NMIO Technical Bulletin

National Maritime Intelligence-Integration Office

NOVEMBER 2014 - VOL 8

Director NMIO View:

Rear Admiral Elizabeth L. Train, USN

As the Director of the National Maritime Intelligence-Integration Office (NMIO), I am pleased to present Volume 8 of NMIO's Technical Bulletin. The volume is primarily focused on data standardization and information sharing. Efforts to standardize data, increase data sharing, and improve interoperability are highlighted and provide insight from international, national, and local perspectives. I highly encourage readers to take advantage of the many tools and resources referenced throughout the bulletin, available from mda.gov and niem.gov. Importantly, this volume's focus on standards is a direct outcome of this year's Global Maritime Forum (GMF) workshop recommendations to enhance Maritime Domain Awareness (MDA) and promote maritime security. A full report detailing the GMF content and recommendations can be found at the following web address: http://nmio.ise.gov/GMF.htm.

I would like to personally thank the authors who have invested their valuable time to contribute to this edition of the Technical Bulletin. As we work together to promote global maritime security, I encourage others to become more involved in this community publication by submitting articles to help us broaden the topics and regions covered in this product.

I am equally grateful to our readers. Your insights, commitment, and feedback continue to positively affect the safety of the international maritime domain. It is my hope that through increased awareness and collaboration our mutual efforts will strengthen the security of the global maritime commons. NMIO is focused on identifying concerns and issues that resonate among government, academic, industry, and foreign partners, to identify the most efficient and cost effective solutions to our mutual maritime challenges.

As reflected in Presidential Policy Directive 18, "Maritime Security," NMIO is designated by the Director of National Intelligence as a U.S. Intelligence Community Service of Common Concern, providing and facilitating maritime intelligence integration and MDA information sharing for operational use by various Federal maritime stakeholder departments and agencies. NMIO continues to be the unifying maritime voice for the U.S. Intelligence Community.

The Technical Bulletin is one of our key vehicles to promote enhanced MDA and information sharing. We appreciate and invite your continued input, interaction, and contributions to this and other efforts that promote this shared mission. We hope you enjoy this publication, and I look forward to working with you to advance maritime security and build shared domain awareness.

NMIO Technical Bulletin **Volume 8, November 2014**

Editor In Chief: Dr. Paul Shapiro, Chief Science and Technology Advisor, NMIO
Phone: 301-669-2269 or 301-669-3400
Email: pshapiro@nmic.navy.mil
Chief, Strategic Engagement, NMIO: Mr. Brian F. Eggleston
Phone: 301-669-3830
Email: beggleston@nmic.navy.mil
Production: ONI Media Services
Address: 4251 Suitland Road
Washington DC 20395

Correspondence : Dr. Paul Shapiro

Contributions welcome: We welcome contributions from all Global Maritime Community of Interest stakeholders, both domestic and international. In submitting your article, please highlight who you are, what you are doing, why you are doing it, and the potential impacts of your work. Please limit your article to approximately one to two pages including graphics.

Cover image: A Coast Guard 25-foot response boat monitors activity as the Liquid Natural Gas (LNG) tanker Berge Boston is moored to the pier at an LNG facility in Boston. U.S. Coast Guard photo by Petty Officer 2nd Class Luke Pinneo.

Table of Contents

PM-ISE AND PROJECT INTEROPERABILITY

Michael Kennedy, Program Manager - Information Sharing Environment (PM-ISE)

Background

"In the aftermath of the 9/11 attacks, our government not only needed to improve its counterterrorism intelligence, but also share information better, faster, and smarter. We found that our national security relies on our ability to share the right information, with the right people, at the right time – and we must 'enlist all of our intelligence, law enforcement, and homeland security capabilities,' as the National Security Strategy states."
Kshemendra Paul, Program Manager – Information Sharing Environment.

The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 reorganized the Intelligence Community and directed the establishment of the Information Sharing Environment (ISE). The law required the President to designate a Program Manager for the ISE, whose role is to manage the ISE, oversee its implementation, assist in the development of ISE standards and practices, and monitor and assess its implementation by federal departments and agencies. In close collaboration with mission partners, the Office of the Program Manager–Information Sharing Environment (PM-ISE) supports implementation of the National Strategy for Information Sharing and Safeguarding (NSISS) as part of Federal policy guiding what we must do to share and safeguard information that enhances national security and protects citizen safety. Building on White House open government initiatives[1], PM-ISE has developed reusable tools to advance security through effective and secure information sharing.

Project Interoperability

Information interoperability is the ability to transfer and use information in a consistent, efficient way across multiple organizations and IT systems. From a technical perspective, interoperability is developed through the consistent application of design principles and design standards to address a specific mission problem. Information interoperability increases timely, responsible information sharing, can reduce costs and redundancy, and use best practices, all of which enhance decision making for government leaders, industry, and citizens.

Project Interoperability is a set of tools and resources made available to improve information interoperability. The ISE Information Interoperability Framework (I2F), Geospatial Information Reference Architecture (GIRA), Data Aggregation Reference Architecture (DARA), and the National Information Exchange Model are just a few of these tools and they are described below.

ISE Information Interoperability Framework (I2F)

The ISE I2F is used to guide the implementation of the ISE information sharing capabilities. This approach links information across jurisdictional boundaries and creates a distributed, protected, trusted environment for sharing information. It provides mechanisms to permit partner agencies at the Federal, state, local, tribal, and territorial levels (e.g., state fusion centers) to share similar data based on common standards and practices. The ISE I2F exploits existing information architectures by suggesting standards, tools, and methodologies to link existing systems as well as specifying the development of common artifacts that will enable disparate departments and agencies' architectures to make the full framework operational.

