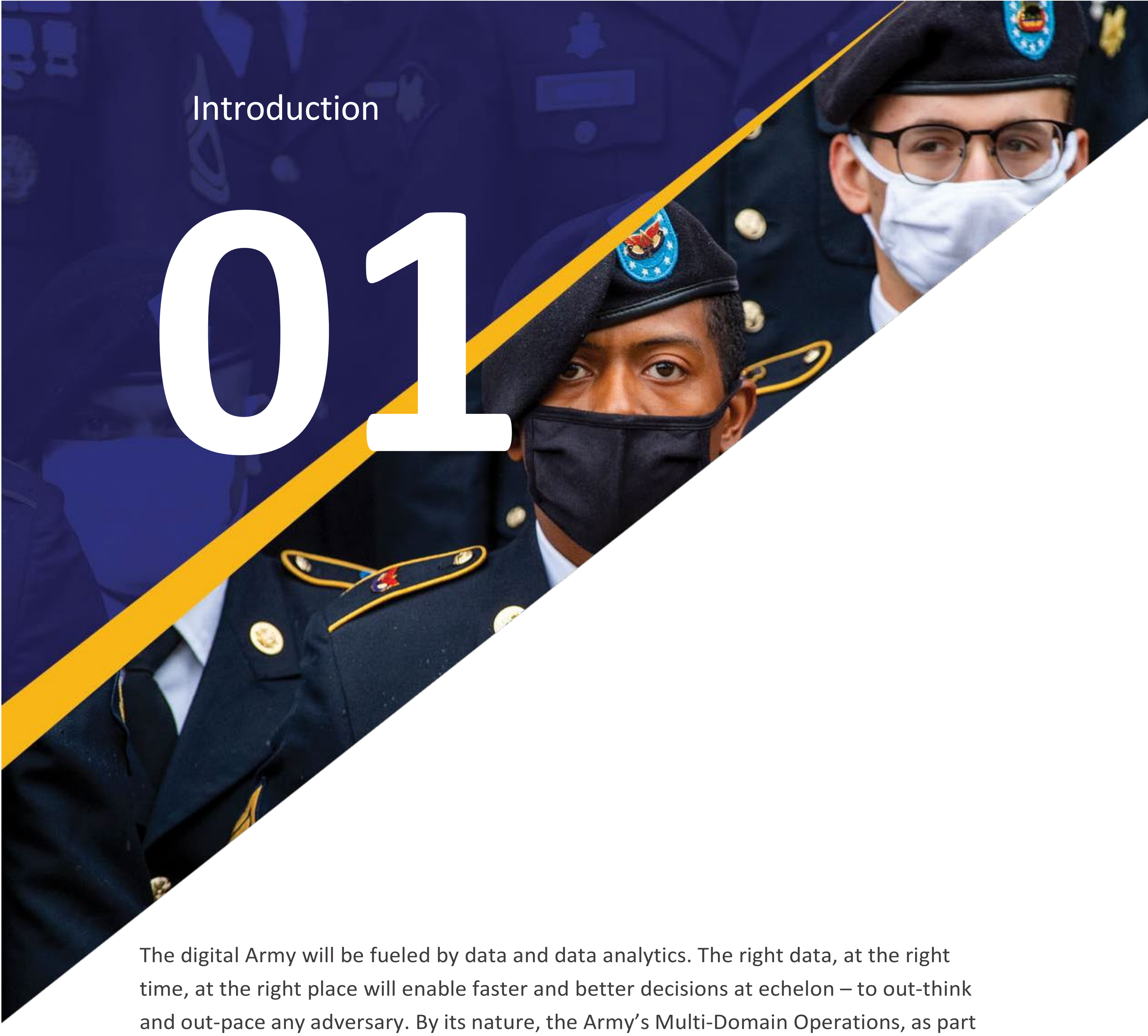
ARMY DATA PLAN

Office of the Chief Information **Officer**

Introduction

01



The digital Army will be fueled by data and data analytics. The right data, at the right time, at the right place will enable faster and better decisions at echelon – to out-think and out-pace any adversary. By its nature, the Army's Multi-Domain Operations, as part of Joint All Domain Operations, has a larger and increasing scope than earlier military operations. Each domain has its own growing information and data flow, from open-source intelligence, space-based sensors, cyber-space queuing to Soldier medical status and vehicle self-diagnostics. Today's Soldiers and Commanders require synthesis across these domains to dominate the battlespace. With the fires growing in range and automation and forces increasingly dispersed on the battlefield, speed of decision to neutralize critical targets can have rapid cascading effects to allow our forces to penetrate, disintegrate, and then exploit in order to win. Integration and speed of information is achieved through data and data analytics.

In her 8 February 2022 message to the force, Secretary of the Army Christine Wormuth set as her second goal for the Army to enable success on the future battlefield is to become "more data-centric. This objective nests with the 5 May 2021 Deputy Secretary of Defense Kathleen Hicks memo "Creating Data Advantage" which establishes five "DoD Data Decrees" to transform the Department into a "data-centric organization." The Decrees set the path to rapidly share decision quality data across the Department of Defense. Moreover, both Secretary Wormuth's and Secretary Hick's direction provides an operational lens for how the Department should implement the 2018 Evidence-Based Policymaking Act of 2018 that set Federal goals for data sharing and management.

Data enabled decisions, decisions that will outpace an adversary, will decide future battles. The Chief of Staff of the Army, General James McConville stated that data is a Commander's business. Army and Joint leaders have referred to data as the new ammunition. This is a useful comparison – when an Apache Attack Helicopter takes off on a mission armed with Hellfire missiles, Commanders intuitively know how many "stowed kills" are on a flight. Similarly, Commanders need to know how many "stowed kills" are enabled by their information. Like ammunition, data does not appear on the battlefield without management. Data needs to be designed, generated, checked for quality, inventoried, distributed, stored, used, and at some point, disposed of. Data life cycle management is just as vital as ammunition management to ensure it meets the Army's operational needs.

