# DOD Guidance for NOT doing your job…

The Department of Defense released to the industry the "DOD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented" this week for review and comment from the industry. Why did the DOD issue this? One can only assume it was because the DOD needs to be clear about how they view and assess industry partners, contractors and supply chain members consistently and equably in the proposal/contracting process. There are a few other possibilities, like source selection teams aren't qualified to review and assess proposals, Contracting Officers aren't qualified to review and assess proposals and/or delivery, or DOD feels compelled to help the industry meet this new benchmark being levied against them and providing some guidance. I find this interesting from an academic analysis point of view.

Once can interpret this as the DOD "flinched". Let me elaborate. The USG through NIST and DOD have been publishing more and more requirements and standards in Cybersecurity over the last 5 years. This push comes with many forms of cost. The industrial base and supply chain have been struggling to comprehend, organize and execute to this new standard for a multitude of reasons. So instead of being Draconian and telling the industrial base what they have been telling them and building up to (get there, no relief in sight, just do it), they now have a way to grade you if you do not make the deadline (which has come and gone) and still use the guise of "risk management" to allow it to happen. I think it is a deadly mistake. The DOD (and NIST and the USG and USCERT) has been quite clear on the direction, objectives and deadlines they want to meet (you just have to have Cyber Awareness and read). The Industrial base is resisting. This creates a conundrum for the USG. Do you just "not do business with those who don't get there for whatever reason"? I say, "yes", or you a) won't achieve your goals, b) you undermine your authority by caving, and c) you can not force cultural change by giving in to the culture.

Now, let's look at this document without the context of concern above. What is in this document? First, it is a table. The table has a few elements one can consider to be attributes. The first column – the NIST SP 800-171 Security Requirement. This is further broken down into NIST SP 800-53r4 Security Controls. Here's our first problem. NIST SP 800-53 has revisions. The revision 4 was released and updated in 2013, 2014 and 2015. Since then NIST has been working on revision 5 which is out. There is no transition period outlined by NIST. Additionally, revision 4 to revision 5 is a wholesale change (not a simple update). I know of many contracts throughout the USG that requires the use of the latest version and some even go as far as requiring implementation of DRAFT versions from NIST. So, this document is already outdated from the start. Moving on, next column lists out NIST's priority scheme for security controls. Then we get to start with the new material in column (DOD Value High (5-3) Moderate (2) Low (1). The first observation is this isn't a bell curve (which would have been High (5) Moderate (4-2) Low (1) or something similar. It is totally weighted top 60% is High. 80% is everything but low. Is everything a priority to DOD? Also, note that DOD aligned the weight to the NIST Priority, so why not just use what is already


# DOD Guidance for NOT doing your job…

established instead of creating an entirely new attribute to a control everyone must keep up with? Now on to the last column, "Comments". Within this section, something new happened and it is quite disturbing… The DOD created a "cheatsheet" for its users. They created a "Method(s) to Implement". The whole concept of the NIST frameworks and guidance has always been to NOT tell you the "HOW" to do it but to drive objectives and results. Here, the DOD opts to tell us "Method" to implement. Now, on the surface, what is the target audience going to do with this? Contractors, partners and supply chain members are all going to say, "Well, if this is what DOD wants to see, this is what we will do." This just became the defacto checklist for proposals and delivery. NOT real security. Remember, CUI (NIST SP 800-171) protections were JUST for the protection of data's confidentiality. It does NOT address all security required for a solution. We moved to a do what I say compliance checklist and not think about real security. Its applicability is VERY limited and won't apply to IoT, ICS, SCADA, CPS, and other non-IT system applications. VERY DISAPPOINTING.

However, the biggest issue I have with this document is it totally misses the qualitative aspects of assessing Cybersecurity. The NIST SP 800-171 has a corresponding assessment guide, NIST SP 800-171a. Was that mentioned at all? NO. Additionally, there is no real understanding of HOW the assessments are handled only the assignment of NIST and/or DOD's "DOD VALUE" scoring. Let's look at an example:

3.1 – Access Control

3.1.1 – Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

Security Control – AC-2 Account Management

NIST Priority – P1

DOD Value – 5

METHOD(S) TO IMPLEMENT – IT Configuration

That is all we are given for the first row in the DOD Guidance table. What does this tell us? Or more importantly, what does it NOT do for us? It says, AC-2 needs to be implemented for credit for NIST SP 800-171. NIST assigns it a P1 and DOD assigns it a value of 5. The only added value here is the arbitrary assignment of a DOD Value attribute. The final column (Comments) lists, "Method(s) to Implement" and its value is "IT Configuration." This may sound simple. This may sound benign.

