Project Herald

Defense Intelligence Digital Transformation Campaign Plan

2022–2027

Organization: Department of Defense
Under Secretary of Defense for
Intelligence & Security

Release Date: December 27, 2021

Table of Contents

List of Figures

List of Tables

Foreword

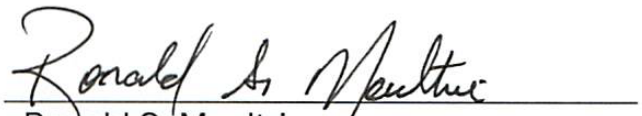
In order to face the challenges posed by great power competition in the digital age, the Defense Intelligence Enterprise (DIE) and Defense Security Enterprise must adapt its mindset and approach by embracing digital transformation. We must lower technological barriers to entry, work more closely with partners, bring artificial intelligence (AI) capabilities at scale, and dynamically create capabilities to support the Joint Force. We must reexamine the value of the legacy systems operating today, avoid vast duplication of effort across the community, and cease to operate where most systems cannot interoperate.

That is why we are embarking on a DIE digital transformation campaign—known as Project Herald—to evolve how the Department of Defense (DoD) delivers intelligence to warfighters while providing the unifying focus to realize next-generation capabilities at the speed of war. Heralds throughout history have signaled significant change on the horizon; Project Herald represents our bold step forward to solidify competitive advantage.

It is time to break free of legacy thought patterns and behaviors. Through process modernization and resource alignment, we can ensure that intelligence personnel and missions can take full advantage of emerging technologies. Beginning immediately with the DIE, we will:

- Adjust our USD(I&S) Charter, DIE responsibilities, and guidance;
- Implement our data-driven oversight of DIE capability execution; and
- Identify resource tradeoffs and investment opportunities to accelerate transformation for Fiscal Year 2024 and beyond.

Project Herald reflects the gravity of mission in front of us and the vital changes that must occur. I am excited to see how far our ingenuity and resourcefulness will take us in delivering remarkable, secure, and flexible capabilities for the next generation of Defense Intelligence.



Ronald S. Moultrie
Under Secretary of Defense for
Intelligence & Security

1.0 Introduction

The DoD must accelerate Digital Transformations to efficiently and effectively share data, information, and intelligence among Military Services, Defense Agencies, and Combatant Commands. Current digital approaches inhibit effective oversight and execution, because solutions typically only exist in individual, mission-specific platforms and programs. For example, the current environment of more than 800 Intelligence, Surveillance, and Reconnaissance (ISR) programs, containing similar systems but unique implementations, causes delays, disorder, and siloed intelligence.

Digital Transformation is not primarily about specific technologies. Digital Transformation means changing our culture and processes using data and technology. We require a set of enabling technology tools in order to change our culture and processes, but technology for its own sake is not our goal.

Our objective is to effect change in three areas:

1. **Speed**: We will adopt, adapt, and overcome. We will increase our digital maneuver capability in order to innovate and adapt within the cycle time of our competitors. The goal is not to provide the speed of specific capabilities in isolation, but to create a culture and process to facilitate rapid integration and deployment of new capabilities in general. We will do this by reducing the time required for the development cycle from testing to operation and shifting the focus to improving survivability and lethality.
2. **Decision Rights**: Centralized execution is slow. We will create an organization and supporting infrastructure to maximize the clear intention and decentralized execution of the smallest, lowest, or least centralized authorities. Where possible, decision rights and other authorities will reside with the organization that performs the actual work. Oversight will be accomplished by clearly communicating intent and minimal possible constraints.
3. **Standards**: Do in common what is commonly done. We will maximize speed and decentralized execution by using standard processes and methodologies for interoperability. We will not reinvent solutions to common problems.

> *The big problems are not technical. In spite of the substantial technical development needed in requirements setting, metrics and measures, tools, etc., the Task Force is convinced that today's major problems with military software development are not technical problems, but management problems.*
>
> *- Report of the Defense Science Board Task Force on Military Software, 1987*

The Defense Intelligence Digital Transformation Campaign Plan, also known as Project Herald, will enhance battlespace awareness (BA) execution by transforming common defense intelligence and intelligence-related capabilities into enterprise services, including, where appropriate, a greater alignment with non-DoD Intelligence Community (IC) activities. It will also outline the steps by which Military Services, Agencies, and Combatant Commands can use these enterprise services to build mission-specific BA capabilities in a rapid and normalized manner. We will become a modern enterprise, providing valuable insights across intelligence disciplines at faster speeds and superior digital maneuvers.

1.1 STRUCTURE AND OVERSIGHT

DIE services will be grouped as follows:

- **Digital Foundation** – Includes services that comprise the digital substructure that enables rapid deployment, scaling, testing, and optimization of intelligence software as an enduring capability. This entails leveraging Intelligence Community Information Technology Enterprise (IC ITE), DoD Chief Information Office (CIO) offerings, and other enterprise-level providers to deliver a centrally orchestrated environment to include state-of-the-art cybersecurity controls.
- **Intelligence-Focused Product Lines** – Includes functions common to the DIE that support the consumption of intelligence as user-facing services and products (e.g., collection orchestration, common intel picture, motion GEOINT exploitation, and intelligence mission data, etc.). Successful delivery of intelligence-focused product lines will be characterized by product-line/block funding, enterprise scope, agile requirements, modern technical interfaces, and instrumented assessment tools.

DIE services will have a designated enterprise manager who will:

- Define, deliver, and/or orchestrate the enterprise service for the DIE.
- Maintain knowledge of the totality of resources and resource needs across the DIE.
- Capture and champion community requirements.
- Establish and direct training and certification, tradecraft, policies, and processes, where appropriate.
- Recommend technical architectures and standards, evaluation criteria, and performance goals to enable efficient interoperability and effective alignment of DIE capabilities with DoD, IC, allies, and partners.
- Monitor compliance with relevant standards and guidance.
- Provide formal recommendations to relevant Military Intelligence Program (MIP) Component Managers across the Planning, Programming, Budgeting, and Execution (PPBE) process and the Under Secretary of Defense for Intelligence and Security (USD[I&S]) as a MIP Executive, to ensure cohesive enterprise activities. Also provide USD(I&S), in the dual hat role as Director of Defense Intelligence, input on related National Intelligence Program (NIP) and BA portfolio resources. Specifically:
  - Assess and recommend to USD(I&S) additions or deletions of programs, functions, and activities to and from respective MIP program lines.
  - When relevant, propose modifications to NIP or BA portfolio resources for USD(I&S) consideration and, if required, in consultation with DNI.
  - Report to USD(I&S) on performance and compliance across the activity, to include expenditure of resources.
  - Use reprogramming activity throughout the established governance process to ensure enterprise effectiveness.