The ISE I2F was developed so that ISE participants could better respond to complex policy challenges and improve the delivery of services and information to protect our citizens. To achieve a connected government, ISE participants confidently manage, transfer, and exchange information by:

- Identifying key decision points for interoperability between disparate systems;
- Providing a comprehensive, high-level description of each interoperability domain; and,
- Establishing the framework for implementing ISE information sharing capabilities.

The ISE I2F delivers a management framework for extensible, measurable, and implementable interoperability requirements throughout the lifecycle of an investment. It prescribes how enterprise architecture, standards development, and profile descriptions can be best utilized to update, adopt, or create reference architecture, supporting system development efforts and governance principles.

[1] Open Government: On his first day in office, President Obama signed the Open Government memo, which articulated the importance of a transparent, participatory, and collaborative government. Later, he issued the Digital Government strategy and signed the Open Data Executive order. In support of this, the administration released Project Open Data on GitHub, a popular web-based collaboration tool. "The White House developed Project Open Data – a collection of code, tools, and case studies – to help agencies adopt the Open Data Policy and unlock the potential of government data," according to the site. Project Open Data is an inspiring example of the government sharing and promoting helpful resources, transparently, in collaboration with the public and other agencies. PM-ISE is borrowing the Whitehouse's Project Open Data approach for its Project Interoperability, by providing a resource for information sharing.

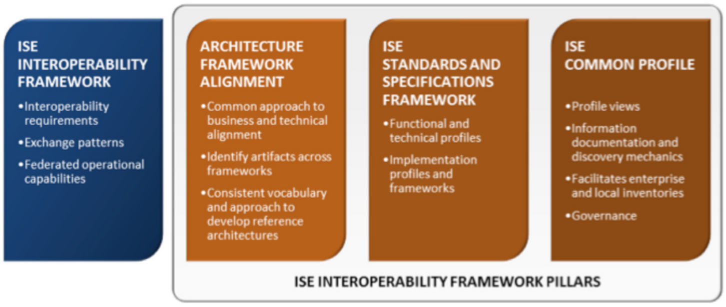

ISE INTEROPERABILITY FRAMEWORK
•Interoperability requirements
•Exchange patterns
•Federated operational capabilities
ARCHITECTURE FRAMEWORK ALIGNMENT
•Common approach to business and technical alignment
•Identify artifacts across frameworks
•Consistent vocabulary and approach to develop reference architectures
ISE STANDARDS AND SPECIFICATIONS FRAMEWORK
•Functional and technical profiles
•Implementation profiles and frameworks
ISE COMMON PROFILE
•Profile views
•Information documentation and discovery mechanics
•Facilitates enterprise and local inventories
•Governance
ISE INTEROPERABILITY FRAMEWORK PILLARS

Figure 1. The Information Sharing Environment (ISE) Information Interoperability Framework (I2F) Integrated Landscape (IL): Links three business and technical management disciplines that assist ISE participants in meeting interoperability requirements within their own operational capabilities.

Together, these tools comprise the ISE I2F Integrated Landscape, illustrated in Figure 1.

Over the long-term, the ISE I2F aims to develop confidence and trust-based culture in interoperability, where communities will look to discover existing standards and capabilities (e.g., managed services) before they focus on developing their own.

Geospatial Information Reference Architecture (GIRA)

A common challenge shared by all geospatial communities—those focused on intelligence, sensitive but unclassified, or public geospatial data—is providing decision makers access to the right data and services at the right time in a secure manner. As illustrated in Figure 2 below, there exists a broad scope of authoritative and trusted geospatial data sources. Based on public and private partnerships across all levels of government, national spatial data infrastructure is being built to promote data and system interoperability and support operational missions.[2]

Geospatial interoperability involves 3 components:

- Policy: align existing policies across government; not layer in additional policies;
- Standards: strengthen existing standards; not create new ones; and,
- Architecture Interoperability: optimize existing investments; not develop new requirements.

GIRA is a framework for developing new geospatial system investments and aligning existing geospatial capabilities that will be developed in coordination with our interagency partners and stakeholders. Architecture is an absolutely critical enabler of information sharing and GIRA holds great potential to accelerate responsible information sharing. The GIRA is:

- An I2F based reference architecture designed with current Federal policy, principles, and practices for Enterprise Architecture and further adds to the authoritative body of knowledge of geospatial architecture documentation;
- An unclassified document aimed at an audience consisting of: executive leaders, program managers, and solution architects across Federal, state, local, and territorial governments and private industry stakeholders; and,
- A practical guide including: templates, charters, exchange agreements, baseline requirements matrices, architecture artifacts, and tools and performance guides.

