



Operational Data Sharing Capability

Report to Congress
March 12, 2025



U.S. Coast Guard

Foreword

March 12, 2025

I am pleased to present the “Operational Data Sharing Capability,” report prepared by the U.S. Coast Guard, U.S. Customs and Border Protection, and U.S. Immigrations and Customs Enforcement.

The Don Young Coast Guard Authorization Act of 2022 directs the submission of a report on the establishment of centralized capability to allow information sharing between U.S. Customs and Border Protection and the Coast Guard for purposes of maritime boundary domain awareness and enforcement activities along the maritime boundaries of the United States. Due to their authorities and responsibilities in the maritime domain, U.S. Immigrations and Customs Enforcement’s Homeland Security Investigations joined this initiative.



Pursuant to Congressional requirements, this report is provided to the following members of Congress:

The Honorable Ted Cruz
Chairman, Senate Committee on
Commerce, Science, and Transportation

The Honorable Rand Paul
Chairman, Senate Committee on
Homeland Security and Governmental
Affairs

The Honorable Sam Graves
Chairman, House Committee on
Transportation and Infrastructure

The Honorable Mark E. Green
Chairman, House Committee on
Homeland Security

The Honorable Maria Cantwell
Ranking Member, Senate Committee on
Commerce, Science, and Transportation

The Honorable Gary C. Peters
Ranking Member, Senate Committee on
Homeland Security and Governmental
Affairs

The Honorable Rick Larsen
Ranking Member, House Committee on
Transportation and Infrastructure.

The Honorable Bennie G. Thompson
Ranking Member, House Committee on
Homeland Security

Should you require additional assistance, please do not hesitate to contact my Senate Liaison Office at (202) 224-2913 or House Liaison Office at (202) 225-4775.

Sincerely,

A handwritten signature in blue ink, appearing to read "Kevin E. Lunday".

Kevin E. Lunday
Admiral, U.S. Coast Guard
Acting Commandant



Operational Data Sharing Capability

Table of Contents

I.	Legislative Language	1
II.	Background	2
III.	Report	4
IV.	Conclusion.....	6
	Appendix: Abbreviations	7

I. Legislative Language

This report responds to the language set forth in Section 11264(e) of the Don Young Coast Guard Authorization Act of 2022 (Pub. L. No. 117-263), which reads:

SEC. 11264. OPERATIONAL DATA SHARING CAPABILITY.

(a) **IN GENERAL.**—Not later than 18 months after the date of enactment of this Act, the Secretary shall, consistent with the ongoing Integrated Multi-Domain Enterprise joint effort by the DHS and the Department of Defense, establish a secure, centralized capability to allow real-time, or near real-time, data and information sharing between Customs and Border Protection and the Coast Guard for purposes of maritime boundary domain awareness and enforcement activities along the maritime boundaries of the United States, including the maritime boundaries in the northern and southern continental United States and Alaska.

(b) **PRIORITY.**—In establishing the capability under subsection (a), the Secretary shall prioritize enforcement areas experiencing the highest levels of enforcement activity.

(c) **REQUIREMENTS.**—The capability established under subsection (a) shall be sufficient for the secure sharing of data, information, and surveillance necessary for operational missions, including data from governmental assets, irrespective of whether an asset located in or around mission operation areas belongs to the Coast Guard, Customs and Border Protection, or any other partner agency.

(d) **ELEMENTS.**—The Commissioner of Customs and Border Protection and the Commandant shall jointly—

- (1) Assess and delineate the types of data and quality of data sharing needed to meet the respective operational missions of Customs and Border Protection and the Coast Guard, including video surveillance, seismic sensors, infrared detection, space-based remote sensing, and any other data or information necessary;
- (2) Develop appropriate requirements and processes for the credentialing of personnel of Customs and Border Protection and personnel of the Coast Guard to access and use the capability established under subsection (a); and
- (3) Establish a cost-sharing agreement for the long-term operation and maintenance of the capability and the assets that provide data to the capability.

(e) **REPORT.**—Not later than 2 years after the date of enactment of this Act, the Secretary shall submit to the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Transportation and Infrastructure and the Committee on Homeland Security of the House of Representatives a report on the establishment of the capability under this section.

(f) **RULE OF CONSTRUCTION.**—Nothing in this section may be construed to authorize the Coast Guard, Customs and Border Protection, or any other partner agency to acquire, share, or transfer personal information relating to an individual in violation of any Federal or State law or regulation.