1.2 CAMPAIGN CONTEXT

Project Herald is a part of a broader effort within the DoD to modernize and transform digital infrastructure. It aligns with the Defense Intelligence Strategy, which draws on the National Defense Strategy, and is derived from the National Security Strategy. The DoD Digital Modernization Strategy, the Defense Innovation Board Software Acquisition and Practices (SWAP) Study, the National Security Commission on Artificial Intelligence (NSCAI) report to Congress, the Future of Defense Task Force report, and the DoD AI Training and Education Strategy further inform it. This campaign incorporates lessons learned from the execution of the Joint Architecture Reference Model (JARM), execution of the Joint Requirements Oversight Council (JROC) validated Combatant Command Intelligence Information System Initial Capability Document, the execution of Services of Common Concern under the IC ITE Strategy, and the execution of capability releases under the Air Force's Advanced Battle Management System (ABMS). It also incorporates transformation approaches and adoption across commercial industry and the OUSD(I&S) ISR Architecture Convergence Study.

Project Herald details the transformation goals shown in Figure 1.

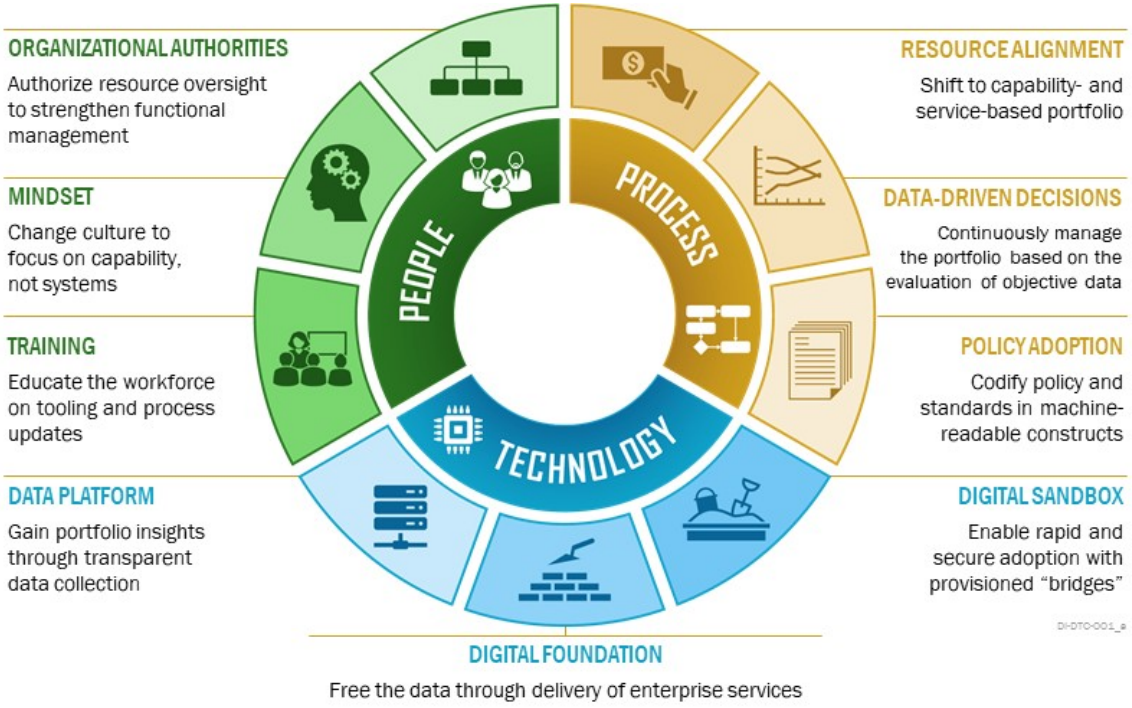


Figure 1: Transformation Goals

This document provides recommendations for OUSD(I&S) to effectively monitor the path to a resilient, secure, and scalable array of services, platforms, and products. The portfolio focuses on enterprise-level services, and facilitates organization-specific solutions where appropriate, in order to enable best-of-breed intelligence and BA capabilities. This plan will enable fast, relevant, and tailored solutions to be rapidly built in a decentralized fashion. Project Herald aligns with the intent of Department-level data, technology, labor, and

procurement strategy. It addresses the modernization needs of the Department, the community's common challenges, and facilitates faster and more efficient fielding of innovative capabilities to the battlefield of the future.

2.0 Overview of Current and Future State Environments

Project Herald focuses on transforming the DIE from a projects- and systems-focused portfolio of programs to a capability portfolio of digital products and services.

2.1 CURRENT ISR ENVIRONMENT

Due to mission-specific platforms, programs, processes, and funding profiles, the current DoD ISR environment is ineffective in sharing data and information across the Military Services, Agencies, and Combatant Commands. The DIE portfolio[1] is structured around the use of traditional project management incentives, patterns, and processes. DIE Program Elements are systems-centric, and their outputs provide organizations with discrete systems to achieve their traditional, specific, intelligence function. Many components of these systems execute the same function across Program Elements and bureaucratic processes actively discourage data sharing between them.

Capability delivery is slow to adjust due to milestone decision points that occur infrequently, roughly every 6 to 12 months. Traditional project management, focus on cost, schedule, and performance, with long cycle times, is not an effective environment for Digital Transformation.

Today, there are at least nine different end-to-end systems across the DIE that provide functions to execute Full-Motion Video (FMV) exploitation. These are all uniquely programmed and designed to serve different FMV exploiters. However, the disparity between these systems provides training challenges for analysts, limit the integration of advanced capabilities, and fail to provide the end-consumer with materially unique capabilities. This results in significant duplication of maintenance efforts and does not provide organizations unique value-added capability that might be incorporated into an FMV workflow.