As per the Army Digital Transformation Strategy, data success will require the Army to prioritize, mature, and scale ongoing data management efforts. This requires addressing people, culture, and building a foundation for change.

People: The Army is increasing data literacy across Soldiers and civilians. Some will be specialists, such as data scientists or data engineers. However, to increase change at scale, the Army needs to increase the basic data skills for generalists that benefit from greater accessibility to quality data to improve daily decisions, that is, ***citizen analysts benefiting from our data democracy***.
Culture: The Army is evolving its culture, not only to embrace data for decision making, but to assist in its generation and quality control. Army leaders should not pass up opportunities to capture information of value to others but rather obtain and pass useful information for the greater good. The Army will achieve success when Army leaders at echelon ***treat data not as digital exhaust but as a strategic asset***. The main mechanism to facilitate this cultural change is through clearly defined and scoped projects in which data use provides operational success.
Foundation: The Army is building a data foundation to guide and accelerate change. The components of the foundation are both materiel and non-materiel. The primary non-materiel portions of the foundation are governance and clearly defined roles and responsibilities of data leaders. Materiel components include the Enterprise Data Service Catalogue, an enterprise API capability, simplified authoritative data products ready for use, and easy access to data platforms and the cloud.

In 2019 and 2020, under the Army Data Plan Implementation in Support of Cloud Migration Execution Order, the Army advanced in all three areas through select projects that: built skills, had near term success in building leadership and organizational understanding, and piloted several aspects of materiel and non-materiel foundational activities. Based on these lessons, the Army drafted a Roles and Responsibilities memorandum specifying key governance roles and their responsibilities in the data life cycle. The Army provided several "data objects" – a data product for use across the Army that simplified complex interactions and provided an easy reference for authoritative Title 10 and readiness data.

