Sample Army Problems for Vendors and for the AFCEA Meeting

Guidance: *In order to outpace peer competitors, Army leadership is challenged to build a survivable unified end-to-end network that enables leaders to prepare, lead, and fight in high-intensity conflict with Unified Action Partners against any adversary from anywhere they choose at any time to win decisively in all domains and all environments.*

1. **MODERNIZE – Cloud & Application Migration/ Enterprise/Hybrid Cloud Strategy** (LOE #2.3)

Problem Statement – The Army develops and sustains applications in a highly distributed manner, and does not have a holistic mechanism to modernize or manage application life cycles. The Army must align to DoD cloud guidance and policy while implementing a strategy to modernize and migrate thousands of applications to the cloud. By doing so, the Army must decrease the cyber-attack surface, protect its data, and fully leverage solutions that generate efficiencies through automation.

Why this is a problem – Army application owners have been reluctant to migrate en masse due to technical limitations, funding availability, priorities, and perceived risk. Cloud services procured in a multi-vendor environment are priced at a higher rate than could be provided in a common environment along with creating individual contracts with cloud service provider (CSP). This model limits our ability to aggregate data for the purpose of Artificial Intelligence and Machine Learning.

Desired Outcome – Establish an enterprise cloud ecosystem that is Artificial Intelligence (AI)-ready, hybrid, protects Army data, increases lethality at each echelon, and generates reinvestment opportunities for modernization. Deploy an agile and flexible cloud framework to adapt legacy software to quickly meet changing operational environments, increase readiness, and improve cybersecurity. The Army is looking for commercial vendors who can advise on comprehensive enterprise/hybrid cloud strategy that will integrate tactical and non-tactical infrastructure.

2. **MODERNIZE – Data Cleansing** (LOE #2.3)

Problem Statement – The Army has data in multiple sources in various degrees of data cleanliness and uncertain data quality. Poor data management and operations without enterprise oversight result in "dirty data" influencing decisions. Data silos make the problem worse, distancing the Army from its goal to be a "data-driven organization." Army leaders are unable to see, share, and act on accurate and quality data.

Why this is a problem – According to a published report, the Pentagon failed its first ever audit in November of Fiscal Year 2018. The same report highlighted three issues of note from the audit, 1) audit and inventory management, 2) cybersecurity, and the 3) poor data quality within the existing systems. Unstructured data is yet another problem. Examples of unstructured data include files that reside on a file share, including text or binary files like Word, PowerPoint, audio files, video files, image files, and more.

It's common for medium-to-large organizations to have terabytes of unstructured data that they need to manage, backup, and potentially recover. It's both a problem for the information technology (IT) department and a significant, if not always visible, cost to the organization in terms of resources (storage space, backup space, backup time, and staff resources) to manage so much unstructured data.

Desired Outcome – The Army needs industry support with efficient and effective data modeling and tagging so that Army can operationalize its data securely. The Army needs open source data quality assessment and standardization (or cleansing) tools to refine data as an enterprise asset. Further, the Army needs innovative ways to protect data throughout its lifecycle no matter the network environment. Finally, the Army needs to eliminate duplicative, out-of-date, and erroneous data and information policies. Without a modernization framework, the Army will continue to experience conflicts with published guidance and will not garner a cohesive strategy to supply relevant data to decision makers on a timely basis.

3. LIFECYCLE MANAGEMENT – Total Army Asset Visibility/Configuration Management (LOE #4.1/4.2)

Problem Statement – The Army has an enormous software license and hardware expenditure that is not accurately tracked and measured. For a complex organization such as the Army, total asset visibility (TAV) need to be comprehensive and organized. There is no enterprise solution across the Army that can provide this capability.

Why this is a problem – The Army discovered a significant shortcoming in operational reporting of Army Cloud Investments for storage, compute power, applications captured in the Army's authoritative IT Investments system of record, the Army Portfolio Management Solution (APMS). The Army CIO/G-6's Enterprise Computing Division has continued its collaboration with Army organizations to improve the quality and accuracy of its APMS data. Although significantly improved, the Army Cloud Investments data in APMS still does not meet the Army's data quality standards.

Desired Outcome – The Army needs industry support to implement IT total asset visibility (IT TAV) to baseline the network and requirements. This includes inventorying and rationalizing applications, software, and hardware that will aid in cloud migrations as well as Enterprise licensing; determining what is general purpose or fit for purpose; and correlating the data from both data stores (VTA & TVEA) and uncover hidden intelligence. It also includes enabling leading edge technologies, such as internet of things (IoT), machine learning, predictive modeling, and artificial intelligence. TAV capability will support the end-to-end process, including data collection, quality control, transformation, analytics, reports, and autonomous configuration control activities.