2.1.1 Current Challenges

In addition to previously referenced studies and guidance, recent Combatant Command Integrated Priority Lists and the Joint Chiefs of Staff (JCS) rehearsal of concept (ROC) drills document the loss of our competitive edge in ISR and identify the following operational shortcomings:

- Inability to dynamically employ ISR to support the force: Adjusting needs across geographically diverse areas requires re-engineering at the edge because current platforms lack agility.
- Inability to meet the speed of battle: If the data can be shared, it takes weeks or months to analyze the data provided.
- Inability to work with allies and partners rapidly at scale: Allies and partners are forced to integrate ad hoc and point-to-point instead of through a common network.
- Inefficient manual processes: Current processes create timelines that take years to field capabilities. Proposed innovation efforts, (e.g., Quick Reaction Capabilities (QRCs), prototypes, and pilots) are rarely transitioned to full operations.

Digital Transformation should address the root causes of these challenges and set the path for a future flexible enterprise that can support dynamically changing threat environment.

[1] The DIE portfolio is all intelligence and intelligence-related program elements within the DoD, which is composed of Military Departments, Defense Intelligence Agencies, and Combatant Commands.

2.1.2 Symptoms and Root Causes

Many process challenges exist in the current environment. These challenges force users to develop their own localized and short-term solutions. In addition, funding is dispersed through Program Elements that compete for funds to grow and sustain their mission capabilities. This discrete and zero-sum environment creates a portfolio that is fragmented and incomplete.

These process challenges are symptoms of the underlying root causes limiting the DIE as shown in Figure 2.

Figure 2: Root Causes and Symptoms of Current DIE Limitations

2.1.2.1 Culture

The culture within the DIE is often risk-averse. To enable effective decision making throughout the organizational hierarchy, DIE corporate decisionmakers must transition to decisions driven by continuous operational and programmatic data of sufficient quality. Being too slow is our existential risk.

The organic technology expertise, training, partnerships, and cultural shifts needed for solution delivery are not present and too many authorities are held at too high of a level. This issue leads to poorly defined requirements and a limited ability for decisionmakers to rapidly evaluate, build, and field advanced technology systems and programs.

2.1.2.2 Structure

The current structure in the DoD's BA portfolio does not encourage a digital enterprise management approach. Defense Intelligence is structurally aligned within two disciplines: capability delivery and capability oversight.

- Capability delivery is currently aligned with the missions of the Military Services and Defense Intelligence Agencies.

  Operating domains:
  - Space
  - Air
  - Ground
  - Maritime
  - Littoral
  - Cyber Space

  Combat Support Agencies' intelligence disciplines:
  - Geospatial Intelligence (GEOINT)
  - Signals Intelligence (SIGINT)
  - Human Intelligence (HUMINT)
  - Measurement and Signature Intelligence (MASINT)
  - Open Source Intelligence (OSINT)

- Capability oversight is nominally assigned to functional managers. In practice, most functional managers lack the requisite authority and ability to influence data standards, engineering solutions, or resourcing decisions needed to align their functional areas in support of enterprise-wide improvements. There must be structural changes to ensure

functional and enterprise managers have the authorities that allow the DIE to prioritize, incentivize, and adjust for enterprise-level capability and alignment.

2.1.2.3 Programmatic Approach

The vast majority of Program Elements in the DIE are built around end-to-end systems. This approach does not allow for funding, large-scale activation of mission partners, or the use of enterprise services to adjust the capabilities of individual components, except through in-depth program review meetings and laborious data calls.

The DIE approach to programming capabilities must be updated to align with modern technology delivery methods and DoD goals on Capability Portfolio Management by changing the Program Element structure to a rationalized portfolio of capabilities. Modernization within the existing program structures will only deepen current problems in newer technology environments.

2.1.3 Risk of Doing Nothing

Maintaining the current ISR environment and methods forces the DoD to make incremental adjustments to systems created by the previous generation for a world that no longer exists. This will result in:

- **Disjointed Intelligence** - Warfighters receive disjointed data, which can lead to a decline in analytic judgment.
- **Incomplete Threat Pictures** - The DIE is unable to use existing communication infrastructure and processes to effectively transmit the large amounts of data collected.
- **Slow Delivery** - A fragmented environment can lead to inefficient and incomplete network communications, manual processes for repairing data, and inefficiency in disseminating analysis results to warfighters.
- **Outdated Technology** - The DIE is unable to adopt and integrate standard technologies such as cloud computing and machine learning at a relevant scale.
- **Lost Opportunity Cost** - An end-to-end system acquisition model wastes resources on repetitive core functions and infrastructure, thereby reducing the resources available for new and unique capabilities and functions.
- **Continued Deference to Outmoded Policy** - The DIE is unable to advance modern solutions due to restrictions of outdated policy.

2.2 FUTURE-STATE ENVIRONMENT

Future-state environment means a portfolio approach focused on outcomes, not outputs. It means the continuous delivery of value and improved capabilities to analysts and warfighters. Managing a portfolio of products and services means changing the mindset from systems to capability areas. These are not the existing Joint Capability Areas (JCA). Instead, they are capability areas defined by how modern technology is delivered to and consumed by analysts and warfighters.

The Future-state environment focuses on addressing current challenges in culture, structure, and programmatic approach. To achieve success, the DIE must address the root cause limitations.

- **Culture:** The culture will evolve into a data-centric and innovation-driven community adept at independent and decentralized execution.
- **Structure:** The current capability delivery structure is based on Service and Agency domain responsibility, and will be enhanced by establishing authorities aligned with a new portfolio.
- **Programmatic Approach:** Within the new portfolio construct, the oversight functions and levers to address operational and fiscal priorities will become processes that enable continuous assessment and adjustment within a capabilities-based structure.

Because the focus will change from output to outcome, the assessment criteria also will change from cost and schedule to mission benefits. Customer feedback will determine success or failure. Block funding of products and services will be allocated based on prioritization of the capability and the outcome the product or service provides. Funding in these blocks will directly support the enterprise at large, to include our ability to operate with mission partners, and be more flexible to enhance and quickly change the technologies in the product line or service category, as shown in Figure 3. Product and service-based Capability Portfolio Management will increase delivery speed. It will also provide more flexibility in addressing operational priorities.

Lastly, it will allow capability delivery to be continually and easily adjusted, instead of adjusted only once per year through individual and hard-fought re-programming actions.

