Tuesday, August 16, 2022
2:30 PM – 2:50 PM
The Need for Automated Data Security

Nancy Patel
Vice President, Public Sector
Immuta

Abstract:
As the Army continues to build toward cloud enterprise architectures and move away from legacy platforms, these systems increasingly require automated data security to be readily available across the force. Policies, regulations, laws, classification rules, and other protections must be implemented and enforced effectively to ensure that the right data is going to the right people, with the right access, and for the right reasons. Applying and enforcing unified data standards across the community for Industry, Intelligence, Defense, Federal, State, and foreign partners is not realistic, but the need for data protection and data handling is an element of common concern.

With the move toward an interoperable landscape, mission analysts, data consumers, and the warfighter require seamless access to data. Leveraging a data management platform at the data layer built to accelerate unified network operations and multi-domain operations (MDO) for data access across multiple data sources is essential to how the DoD will automate digital policy management and enable data access at the speed of mission. In addition, it is inevitable the Army will face disrupted, intermittent, and limited (DIL) network connectivity when deployed or on the move. As PEO-C3T works with the Network Cross Functional Team (N-CFT) to modernize the network, the data will continue to require protection, namely to release and/or redact information at the appropriate level, when the network becomes available. To effectively complete this work, the Army requires data management and analytic tools that create an effective balance between local and distributed computing storage. In addition, endpoint security capabilities must reduce reliance on network-based controls and mature identity, access and asset management to reduce insider threat.

Immuta understands the complexity of disconnected operations, and the transition from disconnect to connected environments. Immuta can be provisioned down to the tactical network cloud and can grant access to data in the same manner, whether the system is disconnected or connected. The IC, U.S. Military, and Foreign Partners will in many ways continue to maintain standalone information systems, but true digital integration will require a unity of effort for software and hardware within a common digital ecosystem in which information is collaboratively and continuously analyzed without burdening the customer with the management and data exchange between systems.

As the central point for data access, Immuta makes data available, discoverable, and secure, and ensures that policies can be created or changed rapidly. Immuta understands and is equipped to empower any Army Cloud Initiative, be it at the AIE (AC2SP), DAIIS, the Army's Enterprise Cloud Management Agency (ECMA), and PEO-C3T's Tactical Cloud Infrastructure. Immuta can bridge the data governance community to easily share and protect data between platforms such as ADVANA and JADC2, to include partner coalition networks, ensuring that information is accessible at the tactical edge and in a highly contested environment. With Immuta, the Army can leverage an automated data access governance platform that protects our national security intelligence information and provides the

principles, policies, processes, frameworks, tools, metrics, and oversight required to effectively manage data at all levels, from creation to disposition.