Overall, the Army has made the greatest progress in areas where decision makers, data analysts, data ownership and process ownership are aligned. The intelligence, cyber mission operations, finance, contracting, and logistics domains have this alignment and have demonstrated an ability to rapidly produce data analytic products in support of decisions. The warfighting mission area is the most complex and has the greatest cross-command sharing of data life cycle management responsibilities of all the Army mission areas. Given these lessons learned, this document provides a refined focus of the Data Cloud Order to facilitate rapid progress in developing a data-centric Army.

This Army Data Plan has four parts:

VAULTIS Principles

It lists the data principles: visible, accessible, understandable, linked, trusted, interoperable, secure.

Strategic Objectives

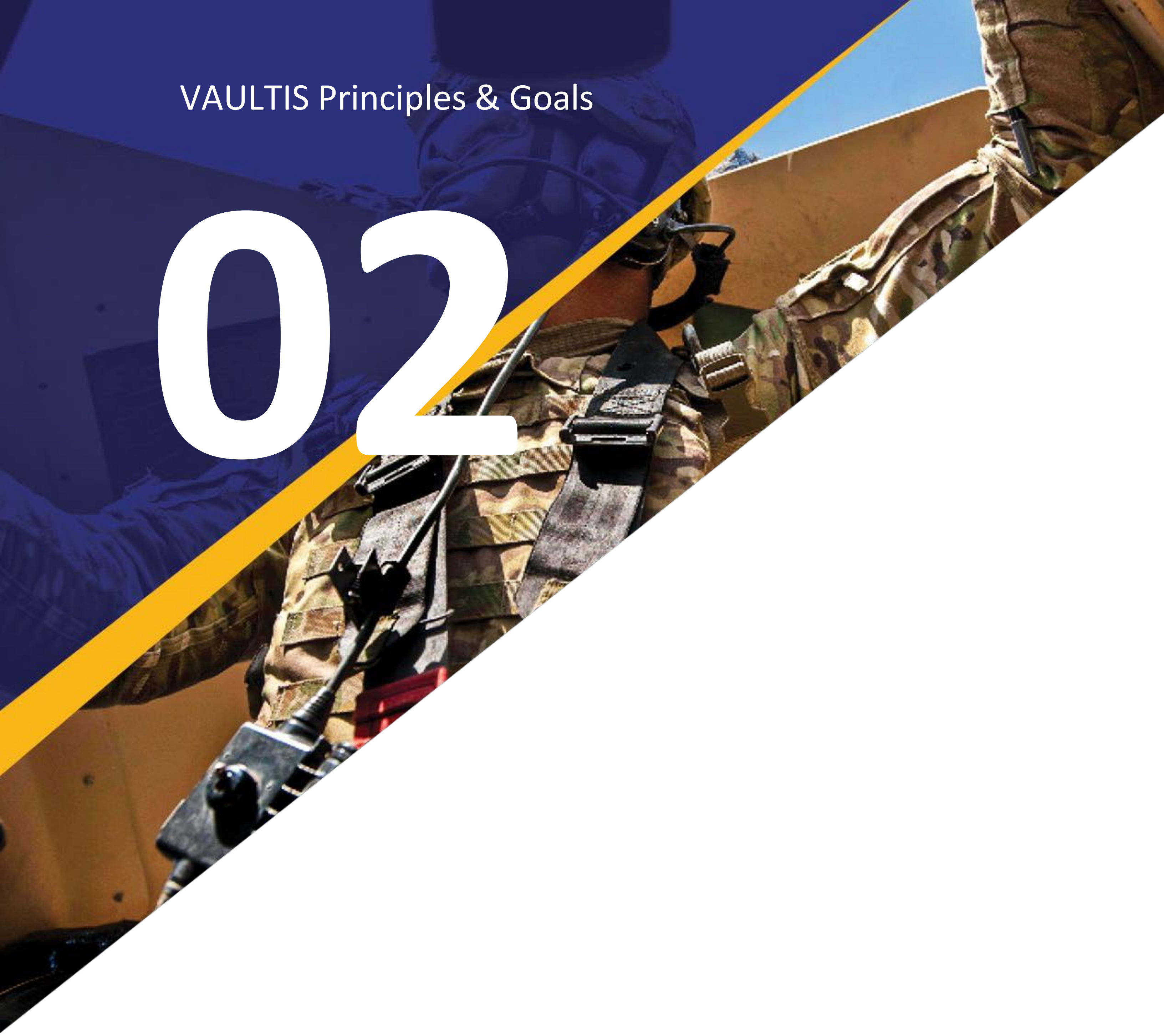
It defines the Strategic Objectives (SO) of the overall effort.

