The Challenge

The Cybersecurity Maturity Model Certification (CMMC) is a unified cybersecurity standard designed to ensure the protection of information in future Department of Defense (DOD) acquisitions. Specifically, it was developed to protect and prevent unauthorized access to Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) within the Defense Industrial Base. The goal of CMMC is to assess and verify the institutionalization and maturity of cybersecurity practices and processes of DOD contractors via a third-party assessment.

The DOD issued an interim rule, effective November 30, 2020, which updates the Defense Federal Acquisition Regulation Supplement (DFARS) to implement the assessment methodology and CMMC framework for DOD procurements as well as adds a new requirement for cybersecurity assessment under the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 framework. Under the proposed rule, contracting officers must verify that an offeror has a current NIST SP 800-171 DOD Assessment (110 controls) on record in the Supplier Performance Risk System (SPRS), before contract award, for applicable solicitations.

Defense contractors will coordinate directly with a certified independent CMMC Third-Party Assessment Organization (C3PAO) to request and schedule a CMMC assessment. Defense contractors can only request an assessment if they have implemented all practices for the requested assessment level – Plans of Action and Milestones (POA&Ms) are not acceptable. Once the assessment process is finalized, upon successful demonstration of the appropriate capabilities and organizational maturity, the organization will receive the corresponding CMMC level certification. All defense contractors will need to be at least CMMC Level 1 unless they solely provide Commercial off-the-shelf (COTS) products.

Achieving certification is a daunting task, especially for small businesses, like Psoas LLC, that lack the capital and resources necessary to understand and execute all requirements.

The Solution

The Defense Cybersecurity Assurance Program (DCAP) assisted small businesses, such as Psoas LLC, by offering expert cybersecurity consulting services and matching funds for CMMC pre-assessments to help identify gaps in existing practices and processes to become compliant with DFARS and NIST requirements. The CMMC pre-assessment provided a valuable characterization to show where Psoas LLC meets these requirements and where the next waypoints are located to achieve CMMC.
About Psoas LLC

Based in Dayton, Ohio, Psoas LLC provides engineering services in three primary areas: open architecture design, model-based systems engineering, and sensor integration. Specifically, Psoas LLC leverages model-based systems engineering and open architecture best practices to design hardware and software systems from a top-down perspective that promotes interoperability and portability. Psoas LLC provides solutions that eliminate inhibitors to innovation and the rapid fielding of new technologies, such as vendor lock and proprietary interfaces, with primary target applications in the DOD and healthcare settings. In the DOD setting, Psoas LLC is a subcontractor that acts in an advisory role to the Air Force to support the Sensor Open Systems Architecture™ (SOSA) Consortium in designing the next generation of sensors based on open architectures. Psoas LLC is researching the methodologies necessary to transfer the technologies and lessons learned from the DOD to promote medical device interoperability in the healthcare setting.

The Process

"The pre-assessment performed by Sawdey Solution Services, Inc. did more than provide a score; it provided an understanding of each of the requirements and a roadmap to mitigating each shortcoming discovered throughout the entire process."
Insight from Psoas LLC

Sawdey Solution Services, Inc. provided a pre-assessment to ensure an unbiased score in the SPRS.

Psoas LLC shared the following about the results of their pre-assessment:

"One eye-opening finding of the pre-assessment came when comparing it to an assessment performed internally. Certain cybersecurity requirements were more nuanced than originally perceived, which of course translates to vulnerabilities and a lower SPRS score. Sawdey Solution Services made it easy to identify the CMMC shortcomings and provided a roadmap to compliance."

The Benefits

Psoas LLC shared the following about how the DCAP program impacted their small business:

"The grant provided by Ohio State enabled the affordability of the pre-assessment that then enhanced the understanding of cybersecurity requirements, which ultimately led to Psoas LLC being accepted into a pilot program by a cybersecurity vendor looking to provide CMMC services to small businesses. In addition to this,
Psoas LLC now feels comfortable meeting the CMMC requirements in the time frame laid out by the DOD without a lapse in funding.

"Pre-assessments performed by companies like Sawdey Solution Services and grants provided by entities like Ohio State are invaluable to achieving and maintaining cybersecurity requirements put forward by the DOD."