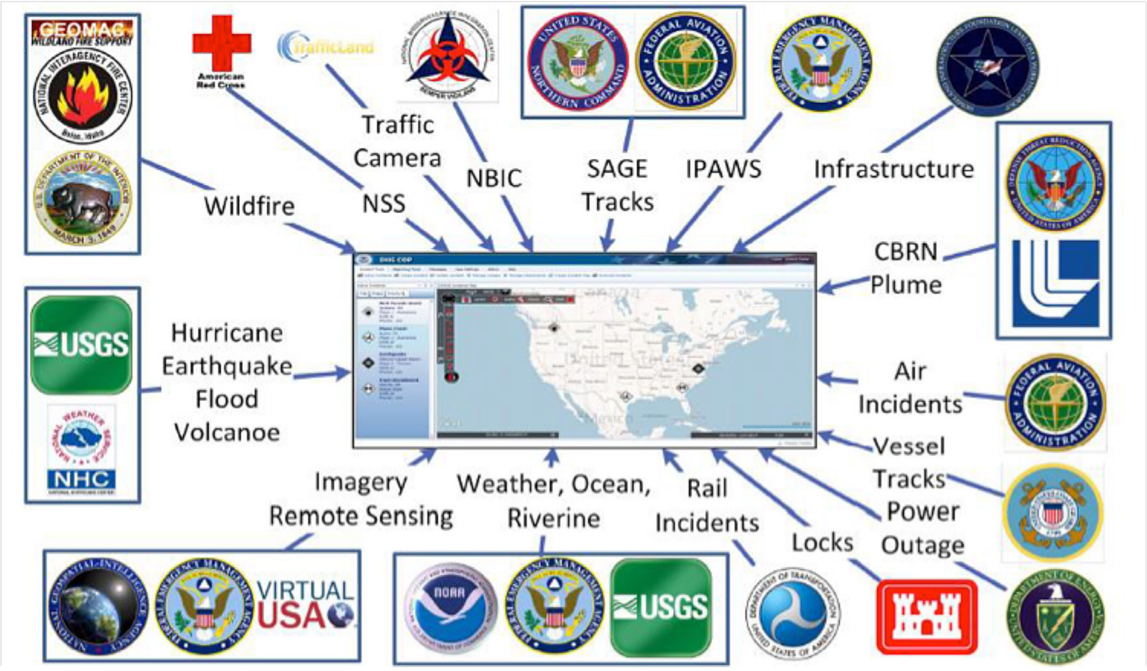


Figure 2. Homeland Security Geospatial Strategy Initiatives - National Spatial Data Infrastructure Built upon Authoritative & Trusted Geospatial Data Sources

[2] http://www.nsgic.org/public_resources/1600_2-25-2014-Alexander.pdf

Elements of the GIRA have been used to develop a Federation of Geospatial Infrastructure[3] to promote data and system interoperability, including data portability and access controls.

Data Aggregation Reference Architecture (DARA)

The DARA is an I2F based reference architecture that provides a representation of a data correlation system expressed in terms of the following functional areas: data, structural metadata, discovery, access control, change data management, transport/ infrastructure, and scalability. The DARA is designed as an instructive guide for executives, program managers, and solution architects. It provides a practical approach for the responsible assessment, planning, design/development, and implementation of an interoperable data aggregation investment.[4]

Organizations that interoperate through the DARA improve analytical capabilities through increased accessibility of information contained in other organizations' systems. When analysts are able to search correlated data that other agencies provide using the DARA framework, then organizations do not need to replicate that information between systems, which saves storage space, bandwidth, and technical staff time across the entire Federal enterprise.

The intent is to build a data and information environment that encourages agency level producers and aggregators to stage and expose their applicable information assets (i.e., leveraging already correlated [staged] data, and capabilities required for interoperability) by making data and information discoverable and sharable by other DARA consumers. Common services and other capabilities that are required for interoperability will be developed and used by data consumers and providers.[5]

As departments and agencies implement changes to the agency's capabilities to make information available, the interagency information sharing landscape changes to improve the mission value of the government's data holdings.

In an interagency data aggregation system assessment, it was determined that systems perform various levels of correlated data services based on the individual mission needs. Identified were three (3) types of data stores:

1) Non-shared Data – Data not for sharing outside of the organization.
2) Shared Raw Data – Data dumps that are made available for information sharing.
3) Shared Correlated Data – Correlated data that is made available for information sharing.

Ultimately, an optimized data aggregation system will present fully correlated entity maps formatted using open standards with granular, attribute based access controls using "data tags" (resource attributes) that are generated with only limited manual intervention. Data exchanges operating at the higher maturity levels result in higher quality analysis and a faster "speed to intelligence."

The future state envisioned with full DARA implementation is the availability to participating organizations of raw and correlated data at the speed necessary to identify and counter rapidly evolving threats. This will occur via the broad or complete adoption of community-wide standards as organizations implement the DARA, and the DARA and community systems continue to evolve over the next several years. An inability to share information at mission speed allows threats to develop and inhibits identification, assessment, and response.

National Information Exchange Model (NIEM)

NIEM, another tool within Project Interoperability, provides a standard, extensible format for use in the exchange of information between systems. The NIEM model defines a reference vocabulary to standardize the contents of messages being exchanged - the data and how it is structured. The following article provides additional information on NIEM and its use in the maritime domain.

For More Information

Resources on the ISE Information Interoperability Framework (I2F), Geospatial Information Reference Architecture (GIRA), Data Aggregation Reference Architecture (DARA), National Information Exchange Model (NIEM), or other Project Interoperability tools, are available at:
http://project-interoperability.github.io/.

[3] http://www.nsgic.org/public_resources/1600_2-25-2014-Alexander.pdf

[4] The ISA IPC Data Aggregation Report, released in 2012—ISE Data Aggregation Capabilities Applicable to Terrorism - presented the findings and recommendations of the interagency Data Aggregation Working Group regarding the current state and potential futures of data aggregation efforts across government agencies both within and outside the Intelligence Community. It outlines three themes for improvement for data aggregation systems: 1) The need for an improved interagency governance framework, 2) The need for improved processes for interagency data sharing agreements and, 3) Accelerate the convergence of existing Data Aggregation Architectures and encourages development of Data Aggregation Reference Architecture (DARA).