FY22-23 Initiatives

It describes the fiscal year (FY) 22-23 Plan, which outlines near-term activities.

Strategic Efforts

It defines Strategic Efforts (SE), which organize the activities that have been tasked to data community stakeholders.



02

VAULTIS Principles & Goals

Data that is visible, accessible, understandable, linked, trusted, interoperable and secure (VAULTIS) improves information sharing for decision-making advantage. These seven characteristics are described in the table below.

Goals	Definition
Visible	Consumers can locate the needed data. The goal of making data visible enables authorized users to discover the existence of data that is of particular interest or value. Data stewards, data custodians, and functional data managers are all responsible and obligated to make their data visible to authorized users by identifying, registering, and exposing data in a way that makes it easily discoverable across the enterprise, and to external partners as appropriate. Moving towards this type of data visibility allows users (person and nonperson entities) to discover and rapidly identify who is responsible for specific data assets, the location of data assets, the types of data assets available, and the means of accessing the data assets.
Accessible	Consumers can retrieve the data. The goal of making data accessible enables authorized users to obtain the data they need when they need it, including having data automatically pushed to interested and authorized users. Data accessibility must comply with Public Law (P.L.) 115-435, the Foundations for Evidence-Based Policymaking Act of 2018. DoD is making data, including warfighting, intelligence, and business data, accessible to authorized users. Accessibility requires that protective mechanisms (e.g., security controls) are in place for credentialed users to ensure that access is permitted in accordance with laws, regulations, and policies.
Understandable	Consumers can recognize the content, context, and applicability. Understanding data is critical to enable enhanced, more accurate, and timely decision-making. The inability to aggregate, compare, and truly understand data adversely affects the ability of the Department to react and respond. Without proper context, interpretation and analysis of the data could be flawed, resulting in potentially fatal outcomes. Bringing together business and technology and applying a data-centric approach enable massive amounts of data to be transformed into the insights needed to lead DoD more effectively and efficiently.
Linked	Consumers can exploit data elements through innate relationships. Data-driven decision-making requires Army data to be linked such that relationships and dependencies can be uncovered and maintained. Adhering to industry best-practices for open data standards, data catalogs, and metadata tagging, the Department ensures that connections across disparate sources can be made and leveraged for analytics.
Trusted	Consumers can be confident in all aspects of data for decision-making. Army data requires trust to deliver the needed value to its Service members, civilians, and stakeholders. Lacking confidence in the data may result in less timely decision-making or, consequently, no decision when one is warranted.
Interoperable	Consumers have a common representation/comprehension of data. Properly exchanging data between systems and maintaining semantic understanding are critical for successful decision-making and joint military operations. Achieving semantic as well as syntactic interoperability using common data formats and machine-to-machine communications accelerates advanced algorithm development and provides a strategic advantage to the Department.
Secure	Consumers know that data is protected from unauthorized use/manipulation. As per the DoD Zero Trust Strategy, protecting Army data while at rest, in motion, and in use (within applications, with analytics, etc.) is a minimum barrier to entry for future combat and weapon systems. Using a disciplined approach to data protection, such as attribute-based access control, across the enterprise allows DoD to maximize the use of data while, at the same time, employing the most stringent security standards to protect the American people.

Strategic Objectives

03

A set of eleven Strategic Objectives has been defined to express the long-term goals of the Army Data Plan effort in support of the Army of 2030. They are often expressed in terms of tenets or conditions of Multi-Domain Operations (MDO).