II. Background

The Department of Homeland Security (DHS) needs an enterprise information sharing environment “operationalized” by an Information Technology (IT) infrastructure and an associated set of enterprise services that facilitate a managed flow of information between Components. This infrastructure would provide DHS Components and participating federal, state, local, tribal, international, public, and private (FSLTIPP) partners the ability to unify efforts through:

- Broader access to common/federated data;
- Synchronized domain and situational awareness;
- Enhanced ability to share unclassified information at national, regional, and tactical levels to maximize the availability and accessibility of the data to improve research, analysis, and threat reporting; and
- Improved ability to connect operational systems, data sources, and application-based functionality using common standards and repeatable integration patterns.

Lacking this capability, DHS Components and their FSLTIPP partners continue to be limited in their ability to share, coordinate, and act on operationally important information, and remain ill-equipped to optimize limited resources against anticipated threats.

The Integrated Multi-Domain Enterprise (IMDE) program was a non-major and non-special interest joint IT acquisition program intended to address these gaps. The effort began in 2015 as a DHS Science and Technology Directorate research project. It involved representatives from U.S. Coast Guard, U.S. Customs and Border Protection (CBP), Homeland Security Investigations (HSI), and the Office of Operations Coordination, as well as support from the DHS Office of the Chief Information Officer (OCIO). The program emerged out of a Joint Mission Need Statement (JMNS), which was completed in 2017 and validated by the Joint Requirements Council in early 2018. To date, the IMDE program has not delivered capability to DHS users.

As originally envisioned, the IMDE program intended to offer DHS Components a Department-level unclassified information sharing capability. This capability was expected to comprise both materiel and non-materiel solutions. The materiel solution was expected to involve the acquisition and implementation of attribute-based access control capabilities. These solutions were expected to enable data owners to control how their data was shared with an external stakeholder. The non-materiel solution involved the harmonization of data policies and governance standards to ensure IMDE’s materiel solutions could fully identify and implement these policies and governance standards.

In August 2023 the DHS Chief Information Officer (CIO) directed the program to reassess whether the program’s original capability gaps, first identified in 2017, remained valid. The CIO also directed the IMDE program to assess the extent to which technological changes implemented at DHS since 2017 could be leveraged to address capability gaps. The findings of this reassessment were presented to the IMDE Component stakeholders in November 2023. This assessment found that many existing Department-level and Component technical and non-materiel solution approaches have significantly matured since validation of the original IMDE

JMNS in 2017. These include significant enhancement of Department-level data access, security, and quality; situational awareness; and data inventory and discovery technical solutions. Further, new capabilities that can be used to address IMDE's non-materiel gaps had been established since validation of the JMNS, including the establishment of Department- and Component-level Chief Data Officers.¹ These roles are intended to action many of IMDE's non-materiel gaps as well as many of the recommendations that were being incorporated into the program's draft IMDE Non-Materiel Change Recommendation. DHS has also established a Department-level Chief Data Officer's Council, which provides Components with a forum in which to raise data management and sharing issues to the DHS Headquarters level.

On July 24, 2024, IMDE Executive Steering Committee (ESC) members met to discuss the program's acquisition way forward. At the meeting, OCIO outlined its position that, given the availability of solution approaches that leverage existing solutions, an acquisition approach to capability development was not appropriate. This report details the efforts to leverage existing Department-level and Component technical and non-material solutions.

¹ DHS has appointed a Department-level Chief Data Officer pursuant to the Foundations for Evidence-based Policymaking Act of 2018, codified in 44 U.S.C. § 3520. DHS established a Chief Data Officer's Council as required by Office of Management and Budget Memorandum M-19-23, *Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance*, 10 July 2019. Each IMDE Operational Component has also appointed a Component-level Chief Data Officer as well as established data and analytics offices to implement data management best practices that align to the intent of the Evidence Act pursuant to direction from the Deputy Under Secretary for Management, *Request for Department of Homeland Security Data Governance Council Nominees*, 19 December 2019. DHS also directed Components to identify and appoint Component CDOs pursuant to Management Directorate guidance issued in 2019.