# DOD Guidance for NOT doing your job…

But, I have serious issues with this…. What IT Configuration? What standard? Who assesses compliance to this arbitrary standard? Does a singular IT Configuration requirement work for any technology or any implementation of any technology?

Now, let's take what we know from AC-2 and understand ALL the things that are missing from true Cybersecurity (per our tenants in the Cybersecurity Awareness and Resiliency - www.eigenspace.us/docs/CybersecurityAwarenessandResiliency.pdf).

AC-2

In order to "get credit" for an organization to get credit for AC-2, they must address all the related controls (AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13). There is no mention of that. BUT, we can take that even farther to understand to get credit for each of these an analysis would also need to be run. For sake of length, I won't run that analysis, but you get my point. Next, AC-2 belongs to many baselines (Organizationally Implemented control per NIST SP 800-171r5, CSRA 578, Cybersecurity Framework, Cybersecurity Resiliency (per the NIST SP 800-160 vol2), DOJ FBI's baseline, FedRAMP's baseline, GDPR requirements, or OMB requirements). There are also many non-Federal specific baselines like COBIT, PCI-DSS, SANS CSC20, ISO 27001 or ISO 15408, etc.). As you can see, if you are in these spaces, then this control causes you to have to look at these other standards and confirm if they are in play or not, and, more importantly, have they been properly mitigated or implemented.

BUT, the most IMPORTANT thing we don't have here, is assessment information. What assessments are required by AC-2 in order to get proper credit? Here is the first problem. What is "proper credit" for the control? Here is where we have the concept and objective of the USG to have evidentiary based assessments to prove you did what you say in order to get credit for it. No longer is this a, "yeah we do that" and we are done. Now, you must define the assessment and provide evidence that you did that. So, now that the definition of evidentiary based assessments is the "proper credit", then what assessments are required. Here the proposed DOD Guidance is woefully faulty. We should be focused on NIST SP 800-171a as the starting point. NIST has started the work here.

From the NIST SP 800-171a:

# DOD Guidance for NOT doing your job…

| | | |
|---|---|---|
| 3.1.1 | **SECURITY REQUIREMENT**<br>Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | |
| | **ASSESSMENT OBJECTIVE**<br>*Determine if:* | |
| | 3.1.1[a] | *authorized users are identified.* |
| | 3.1.1[b] | *processes acting on behalf of authorized users are identified.* |
| | 3.1.1[c] | *devices (including other systems) authorized to connect to the system are identified.* |
| | 3.1.1[d] | *system access is limited to authorized users.* |
| | 3.1.1[e] | *system access is limited to processes acting on behalf of authorized users.* |
| | 3.1.1[f] | *system access is limited to authorized devices (including other systems).* |
| | **POTENTIAL ASSESSMENT METHODS AND OBJECTS**<br>Examine: [*SELECT FROM:* Access control policy; procedures addressing account management; security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; list of conditions for group and role membership; notifications or records of recently transferred, separated, or terminated employees; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; other relevant documents or records; list of devices and other systems authorized to connect to organizational systems].<br>Interview: [*SELECT FROM:* Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities].<br>Test: [*SELECT FROM:* Organizational processes for managing system accounts; mechanisms for implementing account management]. | |
| | DISCUSSION ON SECURITY REQUIREMENT 3.1.1 | |

Note this is only for the one NIST SP 800-171 Security Requirement (objective). The related controls and their assessments aren't here. This is where we, as an industry, truly fail.

The next point I would like to lay out is the issue of "IT Configuration". What does that really mean? We note that to get credit for this one security control, AC-2, we have CM-5, CM-6, CM-11 as related controls. What does it mean? How do we assess? What configuration are we changing that will trip all kinds of other issues or damage position of the related controls? This ill-defined implementation guidance will only confuse and dilute the true Cybersecurity process.

# DOD Guidance for NOT doing your job…

Given that DOD is intimately involved with NIST guidance publication and they are driving compliance rigidly, I can't help wondering how DOD would publish a proposed Cyber document like this. We know that the USG is moving to have its entire Cyber Workforce moved to be aligned with Cybersecurity Workforce Framework. I know, it isn't normal practice to publish names and qualifications of the authors of these types of documents. BUT, I can't help wondering with a document riddled with issues like this, are the authors even qualified per CWF standards to drat these?

To recap, I am really fearful that this document, if allowed to progress to final, will become a defacto checklist for the industry and NOT achieve any of the Cyber goals that this process would undermine. It could even possibly weaken Cybersecurity Posture with unintended consequences. In my opinion, it should be scrapped.


For Additional Information Contact:

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