In the Future, a single Motion GEOINT Exploitation Product line is available enterprise-wide that: Enables best-of-breed Motion GEOINT exploitation techniques and tools for use by the entire community. Ensures compliance with the functional manager's standards for data marking, data quality, data storage, production tradecraft, and Structure Observation Management (SOM) creation. Ensures data is postured for maximum AI/ML exploitation in shared repositories, which should include track data repositories. Allows scale by prioritizing open-source software, or at least enterprise licensing for commercial products. Enables individual organizations to focus on value-added capabilities (e.g., Naval forces developing littoral detection algorithms).

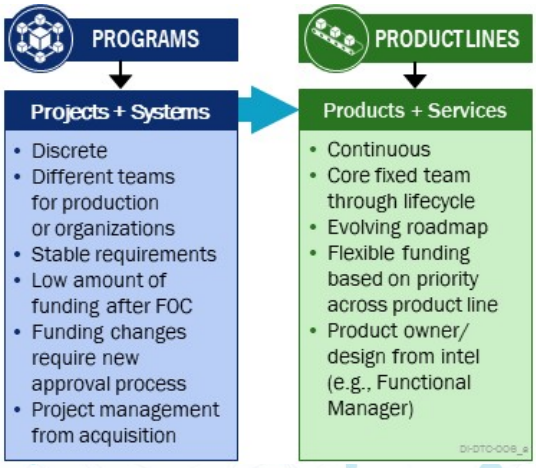


Figure 3: Project/Systems-Focused Portfolio Approach versus Product/Services Portfolio Approach

The utility of these changes in Culture, Structure, and Programmatic approach will be judged based upon the ability of future DIE to demonstrably mitigate the risks outlined in the section titled, “Risk of Doing Nothing” (section 2.1.3), and to deliver the impacts cited in the “Impacts” (section 3.4).

2.3 ENTERPRISE PRINCIPLES

These principles identify the key considerations that are essential to the execution of a Digital Transformation. The key enterprise principles are as follows:

- **People and Talent Matter** - Highly trained personnel, who understand the latest technologies, how to effectively deploy them, and who are incorporated into the decision-making process at all levels, are vital for success.
- **Incentivization** - Culture must shift from a compliance methodology to an approach that enables rapid innovation, reuse of common components, and greater multi-domain and joint interoperability. Funding must be designed and adjusted to reward good enterprise behavior and defund bad enterprise behavior.
- **Baseline Core Enterprise Capabilities** - Core enterprise capabilities should have dedicated funding and, where practicable, any mission-specific enhancement requests should be denied.
- **Agility** - Agility in programming, prioritization, and assessment is just as important as agility in technology development. Lessons learned, technology, and approaches must be continually updated to keep pace with commercial technology and practices. The enterprise must have the agility to adapt to a dynamically changing threat environment.
- **Engage in the Digital Revolution** - Embracing the digital revolution requires a workforce that prepares the DIE for the emerging capabilities shaped by the digital revolution, while providing much-needed incentives and exceptional training for the existing workforce.
- **Do in Common What is Commonly Done -** Identifying common capabilities to serve as enterprise services and platforms that can be widely used and scaled up or down as needed.

3.0 Proposed Digital Transformation

Project Herald will change the way the DoD operates and delivers intelligence to warfighters by setting conditions for intelligence missions to take full advantage of emerging technologies. As shown in Figure 4, the approach to setting new conditions will focus on achieving nine transformation goals in three key areas: People Process, and Technology.

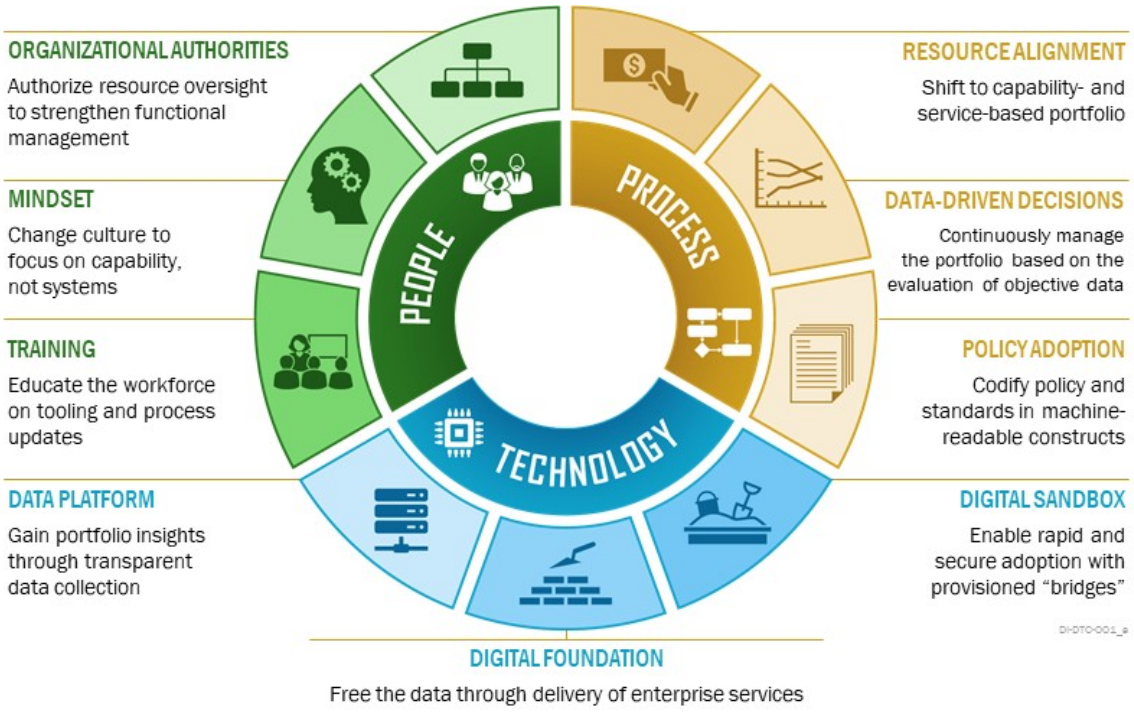


Figure 4: Transformation Goals

3.1 PEOPLE

People refers to all aspects of personnel management focused on OUSD(I&S) employees and assigned DIE authorities and roles, including appropriate training for leaders at all levels. Organizational Authorities, Mindset, and Training are critical for ensuring that the DIE is well managed.

