I have been thinking about how to handle wide-ranging schedule synchronization since I joined the Acquisition Corps in 2007. This is my third attempt to launch a collaborative scheduling tool. My first two attempts failed for various reasons, but mainly because of too many stakeholders and the complications and cost of establishing the software within a military data center. It is only since the Defense Information Systems Agency (DISA) introduction of MilCloud that I have been able to gain traction.
Be advised, the processes that are touched on in this article are not for the faint of heart. My initial intent was to elucidate the multiple processes that work together in order for a Software as a Service (SaaS) to achieve Common Access Card (CAC)-ready operations within a military cloud environment. However, the labyrinth of processes proved too unwieldy to properly document and convey in an article. Instead, I suggest areas for improvement to ease future endeavors.

Department of Defense Instruction (DoDI) 5000.87 (Operation of the Software Acquisition Pathway)) states that program managers (PMs) should “Leverag[e] existing enterprise services, if available, is preferred over creating unique software services for individual programs.” I interpreted this to mean, if the Enterprise Level Service you require is not available, go create your acquisition adventure by establishing that service. One year into this process, there were only seven SaaSs at Impact Level 4 (IL4)—and they were all from large software businesses.

DISA defines impact level as storage or processing of information in the cloud and the potential impact of an event that results in the loss of confidentiality, integrity, or availability. IL4, which is necessary for Controlled Unclassified Information (CUI), requires a CAC for access and allows use of a “.mil” domain name. DISA’s MilCloud offerings provide an alternative path with less resistance and fewer stakeholders to consult.

MilCloud also pushes the cost into the license subscription, which means that upfront infrastructure costs do not burden military organizations. This article outlines the top-level processes involved in establishing a SaaS.

PMs need a tool that formalizes all the scheduling aspects of their program. Excel and PowerPoint are not project management tools—they do not scale up and are prone to configuration management errors. Microsoft Project is not collaborative, and it fosters stovepipes. The Microsoft Project implementations that I have seen force users to proceed through a gatekeeper. In my opinion, the impediment of a gatekeeper outweighs the tool’s benefits. Users ultimately generate their own siloed schedules, thus defeating the usefulness of an integrated master schedule (IMS) at the PM level. Although PMs obtain IMSs from their vendors, those schedules never include details of the bureaucracies and acquisition rigor that PMs need to negotiate. Think acquisition documentation, contracting, testing, integration, fielding, reporting requirements, user feedback, and the plethora of external dependencies that all programs have. We will call this amalgamation of schedule events the Government Integrated Master Schedule (GIMS).

The benefit of using a DoD-wide, collaborative-scheduling tool is that leaders will be able to push the work package responsibilities down to the lower levels where they belong. Decomposing the schedule down to its lowest-level work packages and requiring the work package owners to keep the packages up to date reduces friction. This naturally allows collaboration. The distributive nature of the app is also accompanied by a Kanban view. Mirroring the processes set forth in the Office of the Under Secretary of Defense for Acquisition and Sustainment’s Agile 101 primer, the popular agile Kanban framework enables visualization of the workflow and allows the team to monitor work in queue, work in progress, and the overall flow from inception through completion. The collaborative environment and the Kanban view improve efficiency and facilitate agile acquisition. This particular app is not just agile; it displays a Gantt chart, the critical path, and driving paths. It can allow for shared resources and cross-project dependencies. Think of the possibilities of linking multiple product offices (from different Program Executive Offices—even inter-Service) to know when the product(s) will really be delivered.

To facilitate the GIMS, I aligned with Smartsheet. The vendor already was pursuing hosting within Amazon Web Services (AWS) GovCloud and had licenses for commercial use available for purchase on a General Services Administration schedule. Below is an outline of the process we followed to achieve use of this particular vendor’s SaaS. It may seem oversimplified, but there are numerous forms, meetings, and approvals required throughout. The items below are just the wave tops.
PROCESS

1. Commercial application establishes hosting as a SaaS in one of the DISA-approved cloud providers (Amazon Web Services, Azure, Google, etc.):
   a. These providers already meet specific security control measures. This allows the commercial app to attain IL4 more easily.
   b. A commercial app that already has obtained a moderate rating under its Joint Authorization Board (JAB) Federal Risk and Authorization Management Program (FedRAMP) Provisional Authority to Operate (P-ATO), will streamline the IL4 process since DISA offers reciprocity for the accreditation. This is highly recommended as the JAB ATO accredits the app at an IL2, where there are more than 320 controls. IL4 includes most of the same controls and adds at least 45 more.
   c. A SaaS’ IL2 offering usually will have a distinctly different URL from its commercially offered version and thus will have low traffic. This results in a low reputation score and renders the site mostly unreachable due to military DNS filters, and this prevents resolution of its problems.

