Meeting Government Cybersecurity Requirements with the Niagara Framework

May 28, 2020

Q&A

Answers provided by Aleta Technologies, Inc.

1. Do you have a ATO for the Air Force? I have had a hard time working with the Base IT Dept.
   It doesn't quite work that way. Each system must have an ATO, or can leverage a special sort of generic ATO which is a "Type Authorization". "Type Authorization" is used to deploy identical copies of the system in specified environments. An ATO cannot be reused in nearly all cases. When working with the Air Force Comm Squadron, ask them if the system can be connected to the designated CE vLAN or COINE. These network segments are provided specifically for Civil Engineer control systems including N4/JACE. Also, the Air Force Civil Engineering Center (AFCEC) is a valuable resource and can possibly bridge the gap between you, the base CE, and Comm Squadron to help resolve issues.

2. As well USA Security requirements, have you undertaken the same level of review for deployment within UK / EU in-line with similar legislation and compliance requirements?
   RMF requirements are specific to the US (only) - however, we have responded to requests from other governments and partners who want to know how the process works and what they could do in a similar manner- many US DOD sites are overseas (hundreds) and this material applies to them as well. The EU/UK have not embraced RMF, but usually use something like ISA62443. The "validation" and risk acceptance concepts are not really within ISA as they are within RMF.

3. How does a building controls manufacturer get involved in the process? If a site owner must initiate the process (as opposed to a manufacturer simply meeting a standard like UL, BACnet, etc.), then it seems that the site owners will just go with products that they are used to using instead of starting the process for a new product, manufacturer or service provider. This could end up stifling advancement into new products and technologies.
   RMF is a system-level certification. Each system is authorized. The problem for vendors is how to minimize customer burden through re-use of artifacts, process, and configurations. There is a product-level certification coming called Control Systems Tested Products List which relates to but is different from RMF.

4. Are there other conditions (technical or non-technical) for product acceptance for DOD sites? e.g. being on the GSA Schedules?
   Depends on the type of product. For switches, routers, etc. there is an UC Approved Products List. For control systems, there is something called the Control Systems Tested Products List (CS TPL) coming in the near future.

5. If a project takes 18 months, could there be many software / hardware upgrades needed along the way?
   Yes, these hardware/software upgrades will need to be accounted for during the RMF process and placed on the official HW/SW list which is provided to the Government customer. The documented change management process will need to be followed.

6. What is needed to get remote, live access to DoD facilities?
   DoD facilities do not typically connect outside their network and require high level security access to log into any system. Usually a Government Furnish Equipment (GFE) laptop is provided to the contractor after the contractor has successfully completed the user account/VPN process managed by the local network service provider. Military networks cannot be accessed from public dot com; must be on .mil using an approved DoD installation VPN. User account process requires CAC card to be obtained by the user, background check, and other items as required by the local installation.

7. Do you have an idea on the market size for these DOD projects?
   While Aleta Technologies performs just the cyber portions and we therefore don't always have visibility in overall project size, the DoD control system projects we see range in size from a couple million dollars to $300M per project.

8. How do we set up MFA – Multi-Factor Authentication?
   Often, the local network service provider can assist with this through existing PKI (ie CAC card) deployment. 2FA can be very complex. Use existing infrastructure (e.g., Installation Campus Area Network, Base network) whenever possible to save cost. However, if the system is isolated/closed then the Govt customer may require MFA methods such as YubiKey or RSA. YubiKey is an easier deployment for closed systems and can be installed into environments without Active Directory integration; RSA is more complex and requires RADIUS authentication configuration and other technical items for it to be fully functional.

9. The example RFPs placed a large burden on the contractor in terms of performing a significant amount of the effort needed for the ATO. My understanding is that neither the UFC or UFGS require that level of effort. Can you comment on UFGS/UFC content and how that is different from the examples you cited?
   A traditional RMF effort requires much more work and time. The UFC/UFGS provide less RMF requirements for the contractor to perform and more on the Government customer. In the UFC/UFGS process, the contractor only provides a list of submittals outlined in the UFGS 25 05 11 guide spec to the Government. The Government is required to perform the RMF steps.

10. How can examples be set for DOD projects for developing countries like Bangladesh?
    https://www.nist.gov/publications contains numerous useful publicly-available documents. NIST Special Publication 800-37 is the Federal RMF, and Special Publication 800-53 Rev 4 contains all the security controls (security requirements).

11. If your team was sub-contracted to facilitate the RMF process on a DOD base, with Niagara N4, however no ATO, ATC, etc. currently exist, how much would your firm charge for that support? Rough Order of Magnitude.
    In general, prices range from $35K to $500K+, with the vast majority being in the lower half of that range. The main cost drivers are: 1) Which DoD Service is the system being installed for? 2) How many servers, workstations, laptops, network switches, and Level 2 devices are to be accounted for to undergo security engineering (e.g., DISA STIGs, SCAP scans, Nessus scans, etc.)? 3) Is the system isolated or to be connected to the base network? 4) Where is the installation the system is being installed at (i.e., OCONUS, CONUS)?

12. How much of the control networks daily operations will be affected with the BACnet SC? Will this be towards new construction with Government and Military Sites or existing sites?
    We can provide DoD "success stories."

13. Is there a way to get past the weather/http proxy service issue with 4.8 and lower?
    Aleta defers to Tridium for the answer.

14. RMF Certification is system specific. Is RMF certification required per site or deployment to a building?
    RMF authorization will apply to a specific project and system; for example if a base had 500 buildings, the approved project may span 10 or 50 of them, or the entire site. For every RMF system authorization, there is a system authorization boundary which delineates what hardware/software is included in the RMF ATO.

15. Part of the DOD requirements says only 32 devices allowed per network. Is there an allowance for expansion mstp cards? They do not allow bacnetip networks. Our only solution would be to have multiple Jaces in a building with more than 64 devices.
    We are unaware who the DoD customer is being referenced in the question, but they seem to be very restrictive. We would agree that the best course of action is to install multiple JACEs within the buildings with more than 64 devices to accommodate the customer's request. Regarding the allowance of the expansion MSTP cards, there should not be an issue to expand these cards since the overall security risk is low for Level 1 devices using appropriate defense-in-depth security architecture measures and operational/functional capability of the system is not being adversely impacted.

16. Has DOD used Vdi to access systems (Citrix etc..)?
    Yes, virtual desktop infrastructure (VDI) is used by most DoD Services. Aleta has not seen the DoD use VDI for control systems; only Enterprise IT. However, if you have a very large control system with many operator HMIs and the such then VDI could be a good solution to implement.