3.1.1 Organizational Authorities

USD(I&S), utilizing the authorities described in DoDD 5143.01, will provide guidance, direction, and oversight of the Defense Intelligence Digital Transformation Enterprise managers. These managers will be established to oversee the

processes that govern the enterprise, ensure that properly qualified people are assigned to the appropriate positions, oversee the design of the Future-state environment, drive deliberate mission partner supported interfaces, and ensure that any issues occurring between enterprise services are properly addressed. Enterprise management of intelligence-focused product lines (e.g., Joint Targeting Intelligence and Collection Orchestration) will also be established and codified to ensure that cross-organizational capabilities are considered. Other roles that will be identified, delineated, and authorized include:

- Data & Analytics
- Assessment
- Enterprise Cybersecurity

3.1.2 Mindset

Intelligence analysts and operators are digital natives who are poised to leverage modern technology. In addition to publishing the guidance, we need to convert the rest of the community to a digitally transformed mindset. Finding people who are proficient in modern technology will be a key task for leaders in this effort. To ensure a fast and continuous flow of talented personnel into our organization, we will:

- Incentivize High Value Employees, limited tenure hires in the DoD/DIE/IC by reducing barriers to entry, providing salaries competitive to the private sector, and advertising openings and hiring events side-by-side with the private sector.
- Pursue opportunities, initiatives to hire, and onboard new staff who work fully remotely, as has already been done by Defense Digital Services, Kessel Run, and Platform One.
- Leverage the full benefits of IC Login to enable remote staff to work from existing Sensitive Compartmented Information Facilities (SCIFs) close to their location in the event staff must partially work in a classified setting.
- Seek new hiring pathways using private sector platforms and eliminating onerous and ineffective requirements like government-style resumes. as pioneered by the U.S. Digital Service and Defense Digital Service.
- Expedite clearance access processes for industry allies and partners.
- Remove coding from billets to the maximum extent practicable. Billets will be filled based on skills and competence, not rank or previous position designations.

3.1.3 Training

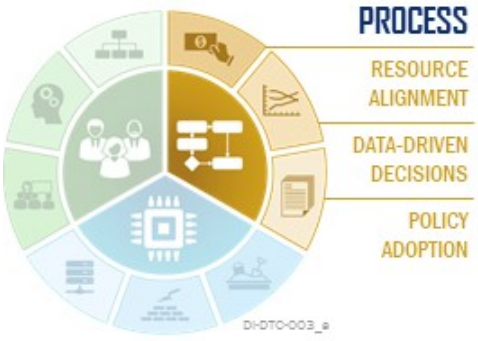
Training ensures the development of skills to lead, design, build, and deploy effective capabilities. We will improve the ability of staff to rotate with private sector companies. We will also promote the use of existing training channels and options in other areas of the DoD, and where feasible, look for opportunities to:

- Establish Digital Foundation Executive Leadership training workshops.
- Enable training to support utilization of emerging technologies delivered by the Digital Foundation.

- Encourage professional certifications (e.g., professional engineering certifications) and establish Education with Industry (EWI) opportunities to align government and commercial standards and incentives.

3.2 PROCESS

The processes used to govern and manage the enterprise have played an important role in the success of this transformation. Efficient processes are needed to define a governance structure and to provide mechanisms to incorporate feedback from the community.



3.2.1 Resource Alignment

Resource Alignment is a necessary component for achieving capability-level solutions. Intelligence-focused product lines and mission-unique capabilities should be built, where practicable, on top of common Digital Foundation services. This must be supported by incentives and policies that promote sharing and the adoption of community standards and enterprise services. Resource Alignment will focus on:

- Restructuring the DIE Portfolio into a products/services-based portfolio of capability areas including Digital Foundation, intelligence-focused product lines, and mission-specific capabilities.
- Divesting from legacy systems, technologies, and programs.
- Establishing a competitive funding program that supports innovative solutions.
- Piloting Mission Capability Threads as intelligence-focused product lines.

3.2.2 Data-Driven Decisions

Accurate and appropriate up-to-date data must be used to make decisions about plans and capabilities. The historical method of distributing programmatic data in slides, spreadsheets, and e-mails is not enough. To support decision rights up and down the chain, we must adopt tools to avoid manual-intensive data calls and focus on providing automated data for the entire enterprise's cost, schedule, and performance indicators. Many tools exist that facilitate tracking and decision making. We will leverage the tools that are currently used, rather than force adoption elsewhere. Beyond support to Department-wide executive analytics, the goal of a data-driven approach will be to:

- Provide continual oversight, assessment, and adjustment of the Digital Foundation and intelligence-focused product lines.
- Enable value-added, mission-unique capabilities to make rapid reprioritizations, thereby encouraging development of fast and attributable solutions over exquisite solutions.

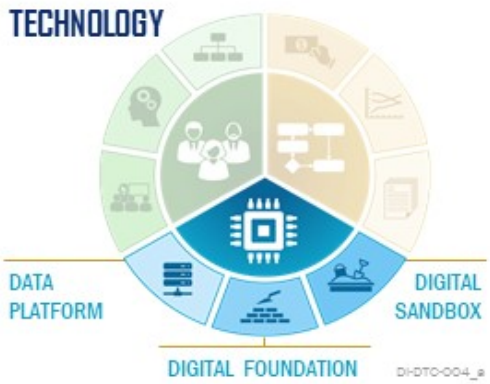
3.2.3 Policy Adoption

Digital Transformation will require centralized policy changes to enable improvements to all areas of the enterprise. These policy changes will seek to reduce variations caused by organizational interpretations, thus enabling innovation and experimentation by mitigating acknowledged policy barriers. When combined with funded implementation methods where feasible, these new policies will reduce the number of unfunded mandates that are pushed to the programs. They should also support streamlined processes from analysis to model creation to meet "anticipatory intelligence" timelines. Some examples we will pursue include:

- Modernizing data sharing policies and associated technical rulesets (e.g., metadata tagging) to enable timely automated sharing to those with the appropriate credentials.
- Revising workplace requirements and classification policies to increase remote staff.
- Implementing DoD Chief Data Officer (CDO) policy to maximize automated, secure, persistent sharing, understanding, and access to the data. Implementing DoD Chief Information Officer (CIO) policy for reciprocity in granting an Authority to Operate (ATO) in order to maximize reuse of ATOs across the enterprise.
- Aggressively re-evaluating Security Classification and Foreign Disclosure Guidance to ensure that as much work as possible can be done at the lowest classification level; shared as widely as possible; and implemented in machine-readable formats. This includes disseminating DoD CIO guidance to increase the flexibility of ATO processes and improving ATO for cross-organizational services.