2. A military unit sponsors an app provider through the Information Level (IL) approval process—DISA requirement:
   a. Cloud Service Provider (CSP), the commercial app provider that intends to provide services via a cloud service, must use and fund a Third Party Assessment Organization (3PAO) and a separate auditor.
      i. The 3PAO will review and assess the risk of all controls working side by side with DISA. The auditor will review all documentation and artifacts from the service provider to ensure compliance with DISA IL4 controls.
      ii. DISA likely will have experience working with specific 3PAOs, so one can be selected that is well known and has a good working relationship with DISA.
      iii. CSP responds to and makes all adjustments found by the 3PAO evaluation. Upon adjudicating all findings, the provider can submit all relevant artifacts.
   b. The sponsoring unit will need to assign two full-time IT/cyber specialists (Information Assurance Management Level II/II) to DISA’s Joint Validation Team (JVT). The JVT will perform a technical review/validation of the CSP/3PAO completed and signed documentation listed below.
      i. Readiness Assessment Report (RAR)
      ii. DoD System Security Plan (SSP), Level 4/5 Addenda for FedRAMP+ controls FedRAMP baseline SSP for baseline controls
   c. Unit engagement is key to prevent the process from stalling.
   d. After validation, DISA will issue a provisional authorization.

3. The sponsoring unit assesses the system, culminating in its authorizing official issuing an Authority to Operate (ATO).

4. The sponsoring unit then submits for connection to the military network via the DISA Cloud Connect Team, works with DISA and the vendor to choose a domain name, and the vendor connects its single sign-on system to the CAC authentication mechanism.

5. The sponsoring unit purchases the requisite licenses, establishes app administrators, trains its workforce, and rolls it out.
Completing the processes should not have taken 28 months. Six months into the process there were only 11 services available on the DISA Cloud Service Offerings List. By the time we achieved CAC authentication services, there were more than 50 on the list (however, many were only at IL2). I appreciate the patience of the various other government and military organizations that have been waiting for my team to reach the finish line. I initially had time estimates for each portion of the process, but the COVID-19 pandemic added time friction to each of the sub-processes, once we found and understood them.

The time estimates from the process that DISA depicts here now appear to be measured from a pre-COVID-19 high-priority system. DISA told us multiple times that it had higher-priority efforts. An executive order from the Army’s newly established Enterprise Cloud Management Office (ECMO) caused us to obtain an exemption from using the Army’s newly established Enterprise Cloud Management Office (ECMO) rather than DISA. But ECMO granted us an exemption because projected use for the SaaS was DoD-wide. Here’s how DISA can improve the process:

1. Provide a more detailed “Process Map,” where each node of the map links to the appropriate sub-process page that has the entrance criteria, documentation, requirements, and process exit criteria. As it currently stands, multiple DISA sub-organizations are shepherds and gatekeepers in their slice of the overarching process.

2. Provide a point of contact for each major step in the process on the process map. At various times in this adventure, we were unsure with whom we should talk. We were referred to other offices multiple times.

3. Establish redirects to avoid link rot, and then implement them properly. For example, do not redirect to a high-level page where users are forced to search for the updated or analogous link. This has become less problematic now, but in the beginning, multiple bookmarks of mine unexpectedly stop working.

4. Think about how to make this process faster. Two-plus years is more time than required for one technology generation.

In conclusion, many blame the Acquisition Corps for slow materiel procurement. Scheduling tools by themselves are not a panacea. Process changes, and adherence to those actual processes, are required for overarching success. However, we will not go faster by using the same unfit tools we have been using. We need enterprise, collaborative, scalable, modern tools that will enable us to reach our potential and remove the ad hoc approach to scheduling.

Navigate to https://app.smartsheetgov.com/ to obtain details on how your office can start using this particular SaaS. In addition, if your program or product has a schedule dependency with mine, let’s link up in the system. If this app does not suit your needs, then follow the process above and create your own acquisition adventure. Now, if I can just get some DoD organization to provide a blanket ATO for these services, my Army Program Executive Office wouldn’t be burdened with maintaining the ATO for all of DoD.

**MDAP/MAIS PROGRAM MANAGER CHANGES**

With the assistance of the Office of the Secretary of Defense, Defense Acquisition magazine publishes the names of incoming and outgoing program managers for major defense acquisition programs (MDAPs) and major automated information system (MAIS) programs. This announcement lists recent such changes of leadership for both civilian and military program managers.

**ARMY**
- **COL MICHAEL J. WILLIAMS** relieved **COL TROY W. CROSBY** as program manager for Mission Command on March 2.
- **AIR FORCE**
  - **COL KIRT CASSELL** relieved **COL MATTHEW BONAVITA** as program manager for the Advanced Pilot Trainer, T-7A Redhawk, on March 19.

**NAVY/MARINE CORPS**
- **CAPT RICHARD M. GENSLEY** relieved **CAPT JOHN E. DOUGHERTY** as program manager for Precision Strike Weapons (PMA 201) on Jan. 4.
- **CAPT JOHN E. DOUGHERTY** relieved **CAPT ALBERT G. MOUSSEAU** as program manager for Next Generation Air Dominance (PMA 230) on Feb. 1.
- **COL VASILIOS E. PAPPAS** relieved **COL David C. Walsh** as program manager for the Attack Helicopter Program H-1 (PMA 276) on March 25.

The author can be contacted at tyronne.g.lastrapes.mil@mail.mil or Tyr/lastrapes@gmail.com.

**LASTRAPES** is product manager for Aerial Communications and Mission Command (PdM ACMC) in the U.S. Army’s Program Executive Office for Aviation at Redstone Arsenal in Alabama. He has a master’s degree in Systems Engineering Management from the Naval Postgraduate School, is Level III-certified in Program Management and Level II in Test and Evaluation.