[5] https://max.omb.gov/community/download/attachments/736986154/Data_Aggregation_Way_Forward_PO10+v1+05312013.pdf

NATIONAL INFORMATION EXCHANGE MODEL (NIEM) AND THE MARITIME DOMAIN

Sean Tweed-Kent, National Maritime Intelligence-Integration Office (NMIO)

Background

The National Information Exchange Model (NIEM) was built upon the global justice xml data model (GJXDM)[1] and launched in 2005, uniting key stakeholders from Federal, state, local, tribal and territorial governments to develop and deploy a national model for information sharing and the organizational structure to govern it. All 50 states and 19 federal agencies are committed to using NIEM at varying levels of maturity. NIEM is a community-driven, standards-based approach to exchanging information through which diverse communities can collectively increase information sharing efficiency and improve decision-making.

NIEM Overview

The purpose of NIEM is to provide a standard, extensible format for use in the exchange of information between systems. It is a standard way of defining the contents of messages being exchanged - it is about the data and how it is structured. NIEM is not a system or database; nor does it specify how to transmit or store data. NIEM is a data layer (i.e., a payload). NIEM is rarely used by itself, as information exchanges often require access controls, policy automation, and other aspects of implementation.

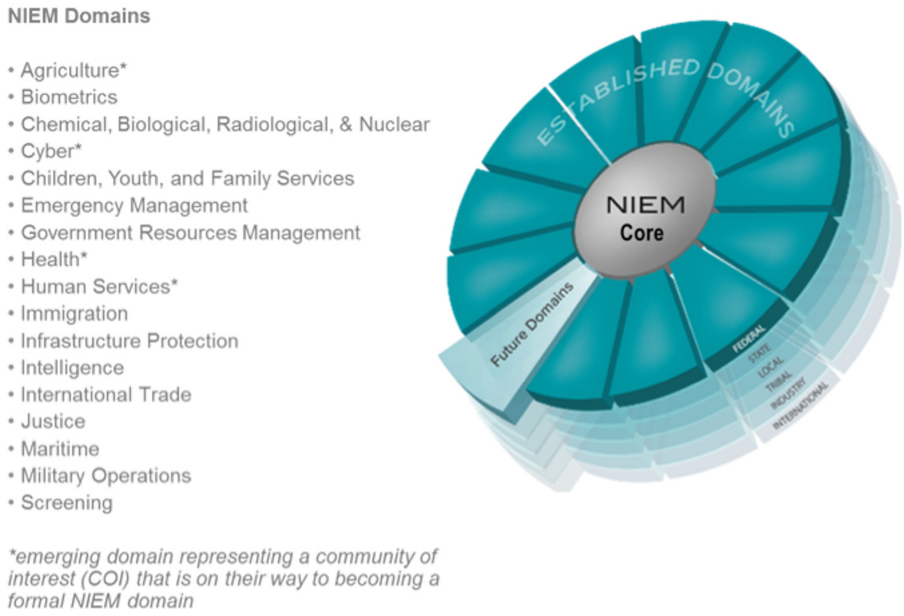
NIEM uses eXtensible Markup Language (XML) - the NIEM model is defined using W3C XML Schema[2] which is technology and platform independent. You can also represent NIEM in Unified Modeling Language (UML) with tooling that implements the NIEM-UML profile, and automatically produces NIEM-conformant XML schema.[3] The use of NIEM results in exchanges that are machine readable and license free.

Any system can put data into an XML document and transmit it to an exchange partner. Any system can receive and parse an XML document to extract the data. The hard part is ensuring that the system producing the data creates an XML document that means what the receiving system developer thinks it means and vice versa. That is what the NIEM standards-based approach is all about.

NIEM: A Common Vocabulary

The NIEM model provides a reference vocabulary for consistent reusable exchanges between systems to include common, agreed-upon terms, definitions, formats, and relationships independent of how information is stored in individual systems.

Within NIEM, there exist two related vocabularies, NIEM core and individual NIEM domains (Figure 1). NIEM core consists of data elements that are commonly understood and defined across domains, such as person, activity, document, location, and item. NIEM domains contain mission-specific data



NIEM Domains

- Agriculture*
- Biometrics
- Chemical, Biological, Radiological, & Nuclear
- Cyber*
- Children, Youth, and Family Services
- Emergency Management
- Government Resources Management
- Health*
- Human Services*
- Immigration
- Infrastructure Protection
- Intelligence
- International Trade
- Justice
- Maritime
- Military Operations
- Screening

emerging domain representing a community of interest (COI) that is on their way to becoming a formal NIEM domain

Figure 1. NIEM Domains.

[1] https://it.ojp.gov/default.aspx?area=nationalInitiatives&page=1013

[2] http://www.w3.org/standards/techs/xmlschema#w3c_all

[3] https://www.niem.gov/technical/Pages/niem-uml.aspx

components that build upon NIEM core concepts and add additional content specific to the community supporting that mission. A NIEM domain represents both the governance and model content oriented around a community's business needs. Each domain manages their portion of the NIEM data model and works with other domains to collaboratively identify areas of overlapping interest.

As a NIEM community member, involvement can span one or more NIEM domains and official alignment to an existing NIEM domain is not required to be a user of NIEM. Future domains are added as necessary, based on an established business need.

Exchange Development

NIEM is about the data and its structure as it moves between systems—i.e., "data in motion." Implementing NIEM provides a consistent, repeatable, and reusable way to build information exchanges. These exchanges are termed Information Exchange Package Documentation – or IEPD. An IEPD is a combination of both business and technical information for an information exchange. A developer builds an IEPD by incorporating the necessary NIEM core and domain model content. The developer may also extend that content as needed to account for information requirements that are not yet addressed in NIEM. The IEPD will ultimately define XML instance documents that will contain the information to be exchanged. Extended and new content developed in IEPD extension schema documents may be considered for future model updates. In turn, domain and core model updates will be harmonized and integrated into future NIEM releases. In this way, NIEM evolves with new and changing needs.