3.3 TECHNOLOGY

Achieving mission objectives, supporting end-users, and meeting future needs require access to data, tools, services, and environments to support deployment/theatre technology. The provision of technology and innovative solutions and the development of skills and expertise are critical to the success and execution of Digital Foundation deployments. Where practicable, we will:



- Use approved open-source software and tooling.
- Use IC & DoD enterprise services including cloud and on-premises infrastructure contracts and environments, with a preference for cloud infrastructure solutions.
- Enable reuse of government-owned capabilities such as government reference architectures (GRA), government-owned waveforms, multi-caveated software engineering labs, and government-owned testbeds.
- Develop technology consistent with Zero Trust Architecture principles.

3.3.1 Data Platform

The Data Platform directly supports databased decision making by storing and visualizing complete and accurate information obtained from automated and transparent data collection from the capabilities throughout the DIE. This data will be collected and aggregated in numerous ways, including:

- Structured event data from DIE applications.
- Application Programming Interfaces (APIs) from workflow tracking systems (e.g., Atlassian Jira).
- APIs from other business intelligence or data warehousing systems.

Non-application-specific data will be stored on this centralized data platform to the extent feasible. The platform must be vendor agnostic and support data analysis with standard tools and leverage open-source software to the maximum extent practicable.

3.3.2 Digital Foundation

A secure, agile, and robust Digital Foundation that draws on enterprise principles from industry and government best practices is required to meet current DIE needs and adapt to future warfighting scenarios. A Digital Foundation enables innovation through broad access to common services, tools, data, and resources. A Digital Foundation will begin with the following:

- A self-service portal.
- An enterprise data broker.
- A team collaboration and knowledge management system.
- An issue tracking and workflow management system.
- Git-based version control capability.
- An integrated developer environment.
- A build tool.
- An alerting, messaging, and notification service.
- An identity management service.
- A user and system attribute management service.
- Modernized data transport services.

The Digital Foundation will scale over time as additional services and tools are designated for enterprise provisioning, such as those recommended in the ISR Architecture Convergence Study as shown in Figure 5.

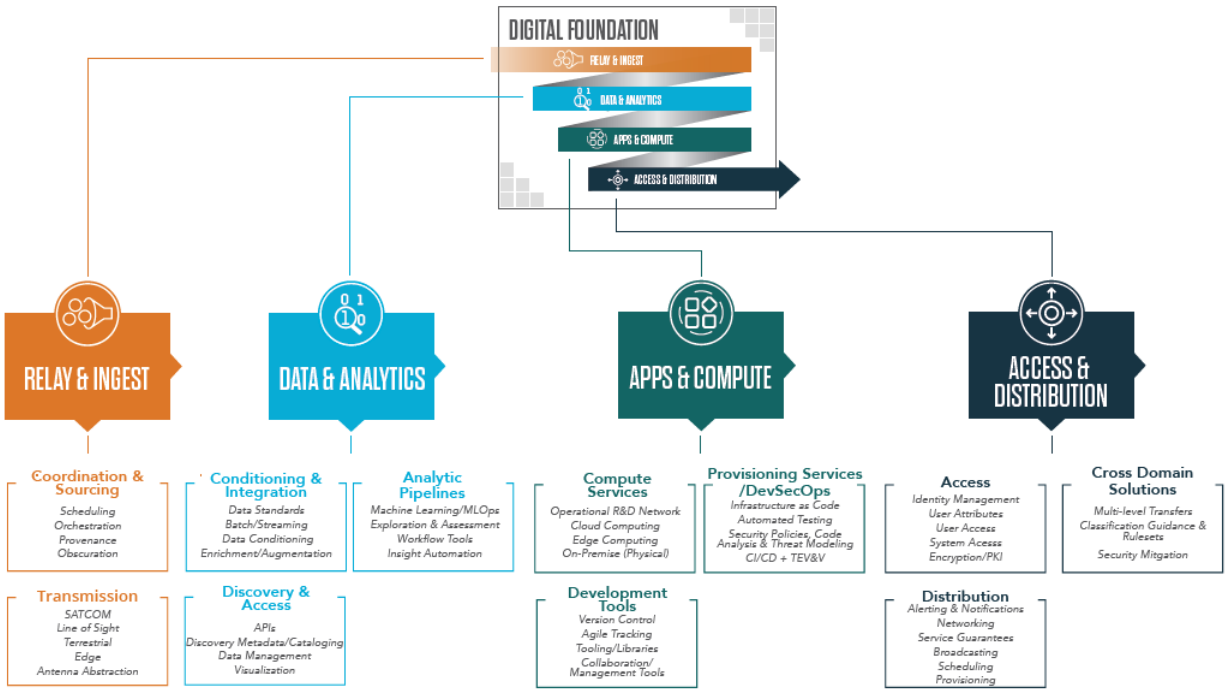


Figure 5: Components of Digital Foundation
Recommendations from ISR Architecture Convergence Study

3.3.3 Digital Sandbox

The Digital Sandbox is a part of the technology platform that allows rapid and secure integration of intelligence capabilities, provisioning, and continuous accreditation into operational environments. This will eventually lead to continuous rapid innovation and contributions to the enterprise by users outside the historical program lanes. Although the Digital Sandbox is a place to test and prototype new technologies, technologists will also have access to the same tooling, provisioning services, DevSecOps pipelines, and, to the extent practicable, the same data that exists in a production environment. In addition to provisioning this persistent Digital Sandbox, we will support innovation by:

- Hosting quarterly innovation events.
- Building Combat Coder and Enterprise Services Strike Teams.
- Defining baseline characteristics for the Digital Sandbox environment and innovation efforts.

3.4 IMPACT

A focused transformation across People, Process, and Technology areas will enable us to deal with the most severe challenges from different perspectives. By combining efforts across the campaign, we see how these create "supporting fires" to tackle specific challenges. (Refer to Section 2.1.1.)