III. Report

CBP, ICE/HSI, and the Coast Guard continue to pursue capabilities to enhance marine domain awareness and provide opportunities to improve information sharing between components. Examples of these projects include:

- The Joint Persistence Wide-Area Maritime Surveillance Project;
- The joint use of Coast Guard and CBP Minotaur data;
- HSI efforts to share intelligence products from RAVEN; and
- CBP's Unified Immigration Portal.

Components also implemented non-materiel efforts such as the recent modernization of the Maritime Operations Coordination Plan (2022), which establishes requirements to improve operational and intelligence coordination. Although these efforts are worthwhile, none of these projects represents a centralized DHS-level enterprise solution to information sharing. This report endeavors to answer requirements of Section 11264. Report elements are specific to the IMDE and are collaboratively developed and submitted by the Coast Guard, CBP, and HSI Component executives who are assigned to the joint IMDE ESC.

11264(d)(1): Assess and delineate the types of data and quality of data sharing needed to meet the respective operational missions of Customs and Border Protection and the Coast Guard, including video surveillance, seismic sensors, infrared detection, space-based remote sensing, and any other data or information necessary.

CBP, ICE/HSI, and Coast Guard assessed and delineated data essential to meeting their respective operational missions. These include structured and unstructured unclassified data from relational databases and non-relational databases; analytic products; spreadsheets conforming to Open Document Format for Office applications; documents conforming to Open Document Format for Office applications; images; geospatial data; video formats; and raw sensor data.

11264(d)(2): Develop appropriate requirements and processes for the credentialing of personnel of Customs and Border Protection and personnel of the Coast Guard to access and use the capability established under subsection (a);

Components have worked collaboratively to develop and submit joint documents to address information sharing gaps. These documents include: Three Joint Capability Analysis Reports (2016); Joint Homeland Security-Information Sharing Joint Mission Needs Statement (2017); and IMDE Joint Concept of Operations Document (2023).

These documents provide Component sponsors' analysis of information sharing gaps and impacts on the ability to identify, plan, and respond to known and anticipated risks and threats to the United States. Further, lacking capability to share information in real-time inhibits the ability to deploy limited resources in a layered and systematic approach to maximize coverage.

The Components have outlined concepts and processes desired for the IMDE capability to support credentialing of personnel and those from partner organizations. Draft joint operational requirements were developed by Component sponsors in coordination with DHS CDOD staff; however, these requirements have not been assessed for viability nor validated by the

Components for OCIO to action. The Components anticipate existing DHS OCIO services and solutions will be leveraged to the maximum extent practicable to address the Mission Needs Statement gaps and requirements once they are finalized by the Components.

11264(d)(3): Establish a cost-sharing agreement for the long-term operation and maintenance of the capability and the assets that provide data to the capability.

Costs and sustainment strategies (to include any identified cost share) are generally articulated upon completion of the Life Cycle Cost Estimate and the Integrated Logistics and Support Plan (ILSP). The ILSP is developed once prototypes, reflecting a final solution, are identified. Based on data identified within these two documents, each Components' fiscal responsibilities and/or cost-sharing agreements are coordinated.

IV. Conclusion

No centralized capability currently exists that allows the Coast Guard, CBP, ICE, and authorized mission partners to share operational information at the tactical, operational, or strategic levels simultaneously, in real-time, and in a user's native system across all mission spaces. As a result, there is a continued need for DHS to invest in an improved information sharing capability that allows users to view information in their native system is an operational imperative across the DHS Enterprise and with FSLTIPP partners.

Component sponsors remain committed to the goal of operational information sharing. CBP, ICE/HSI, and the Coast Guard continue to collaborate at the Component level to establish requisite data governance and technical infrastructure; improve efficiency and effectiveness of our combined operations, enforcement activities, and investigative efforts; and advance our efforts to improve operations with our partner nations.

Appendix: Abbreviations

Abbreviations	Definition
CBP	U.S. Customs and Border Protection
DHS	Department of Homeland Security
DHS CDOD	DHS Chief Data Officer Directorate
DHS OCIO	DHS Office of the Chief Information Officer
ESC	Executive Steering Committee
FSLTIPP	Federal, State, Local, Tribal, International, Public, and Private
ICE/HSI	U.S. Immigration and Customs Enforcement/Homeland Security Investigations
ILSP	Integrated Logistics and Support Plan
IMDE	Integrated Multi-Domain Enterprise
IT	Information Technology
JMNS	Joint Mission Need Statement