SO 1 - Operationalized Data-Driven Decisions that Support Multi-Domain Operations at Echelon

As part of Information Advantage, multi-domain operations require our Soldiers to make rapid, informed decisions within the decision loop of an adversary. Our goal is to avoid having our Soldiers either waste time finding the right data for decision or make decisions without the appropriate information. The desired outcome is that at all echelons the Army leverages authoritative data and improves its ability to identify, access, process, analyze, comprehend, and use information to improve decision-making while decreasing the workload. Data can be thought of in terms of integrated products that are delivered to our warfighter at the right time and place. The focus of this outcome is to refine, simplify, and automate data where appropriate to improve decision-making.

SO 2 - Decreased Time to Field Software and Decision Analytics to Outpace Any Adversary

The future battlefield is uncertain. Our nation can ask our Soldiers to perform missions we do not anticipate. The Army needs the ability to innovate and react at speed to support operations faster than our adversary. Our Army requires the ability to provide new decision aids, such as data analytics or new software tools to meet mission requirements. The desired outcome is to improve ways to decrease the time for rapid data analytics and for identifying needs across the process from validated need through to initial fielded capability. The focus is on speed of delivery of capability.

SO 3 - Resilient, Protected Data to Sustain Operations in Contested Environments

The Army cannot assume dominance in the cyber domain. Data assets are high value targets. The Army needs to ensure that in an operation it can count on data being resilient under enemy attack. The desired outcome is that the necessary changes in process and technology are implemented to ensure software, data, hosting systems, and transport systems meet and are kept within security requirements. Data has the right security levels applied, it is replicated, it is encrypted (confidentiality), any tampering is evident (integrity), and it is hosted in a manner that it is still discoverable if the network has pressure from attack (availability).

SO 4 - Holistic and Well-Understood As-Is Data Models to Allow Agile Responses to Changing Conditions

Understanding of the Army's data is foundational to Strategic Objectives 1 and 2. This objective spans beyond understanding of individual systems to broader Army processes. How information is generated, how separate activities interact using data as the critical interface, how the context of the data shapes or limits decisions – these are examples of critical questions the Army needs to answer. Without this understanding, the Army will not have the ability to achieve the speed identified in earlier SOs. This desired outcome is an Army with a mature understanding of how data supports the decision process—sources, needs, flows, processes— so that the Army can rapidly adapt these things in a dynamic environment. This SO focuses on the doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) aspects of quick delivery, and workforce familiarity with the processes and the systems to be updated.

SO 5 - Asset/Cost Transparency and Accountability

As part of the Army's data journey, the Army must make resourced informed decisions. Total life cycle costs need to be comprehensive so that labor and operations costs can be weighed against capital investments. The Army must also maintain control over its intellectual property associated with data and data rights. The desired outcome is an integrated view of costs that incorporates labor, processes, and tools throughout software and data lifecycles. Transparency and accountability are enabled through better cost accounting, contract structure, and automated monitoring tools, ensuring efficient use of resources and compliance with federal and DoD directives and inquiries into IT spending.

SO 6 - Data Available at the Point of Decision, to Employ Capability at Lower Echelons and in Disconnected, Intermittent or Limited (DIL) Environments

As a support to Strategic Objective 1, data needs to be available under wartime conditions against a peer adversary, including in disconnected, intermittent, or limited (DIL) environments. Not all data needs to be available everywhere on the battlefield. However, our combat formations need to be able to tailor data transmission and locally store data to add resiliency to the data needs at echelon. The focus of this SO is on the infrastructure supporting the data.