Challenge #1: Current processes create timelines that take years to field capabilities.

Transformed Approach: To get innovative solutions over the valley of death, we host innovation events at least quarterly in the Digital Sandbox to focus community innovation toward identified and prioritized gaps. These events will leverage provisioned tools, services, and embedded security approvals from the Digital Foundation and include events that leverage commercial industry, research labs, and academia, industry partnerships (Defense Innovation Unit [DIU], Team of Air Force Innovation [AFWERX], etc.), Federally Funded Research and Development Centers (FFRDCs) and University Affiliated Research Centers (UARCs), combat coders, and traditional program engineers. These events can be paired with a competitive funding program in Resource Alignment in order to bridge small successful capabilities for a few years until they can be deliberately programmed for, transitioned to an established product line, or are overcome by other solutions.

Challenge #2: Adjusting needs across geographically diverse areas requires re-engineering at the edge due to the lack of agility of the current platforms.

Transformed Approach: To attain a flexible enterprise ready to support the full range of military operations globally, we will enable sensors and platforms to connect to the Digital Foundation and leverage common interfaces, tools, and services that can be tailored to support any theater through either CONUS-based reachback or edge deployed. The Digital Foundation and associated mission workflows will be instrumented to provide real-time metrics via the Data Platform that will be used to support Data-Driven Decisions on reallocation, reapportionment, and reprioritization of intelligence capabilities and resources.

Challenge #3: If the data can be shared, it takes weeks or months to analyze the data provided. Increasing amounts of data from both open and government sources will demand a need to automate exploitation methods for analytic production.

Transformed Approach: To speed access to data for analysis, we will update the data policies to support automated mechanisms including data tagging and brokering services, as well as analytic and machine learning pipelines, in the Digital Foundation. We will also empower functional managers to own intelligence-focused product lines that will use those automated mechanisms to share data and derived observations at speed and scale.

Challenge #4: Allies and partners are forced to integrate ad hoc and point-to-point instead of through a common network.

Transformed Approach: When shifting our mindset away from end-to-end architectures that support specific sensor and platform capabilities, we must also apply this to allies and partners. When deploying enterprise-level services, those product owners will be responsible for managing the interfaces that support allies and partners. We will enable the ingestion of partner collection through Relay and Ingest services. We will fund activities to collaborate in the data and analytics and allow allies and partners to leverage provisioned services. Finally, we will normalize partner access through network connectivity as we move toward a Zero Trust Architecture in the Digital Foundation. These product owners will inform allies and partners of specific APIs, data links, data formats, and other requirements needed to interoperate with the enterprise services.

4.0 A Way Ahead for Implementation

Digital Transformation in the DIE is a continuous process. It will require collaboration and coordination with all Military Services, Defense Agencies, Combatant Commands, and Interagency Partners. The implementation of this strategy, and specifically the restructuring of our internal OUSD(I&S) processes over the next five years, will be led by the Project Herald Working Group.

4.1 PROJECT HERALD WORKING GROUP

The Project Herald Working Group will detail the steps required to identify, resource, and authorize enterprise-level services, reduce bureaucratic and overly burdensome processes, collaborate with allies and partners, and create capabilities to use ISR in support of the Joint Force. The Project Herald Working Group will be established within 30 days of approval and release of this document. Figure 6 outlines the structure and members of the Project Herald Working Group.

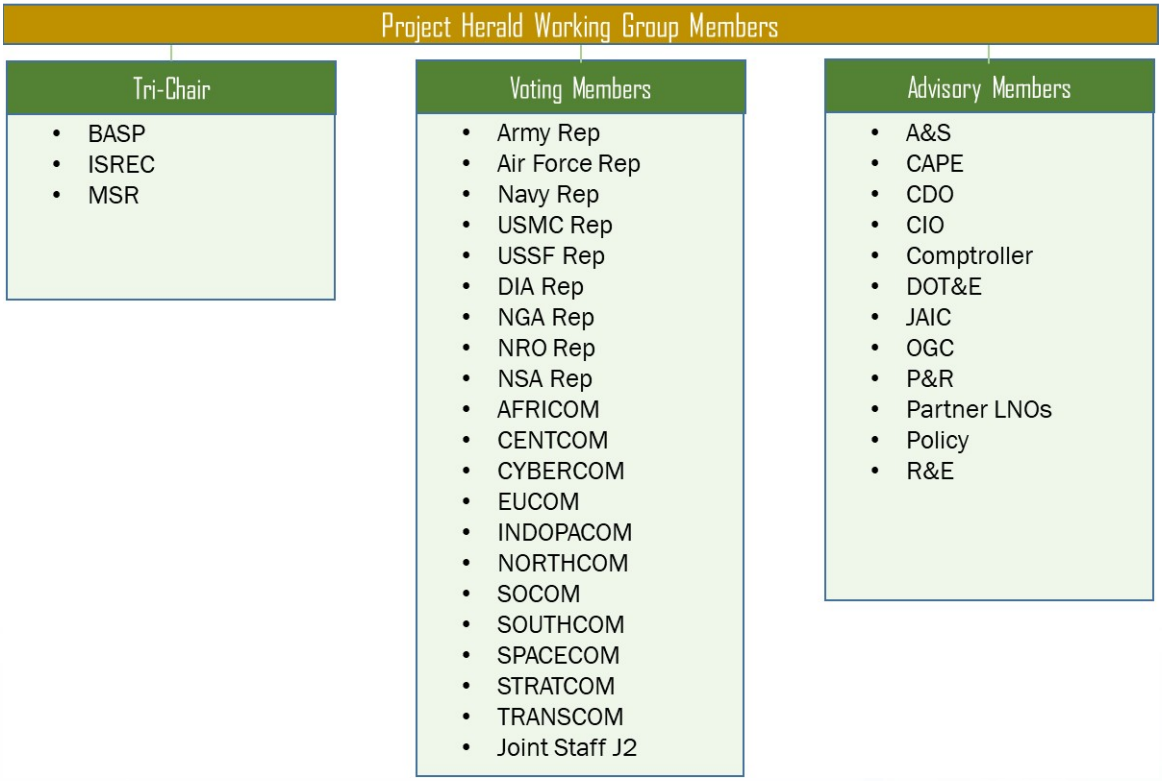


Figure 6: Project Herald Working Group Members

4.1.1 Roles and Responsibilities

The key responsibilities of the Project Herald Working Group are as follows:

- Execute capability portfolio mapping to better enable enterprise behavior.
  - Scope and define capability areas including enterprise services and mission-unique capabilities.
- Map current programs, systems, and efforts to capability areas.
- Support capability portfolio management.
  - Identify and assess existing programs for potential enterprise services.
  - Develop courses of action (COAs) for enterprise manager designations and resourcing strategy.
  - Establish criteria for execution assessment to support objective metrics collection per capability area.
- Make recommendations to appropriate governing bodies as required.