From a technical perspective, an IEPD is a set of XML schema documents that define instance XML documents which, in turn, will tag and carry the data and information to be exchanged. For example, when you want to exchange "person" data and its related attributes, you will leverage (essentially reuse from a NIEM release) XML schema components that define the "person" related tags and structures.

From the business perspective, an IEPD provides documentation such as business scenarios and other aspects of the business requirements for the exchange, including a catalog of its content, a change log, a conformance assertion, etc. In addition, reusing existing IEPDs that meet or can be easily adapted for similar business requirements is encouraged.

Resources for NIEM can be found at NIEM.gov, including tools for implementation, free online training, and the latest events.

NIEM in the Maritime Domain

In 2008, the NIEM program and the U.S. Department of Defense Executive Agent (DoD EA) for Maritime Domain Awareness (MDA) entered into a strategic partnership designed to strengthen information exchange for MDA by leveraging NIEM and founding the NIEM-Maritime (NIEM-M) domain. By 2012, a DoD Chief Information Officer (CIO) memorandum made NIEM the preferred data exchange standard for DoD information sharing solutions and authorized work with the NIEM Program Management Office to create a Military Operations (MilOps) domain.[4]

The NIEM-Maritime (NIEM-M) domain has taken an innovative management approach by implementing the first Enterprise Information Exchange Model (EIEM), winning "Best of NIEM 2013". The EIEM construct represents a new class of NIEM Model Package Definition (MPD) from which one or more NIEM-conforming IEPDs can be built. As a domain develops IEPDs, they may recognize similar business data. This collection of closely related business data can be organized at an object level and defined as extension data components, referred to as Business Information Exchange Components (BIEC). While IEPDs define recurring XML data exchanges, a BIEC is just the definition of a data component without the context of an exchange. Creating and maintaining an EIEM to author IEPDs encourages content reuse, reducing complexity and cost, and accelerates development.

NIEM-Maritime (NIEM-M) Enterprise Information Exchange Model (EIEM)

The Maritime EIEM is a NIEM-conformant set of XML schemas and other artifacts defining core maritime focused entities, or BIECs. The following high-level BIECs serve as building blocks to be used across multiple maritime exchanges.

- Activity
- CDC Cargo (Certain dangerous cargo as declared in an Advance Notice of Arrival)
- Crew Nationality Count
- GeoLocation
- Interest
- Movement
- Notice of Arrival (NOA) Cargo (Bulk cargo as declared in an Advance Notice of Arrival)
- Non-Crew Nationality Count
- Port Visits

[4] DoD adoption of NIEM per DoD CIO Memorandum dated March 28, 2012

- Position
- Record Metadata
- Vessel Characteristics
- Vessel History
- Vessel Identification
- Vessel Information

Implementing an EIEM increases the commonalities among models and delivers a number of benefits, because it:

1. Simplifies development and allows users to develop reusable processes that work across multiple record types,
2. Reduces complexity by reducing the number of overall elements that need to be supported,
3. Decreases the time and cost of maintaining the model because it is simpler and has less overlap,
4. Reduces implementation time for new exchanges from weeks to days.

NIEM-Maritime Exchanges

As previously described, an IEPD defines a particular record type, the basic unit of shared information. The IEPDs with a maritime focus are:

- Advance Notice of Arrival (NOA)
- Indicators and Notifications (IAN)
- Vessel Positions and Tracks
- Maritime Operational Threat Response (MOTR)
- Levels of Awareness

As depicted in Figure 2, each NIEM-M IEPD uses a subset of the core BIECs defined in the EIEM and assembles them into a particular record type with its own unique root element. As new requirements are defined, new IEPDs can be created that build on the same EIEM core entities.

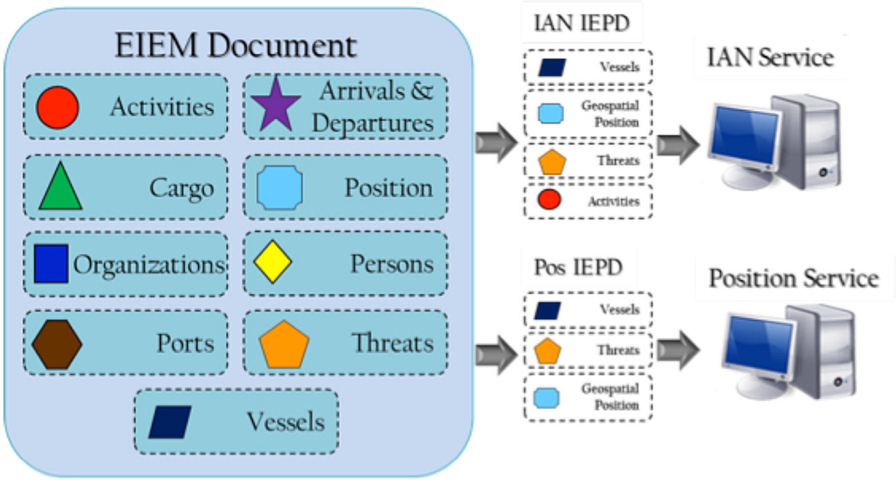


Figure 2. EIEM core entities and NIEM-Maritime IEPDs

NIEM: Moving Forward

Organizations across the public, government, and private sector are committed to advancing and substantially improving the way information is shared to deliver results that improve performance, increase efficiency, and support transparency. NIEM, a tool within PM-ISE's Project Interoperability, is a model for community led standards development that continues to expand through new domains and further development of existing domains.