4. SECURITY & SURVIVABILITY – Risk Management Framework (RMF) Optimization (LOE# 6.3)

Problem Statement – The complexity of the RMF process contributes to non-compliancy. RMF consists of numerous mandated security controls and correlation control identifiers that must be met. The Army must be able to fully assess the Cybersecurity risk within Cyberspace to enable Cyber readiness and the fight in a contested environment.

Why this is a problem – The current RMF process is cumbersome and time consuming. RMF needs to be fully integrated in the lifecycle management of a capability. RMF processes needs to be automated, where necessary, to provide a capability to rapidly assess risk and risk mitigation strategies enabling leader's decisions.

Desired Outcome – The Army needs industry support to operationalize RMF to ensure successful implementation equally at the enterprise and tactical levels. The Army requires a tool (or suite of tools) that can seamlessly integrate with the current systems to automate RMF where possible to shorten the process.

5. SECURITY & SURVIVABILITY – Continuous Cyber Security Compliancy Monitoring (CCSCM) (LOE# 6.3)

Problem Statement – The integrity and security posture of Army infrastructures must be maintained continuously before, during, and after accreditation. Continuous monitoring will aid in insuring cyber security compliancy. CCSCM needs to assess risks, threats, and standards through a continuous automated method.

Why this is a problem – Continuous compliancy will insure Cybersecurity readiness and assist leaders with making informed cyber security decisions. CCSCM will reduce the human error and increase Army Cyber security readiness.

Desired Outcome – Establishment of a baseline tool or suite of tools for continuous monitoring is needed. CCSCM must provide real-time continuous monitoring of the Commander Cyber Readiness inspection (CCRI) controls. CCSCM must enable Army-wide consolidation and correlation of CCRI data.

6. SECURITY & SURVIVABILITY – Insider Threat (LOE# 6.1), Zero Trust Environment (LOE# 6.2)

Problem Statement – One-quarter of known breaches were the result of insider activity in 2017, according to a Forrester report. Insider Threats pose multifaceted problems for the Army. The threats can be intentional and unintentional. Both intentions provide similar devastation, if proactive and reactive/Disaster Recovery (DR) controls are not considered.

Why this is a problem – Cleared personnel are able to manipulate information systems and data maliciously, usually without detection. The detection of an insider threat is difficult, and once identified, the distinction between intentional and unintentional is challenging. Insiders often know the policies and other security controls that are in place to mitigate, detect, deter, and prevent attacks against the Army. Security policies address insider threats but there are minimal standardization of controls and tools to assist with the threat.

Desired Outcome - Development of a standard tool to identify indicators and defend against insider threats. Standardization allows auditors and other security personnel a common platform that can aid in quickly identifying and assessing incidents. This program will inform future protection measures to combat current and emerging insider threats. The solution should address Technical, Administrative, and Physical (TAP) Controls in order to be effective. Additionally, the Army requires assistance with composing Tactics, Techniques, and Procedures (TTPs) to make a more secured environment. There needs to be a "Never Trust, Always Verify" framework to ensure our Cyber Readiness. The Army is interested in a holistic security solution that could help ensure a zero trust environment through monitoring and trust assurance at every level.

7. SECURITY & SURVIVABILITY – Protected Data (LOE #6.4)

Problem Statement – Data security and integrity remain a top priority for the Army. Data is constantly being used, transmitted, and stored at multiple levels. Protection of data must include protection from internal and external threats. Manipulation of data could be just as malicious as theft of data. Safeguarding data should not degrade operations. Endpoints are one of our most critical avenues of approach/breach, so protection methodologies must include endpoints.

Why this is a problem – Loss of data is a principal concern for Army leaders. With so much data being used, transmitted, and stored, it is difficult to determine what data has been lost or stolen. In addition, the Army needs to have a more effective access control methodology for all echelons. The Army has been effective at protecting data at some levels of security, but other levels have been less effective.

Desired Outcome – An aggressive accountability and auditing tool is needed to inventory and safeguard data at all levels. The Army needs an automated methodology to tag and categorize all unstructured data, and to properly categorize and classify the data. This will support safeguard methods and protection activities. This must be a verifiable process that enables machine learning/AI. The ideal tool should address protection from loss of information, modification, and loss of availability, which should be in the forefront of Army Cyber protection and Cyber Readiness, and should include TAP controls to ensure all malicious avenues of approach are considered.