4.1.2 Recommendations - Phased Implementation

Recommendations from the Working Group will be integrated into USD(I&S) owned DoD Directives and Instructions, as well as other USD(I&S) policy updates; Fiscal and Functional annual guidance to the DIE Components; and a Technical Service Delivery Roadmap. The structure of all recommendations and guidelines will support a phased implementation to provide Initial Services, Core Services, and Enhanced Services, as shown in Figure 7.

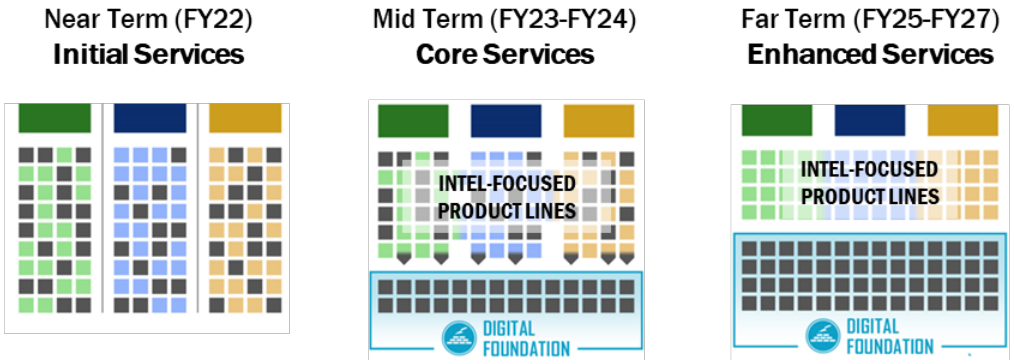


Figure 7: Recommendations - Phased Implementation

The DIE's Digital Transformation will allow us to meet the speed of battle. We will reduce the burden on the combat personnel, staff, and programs. We will improve the access, discovery, and quality of intelligence information. Through these outcomes, our Digital Transformation will increase the overall mission value of the DIE.

This strategy supersedes, updates, and replaces any previous guidance on the modernization of Defense Intelligence capabilities.

Appendix A. Glossary of Abbreviations and Acronyms

The following abbreviations and acronyms are used within this document.

Acronym	Definition
A&S	Office of the Under Secretary of Defense for Acquisition & Sustainment
ABMS	Advanced Battle Management System
AFRICOM	U.S. Africa Command
AFWERX	Team of Air Force Innovation
AI	Artificial Intelligence
ATO	Authority to Operate
API	Application Programming Interface
BA	Battlespace Awareness
BASP	Battlespace Awareness & Security Programs
CAPE	Office of Cost Assessment and Program Evaluation
CDO	DoD Chief Data Officer
CENTCOM	U.S. Central Command
CIO	DoD Chief Information Officer
COA	Course of Action
CSA	Combat Support Agencies
CYBERCOM	U.S. Cyber Command
DIA	Defense Intelligence Agency
DIE	Defense Intelligence Enterprise
DIU	Defense Innovation Unit
DoD	U.S. Department of Defense
DOT&E	Director, Operational Test & Evaluation
EUCOM	U.S. European Command
EWI	Education with Industry
FFRDC	Federally Funded Research and Development Center
FMV	Full-Motion Video
GEOINT	Geospatial Intelligence
GRA	Government Reference Architectures
HUMINT	Human Intelligence
IC	Intelligence Community
IC ITE	Intelligence Community Information Technology Enterprise
INDOPACOM	U.S. Indo-Pacific Command
ISR	Intelligence, Surveillance, and Reconnaissance
ISREC	Intelligence Surveillance and Reconnaissance Enterprise Capabilities
IT	Information Technology
JAIC	Joint Artificial Intelligence Center
JARM	Joint Architecture Reference Model
JCA	Joint Capability Areas
JCS	Joint Chiefs of Staff
Joint Staff J2	Joint Staff Intelligence Directorate
JROC	Joint Requirements Oversight Council

Acronym	Definition
LNO	Liaison Officer
MASINT	Measurement and Signature Intelligence
MIP	Military Intelligence Program
MSR	Military Intelligence Programs & Security Resources
NGA	National Geospatial-Intelligence Agency
NIP	National Intelligence Program
NORTHCOM	U.S. Northern Command
NRO	National Reconnaissance Office
NSA	National Security Agency
NSCAI	National Security Commission on Artificial Intelligence
OGC	Office of General Counsel
OSINT	Open Source Intelligence
OUSD(I&S)	Office of the Under Secretary of Defense for Intelligence and Security
P&R	Personnel & Readiness
PPBE	Planning, Programming, Budgeting, and Executing
QRC	Quick Reaction Capability
R&E	Office of the Under Secretary of Defense for Research and Engineering
ROC	Rehearsal of Concepts
SCIF	Sensitive Compartmented Information Facility
SIGINT	Signals Intelligence
SOCOM	U.S. Special Operations Command
SOM	Structure Observation Management
SOUTHCOM	U.S. Southern Command
SPACECOM	U.S. Space Command
STRATCOM	U.S. Strategic Command
SWAP	Software Acquisition and Practices
TRANSCOM	U.S. Transportation Command
UARC	University Affiliated Research Center
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USMC	U.S. Marine Corps
USSF	U.S. Space Force

Appendix B. Referenced Documents

The following is a list of referenced documents.

Table 1: Referenced Documents

Title	Date Signed
Defense Intelligence Strategy	11/2020
DoD Digital Modernization Strategy	07/2019
National Defense Strategy	12/2018
National Security Strategy	12/2017
Interim National Security Strategic Guidance	03/2021
OUSD(I&S) ISR Architecture Convergence Study	09/2020
Report of the Defense Science Board Task Force on Military Software	09/1987