Resources and opportunities to collaborate are available at niem.gov and mda.gov. Additional questions about NIEM-Maritime can be answered by the NIEM Maritime Domain Steward, Mr. Frank Sisto, at frank.sisto@navy.mil.

ENHANCING MARITIME SITUATIONAL AWARENESS THROUGH INFORMATION INTEROPERABILITY

Steven Horn, NATO Centre for Maritime Research and Experimentation (CMRE)

Maritime Situational Awareness is an enabling component of Maritime Operations. Although NATO is a military alliance, today NATO conducts two maritime operations, both of which are outside the scope of conventional warfare. Operation Ocean Shield, conducted in and around the Indian Ocean, counters the piracy problem along the east coast of Africa. Operation Active Endeavour, conducted in the Mediterranean Sea, combats terrorism and the illegal movement of weapons of mass destruction. In both these operations, the adversaries are not easily identified and compounded to this problem is that the area of operations are enormous. It is clear that meeting the NATO Maritime operational objectives is a difficult challenge.

Securing the global stake in the maritime commons means that interagency and international cooperation, combined with coordinated response, is important for effectiveness and success. The concept of operations for conducting these security operations is new to the Alliance, and effectiveness and success depends on being able to adapt to the challenges.

One adaption stems from the need to identify threats far away from where they may strike, which decreases vulnerability by reducing the necessity to respond to threats on short timescales. In order to detect and identify these threats, two vectors of action have taken place: 1) more data is being collected, and 2) more data is being shared. In the course of these actions, the operational commands, in their pursuit of detecting a threat, have transitioned from a state of information scarcity to information abundance. This is driving the tantalizing thought that the information required to detect a threat could be in the data available, but the "how to" of fully using all of the available information to make the connections sufficiently in advance is often missing.

Enabling the transition to information abundance is the ongoing improvement of Information Interoperability within the Alliance, which makes the sharing of information technically possible. The interoperability afforded by improved, standardized, and extensible information exchange techniques, such as the National Information Exchange Model (NIEM), opens the door to more exchange partners than ever before.

The level of interoperability in the Alliance will continue to increase in future years as the Federated Mission Network (FMN) is implemented (Figure 1). The effect of this trend is that the capability and capacity of the Alliance to manage the scale of effort required will be established. Within the FMN, it is important that the "how to" for using the abundance of information is included.

Exploiting the data, now that the technology will be in place to make it accessible, is an important S&T activity. For example, the method of deriving higher-level knowledge from noisy or low-signal data is the key to being able to use the abundance. Furthermore, it is unlikely that a single data source will have all the critical pieces

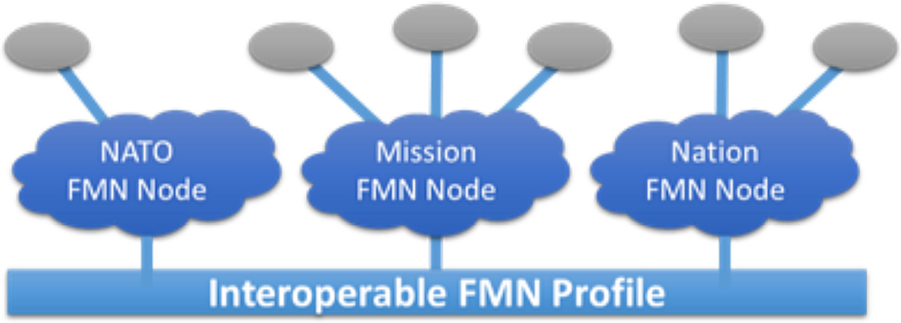


Figure 1. Federated Mission Network (FMN)