SO 7 - Cloud, Data, and Development, Security and Operations (DevSecOps) Enabled Workforce & Leaders That Support Digital Operations

The Army's journey to a data-centric organization will consist of continuous feedback between data tools and our Soldiers and civilians. In order for the Army to move at speed and scale, the data tools and software need to be intuitive, easy to use from mission need to continuous improvement. The Army recognizes that DevSecOps tools in a robust cloud environment are a critical component for speed and enablement. Easy to use tools will grow skills and data capacity within the Army. Skilled and empowered users in turn will drive change in the data toolsets. Army leaders will gain experience managing this feedback. The focus of this objective is providing the right environment to improve workforce digital literacy and culture.

SO 8 - Innovation and Modernization Through Data for Warfighting Functions in Order to Overmatch the Enemy

Data enabled operations span all the traditional warfighting functions, from fires to logistics to maneuver. The focus of this objective is to ensure all Army battlefield processes benefit from data driven decisions.

SO 9 - Secure & Interoperable Joint/Coalition Capable Army Data Platforms that will Enable Defeat of Near-Peer Adversaries

Joint All Domain Command and Control requires integration and synchronization of the Joint force at the data level. Army data processes and systems need to work seamlessly and flexibly with Joint and coalition partner equivalents in a dynamic wartime environment. Sharing of information at the data layer, as opposed to system integration, can offer this speed and flexibility. This objective requires purposeful data management to promote this type of interoperability. For example, data tagging to support data permission with coalition partners needs to be designed and managed as part of the data lifecycle. This objective focuses on joint and coalition interoperability at the data level.

SO 10 - Distributed Decision-Support Capability to Take Full Advantage of Army Expertise in Contested Environments

As an adjunct to Strategic Objective 6, the Army needs to ensure flexibility across the range of military operations. As Multi-Domain Operations transition between phases and have changing command and control (C2) relationships, with a very dispersed threat environment, the Army needs to call on the expertise needed to understand the pieces of that environment to enable decision making in a fluid situation under enemy attack. Distribution helps with resiliency and brings broader expertise to bear immediately that can't all be deployed or collocated. The focus here is on ensuring capabilities work from competition to conflict.

SO 11 - Refined Understanding of DOTMLPF-P for Future Cloud and Data Requirements

Any comprehensive change in the Army touches doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy. Becoming a data-centric Army is no different. The outcome is that the Army absorbs lessons learned regarding all DOTMLPF-P aspects of data enabled operations, incorporates them as requirements for the future Army, and applies them in operations.

FY22-23 Plan

04

The near-term lines of effort to achieve the Strategic Objectives are encapsulated in the FY 22-23 Plan. The approach is not to attempt to solve all digital operations issues in the Army at the outset. Gaining feedback from actual Army operations is necessary to ensure a lasting and effective solution. Therefore, the FY22-23 Plan focuses on exercises involving a small number of operational units. Once real-world experience is gained the lessons learned will be institutionalized across the broader Army in a later phase leading up to the Army of 2030. The following figure provides an overview of the Plan, with the text below each bubble describing each Step.

FY 22-23 Plan

Step 1	Echelons Above Brigade (EAB) Operational Framework	Forces Command (FORSCOM) and G-3/5/7 identify the units and exercises. Strategic Focus is:	• Theater • Aligned Corps –Multi- Domain Task Force (MDTF) • Divisions
Step 2	Finalize Prioritization of Needs	Get digital operations (i.e. data, cloud, Unified Network, and artificial intelligence (AI)) needs statements (from field units identified in Step 1)	• Mission statement of needs (requirements) to enable experiments that identify take-aways(capabilities to be sustained past the experiments and leave residual value)
Step 3	Finalize Prioritization of Solutions	SE teams identify solutions to address the capability gaps identified in Step 2	• Work with the units to further refine the requirements • Determine the nature of solution, resourcing, and timeline to achieve the solution • Bring in expertise as needed to assist (e.g. Cross-Functional Team skills) • Provide the plan to achieve the need
Step 4	Program Objective Memorandum 24 (POM24) Implications	Execution and Monitoring	• Provide the solution to the field/units • Monitor progress and capture lessons learned • Army Data Panel (ADP) to review implementations of the digital operations needs statements: resourcing, integration, overcoming friction points, proposed solutions, and policy issues • ADP to provide a foundation for follow-on work to include planning for the next POM cycle

Strategic Efforts

05

The lines of effort to achieve the FY 22-23 Plan are expressed in terms of a set of eight Strategic Efforts. They are defined below.

