirements, it still isn't comprehensive.

So, we need to add the JEDI Cybersecurity Plan and DD254 to this analysis. The DD254 basically says any data in use from the DoD regardless of its classification or handling requirements apply to JEDI. There are references to For Official Use Only (FOUO) documents that won't be reviewed here. There are also inferences that classified task orders will have their own security guidance under the JEDI ID/IQ. Those, obviously, won't be discussed here.

So, that leaves the JEDI Cybersecurity Plan.

The most glaring thing that stands out from the JEDI Cybersecurity Plan is that it is a document that professes a "new" approach to defining Cybersecurity. It creates "an exacting bar for outcomes." They purposefully aren't explaining how they want things done. That is quite fascinating. One can interpret this as JEDI doesn't know how to select Security Controls. Another interpretation, it is a test to the offerors understanding of the Security Controls (although, I doubt it based on the lack of security focus on selection criteria). A nefarious interpretation is that DOD is purposefully trying to create a solution with little focus on Cybersecurity on purpose. What could be the reasons behind that?

The JEDI Cybersecurity Plan drops in passing quite a few nuggets that should alarm any reader…

1) Main Section
    a. The solution is subject to DoDIN security requirements.
    b. DOD SRG is required to be compliant.
        i. Some explicit requirements about isolation, encryption and Personnel Security.
    c. Immutable logs in accordance with DOD Instruction 8530.01
2) Compliance Section
    a. Explicit JEDI Contract requirements
    b. Report according to 252.239-7010
    c. Open to all JEDI authorized auditors
    d. Vulnerabilities and Patching expectations
    e. Personnel training according to DD254
    f. Accreditation according to DD254
3) Modernization Section

DOD JEDI Contract – It doesn't care about Cybersecurity!

   a. Must stay current with Security Technologies
   b. Must stay current with Hardware, Software, Firmware and Hardware
4) Explicit Requirements
   a. High Availability requirements
   b. Physical Access Control requirements
   c. Logical Control requirements
      i. MFA according to DOD Instruction 8520.03 and NIST SP 800-63 series
      ii. Unique IDAM requirements
   d. Network security requirements
   e. Possible Supply Chain prohibition preparedness
   f. Requirement for internal and boundary capabilities to detect
   g. May require network profiles capture and storage
   h. Risk vulnerability notification
   i. Manage vulnerabilities and test for vulnerability exploitation
   j. Audits
   k. DOD Instruction 8510.01 Risk Management Framework
5) Appendix D – References
   a. Joint Publication (JP) 3-12(R): Cyberspace Operations, dated February 5, 2013
   b. Executive Order 12829 – National Industrial Security Program, dated January 8, 1993
   c. DoD Cloud Computing Security Requirements Guide, Version 1 Revision 3 dated March 6, 2017
   d. DFARS 252.239-7010: Cloud Computing Services
   e. DoD Instruction 8540.01: Cross Domain (CD) Policy, dated August 28, 2017
   f. CNSS Instruction 1253F Attachment 3: Cross Domain Solution Overlay, dated September 12, 2017
   g. DoD Instruction 8530.01: Cybersecurity Activities Support to DoD Information Network Operations, dated July 25, 2017
   h. DoD Directive Form 254: JEDI ID/IQ Contract Security Classification Specification
   i. Federal Acquisition Regulation (FAR) 2.101: Definitions
   j. DoD Directive 5220.22-M: National Industrial Security Program Operating Manual, dated February 28, 2006
   k. National Security Telecommunications and Information Systems Security Advisory Memoranda (NSTISSAM) Level I: Compromising Emanations Laboratory Test Standard
   l. Committee on National Security Systems (CNSS) Policy 15: Use of Public Standards for Secure Information Sharing, dated October 20, 2016
   m. CNSS Policy 30: Cryptographic Key Protection, dated December 28, 2017
   n. DoD Instruction 8520.03: Identity Authentication for Information Systems, dated July 27, 2017 and subsequent guidance dated June 2018
   o. CNSSP 25: National Policy for Public Key Infrastructure in National Security Systems, dated December 11, 2017
   p. NIST SP 800-63: Digital Identity Guidelines, Revision 3 dated June 2017

DOD JEDI Contract – It doesn't care about Cybersecurity!

q. NIST SP 800-88: Guidelines for Media Sanitization, Revision 1 dated February 5, 2015
r. NISTIR 8006: Cloud Computing Forensic Science Challenges, dated June 30, 2014
s. 44 USC Chapter 31: Records Management by Federal Agencies
t. DoD Instruction 8510.01: Risk Management Framework (RMF), dated July 28, 2017
u. DoD Memorandum: Cybersecurity Activities Performed for Cloud Service Offerings, dated November 15, 2017
v. CNSS Instruction 1253F Attachment 5: Classified Information Overlay, dated May 9, 2014
w. DoD Directive 8100.02: Use of Commercial Wireless Devices, Services and Technologies in the Department of Defense Global information Grid, dated April 23, 2007
x. FIPS PUB 140-2: Security Requirements for Cryptographic Modules, dated December 3, 2002
y. OMB Circular No. A-130: Managing Information as a Strategic Resource, dated July 28, 2016
z. CNSS Policy 11: Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products, dated June 1, 2013

And, that is everything that is openly available for JEDI. Given that this contract is the "future" of modernizing the US Fighting Force's Information systems, one would expect World Class Cybersecurity. Yet, this document doesn't recognize the obvious requirements and compliance issues, it doesn't set examples of what security controls are required (other than a few explicitly called out), it doesn't discuss Federally mandated requirements like Cybersecurity Framework, Cybersecurity Workforce Framework, all privacy requirements, their inter-relations with each other, the Continuous Diagnostic Monitoring requirements, the APT requirements, the Insider Threat requirements, the Cybersecurity Supply Chain objectives/requirements, and, most importantly, it doesn't discuss how Cybersecurity will evolve like the technology modernization requirements. This last one is about how will the Cybersecurity requirements change as DoD and NIST requirements change? The future US Government requirement of evidentiary based assessments is not addressed here, SP 800-53 rev5 is not addressed here, Cybersecurity Framework CRR is not addressed here, and assessment requirements and models are not addressed here. As you can see, I can go on and on about how this RFP isn't about Cybersecurity.

This RFP is about a certain technology (AWS) meeting their "go to market quickly" and be relevant strategy. I'm VERY disappointed.

In conclusion, DoD has just asked offerors to provide security and meet a few disjointed objectives (some in SOW others in Volume instructions). If the government wishes the offeror to know and apply all the required Cybersecurity measures, then they should state that in the RFP, otherwise, how can they hold these contractors accountable? While I know that companies will bid on this (can't afford to miss this

DOD JEDI Contract – It doesn't care about Cybersecurity!

opportunity), I would tell them this is a UNICORN. It can't be done as laid out in this RFP. Don't bid on it and send a message to DoD over this terrible RFP.

For Additional Information Contact:

Eigenspace
312 Main Street, Suite 300
Gaithersburg, MD 20878
240-654-4097
www.eigenspace.us