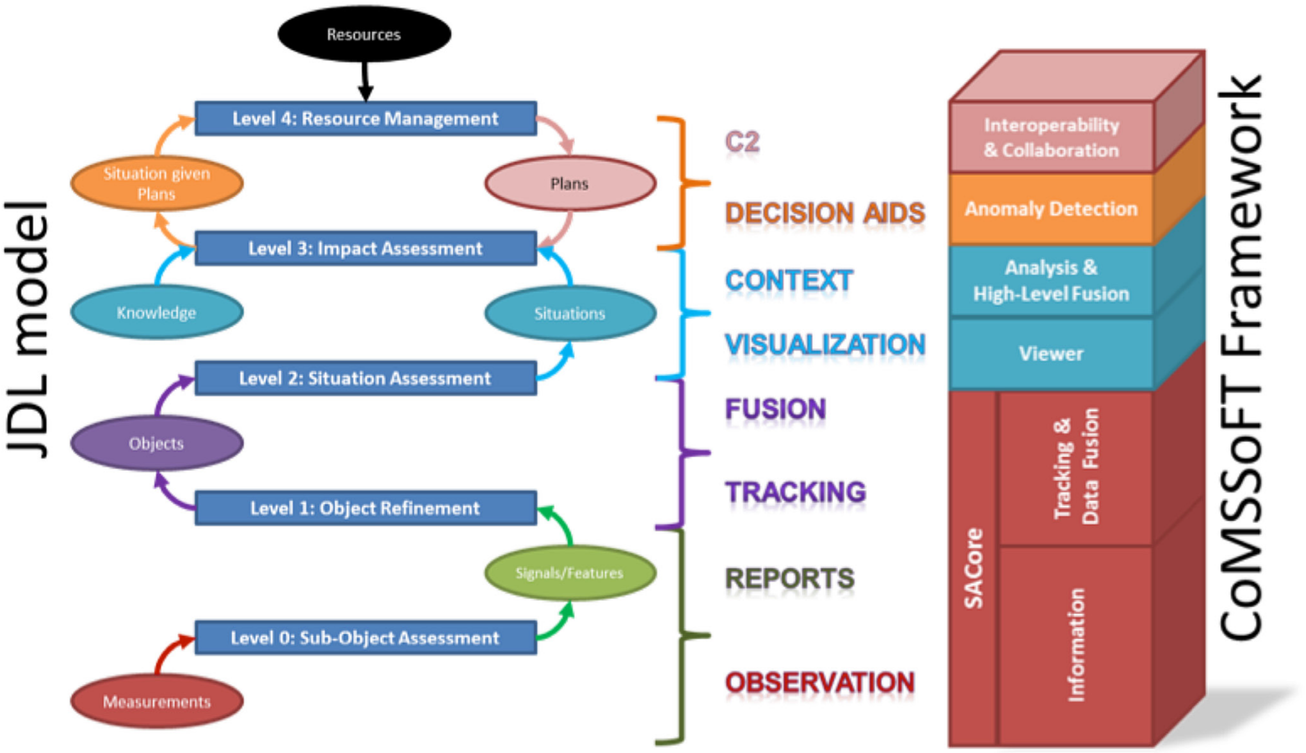


Figure 2: JDL Model and the CoMSSoFT Framework

of information. Aligned with the FMN approach, CMRE is developing and experimenting with Service Oriented Architecture (SOA) solutions which can better combine and process the various sources of data. Fusion as a Service (FaaS) is one capability which uses the Collaborative Multi-Sensor/Source Fusion and Tracking (CoMSSoFT) concept as a means to rapidly incorporate information from new sensors and sources, and provide augmented information to the command and control chain (Figure 2).

Building on the FaaS platform, additional processing of the information provides higher-level situational awareness not previously possible. For example, another project at CMRE, developing the Traffic Route Extraction and Anomaly Detection (TREAD) tool, automatically identifies normal patterns in the data (Figure 3). With this knowledge, it is then possible to identify abnormal or anomalous patterns in the data – possibly a threat. Currently, these types of machine learning techniques complement human operators by identifying patterns in large sets of data that would be difficult for humans to see. In the future, further automation of these processes will allow also the scalability of threat detection beyond what can be done by a limited set of human operators.

The concept and conduct of operations can be transformed based on these services to optimize the effectiveness and opportunity for success for NATO operations, which for the foreseeable future will include security operations. This transformation is not linear and is enabled by a strong interaction between the military operational domain and S&T domain.

The bridge from R&D to operational capability must be created in order for fast and timely transformation to operations. Through operational experimentation, the experimental tools and products can be provided to the operational community for quick exploitation and to collect feedback and experimental observations of use. The value added from these real world use case observations for further research is invaluable for the identification of future directions of relevant research and the generation of requirements. Closing the loop then provides a better experimental capability for operations, and so on. To achieve this loop,