SE01 - Activities for Future Decision Making

Identify and perform priority operational activities and exercises in support of Army 2030 force development that center on future force data-centric decision making and operations. Although activities across the Army enterprise are in scope, activities here are mainly focused on three echelons: theater, aligned corps (MDTF) and divisions as a unit of action. SE01 will identify opportunities to employ data in novel ways against relevant problems. Feedback from users/operators will be captured. Establish and institutionalize a feedback process and mechanism for decisions across DOTMLPF-P. The goal is that lessons learned from the activities provide a robust knowledge base for optimizing data-centric decision making across the DOTMLPF-P.

SE02 - Data Management and Engineering

Provide data management, processes, and data services to support rapid development of data-driven decision capability, to include appointment of data stewards, identification of authoritative and priority data, and mature Identity, Credential, and Access Management (ICAM) solutions. The main focus here is on the data that supports SE01 activity. Factor in echelon data needs and relevant user stories. SE02 will result in data that supports decision making and innovation at speed, achieved through the VAULTIS goals of Army data strategy and managed by a well-defined and mature data governance practice.

SE03 - Architecture

Architect and govern the infrastructure required for supporting critical missions and capabilities such as operations / intelligence (ops/intel) integration. If a new mission thread or capability is identified in SE01, SE03 generates the architecture of how the systems and business activities work together to achieve that outcome. Look for flexible operational and system architectures that are force structure and geographically agnostic to accommodate multi-domain formations and theater specific environments.

SE04 - Unified Network

SE04 provides a Unified Network in support of SE01. The Unified Network (UN) is a weapons system that enables MDO, and aligns multiple, complex network modernization, data, cloud, and convergence efforts into a single coherent approach to support large-scale ground combat operations (LSGCO), Joint All-Domain Command and Control (JADC2), and MDO-capable Army operating with joint/coalition partners. The UN delivers a common suite of hardware and software, employing the principles of zero-trust, through a series of integrated activities encompassing the operating environment, services infrastructure, and the transport layer, and is built to support the convergence of the Army Integrated Tactical Network (ITN) and Integrated Enterprise Network (IEN).

SE05 - Talent

Deploy existing talent, train Army manpower, and hire needed expertise to deliver the right talent at the right locations. SE05 strives to achieve:

- An Army that is data-informed, technologically-enabled, and capable of Multi-Domain Operations supporting global competition and armed conflict
- Increased availability of technical skillsets and the ability to rapidly derive insight from data and field applications across Army formations

SE06 – Scalable Data-driven Decision Support

SE06 seeks to define the decision frameworks, technological requirements, and governance needed to enable self-service, data-driven decision support at echelon in a secure, scalable, repeatable manner. In order to accomplish this we will:

- Define the frameworks that enable operational data consumers to design and implement decision support products
- Establish the requirements to broadly enable secure, scalable, autonomous data sharing
- Develop the requirements for a self-service data platform
- Establish a federated computational governance model

SE07 - Cloud at Echelon

Provide cloud and cloud services at echelon. Cloud is the backbone of the Army's modernization strategy—cloud-enabled, data-driven decisions at the speed of relevance. The effects of SE07 activity include:

- Reduce barriers to entry
- Accelerate data-driven decisions
- Optimize the security accreditation process
- Provide IT asset/cost transparency and accountability

SE08 - Data Protect

Develop enterprise-wide policy and guidance for the Army to specify, when data is aggregated and integrated into operations, how the classification level of data may change and how to further protect its dissemination and use throughout its lifecycle. The term "aggregation" is used here in the sense of associating data describing one set of information to data for a different set of information, e.g. ammunition and location. Doing so can potentially raise the classification level of the aggregation relative to the individual sources.