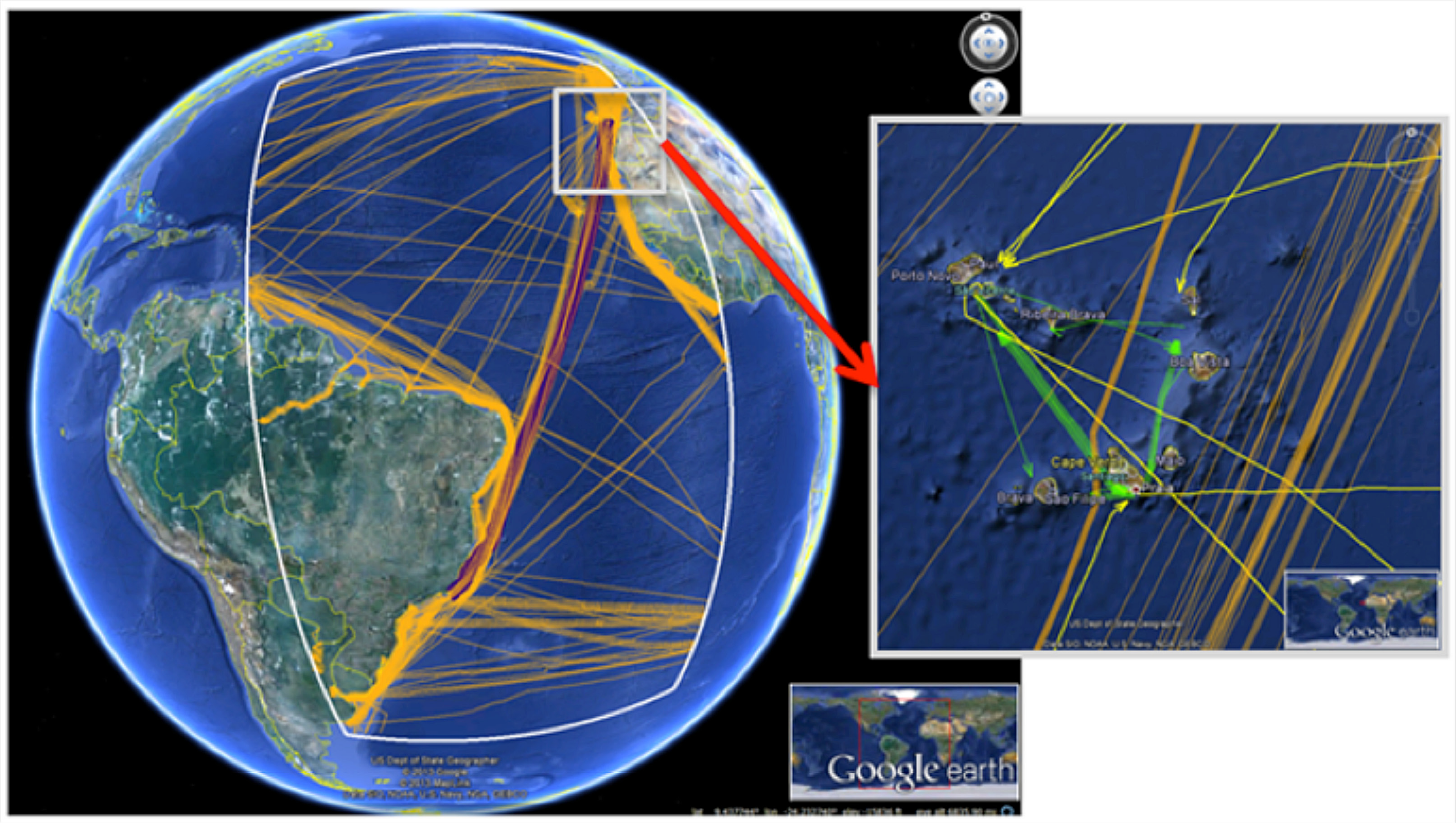


Figure 3: Traffic Route Extraction and Anomaly Detection (TREAD) automatic identification of normal patterns

there must be frequent and close connection between the research and experimentation communities and the operational communities.

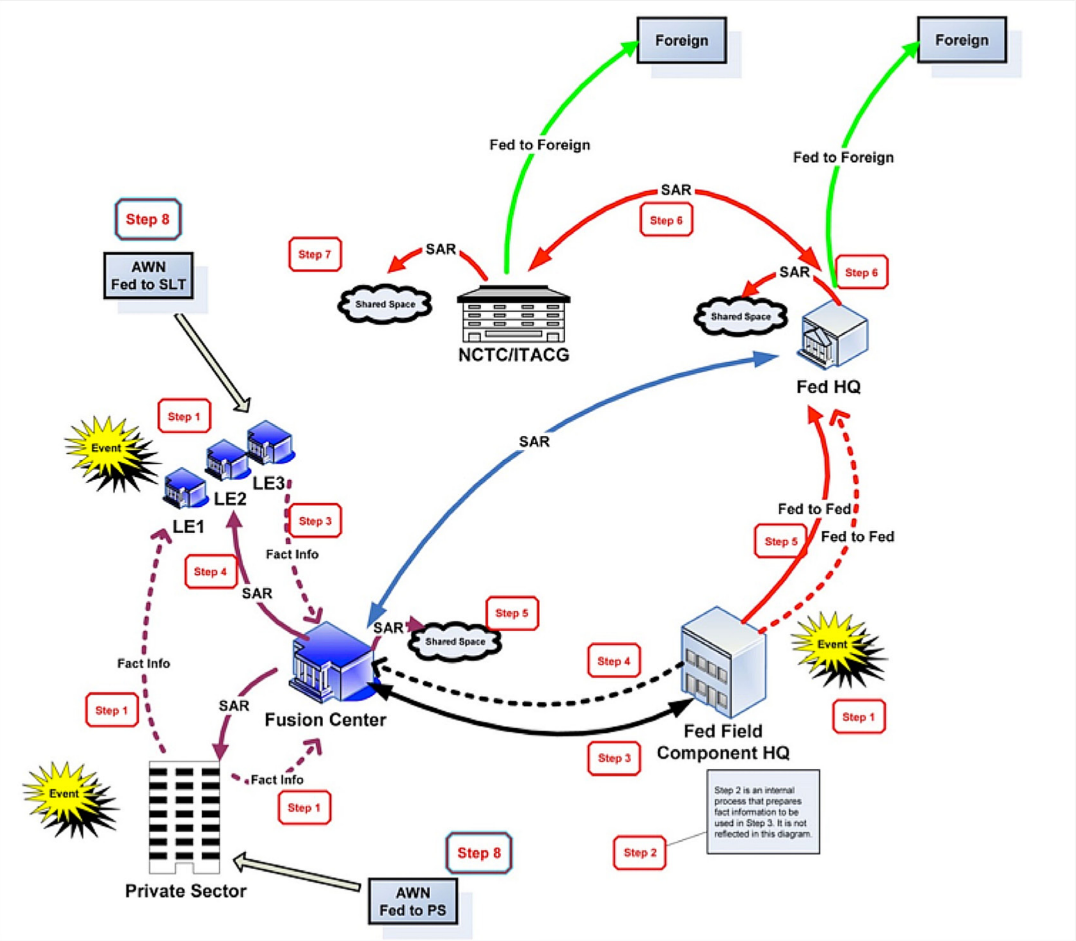
Effectively exploiting the newfound information abundance will lead to a needed change in the way operations are conducted. A move from a reactive stance to a more proactive stance will ensure that more threats are detected and identified as early as possible to reduce the risk to the economies and security of the Alliance and the global maritime commons.

MARITIME SUSPICIOUS ACTIVITY REPORTING (SAR) INITIATIVE (MSI) AND THE ISE-SAR FUNCTIONAL STANDARD

Robert Hall, National Maritime Intelligence-Integration Office (NMIO)

The Maritime Suspicious Activity Reporting (SAR) Initiative (MSI) was a partnership formed between the National Maritime Intelligence-Integration Office (NMIO) and the Nationwide Suspicious Activity Reporting Initiative (NSI) for the purpose of increasing suspicious activity awareness and reporting among the maritime community's workers, security personnel, and executives (Figure 1). Due to national level interest and the interagency nature of suspicious activity reporting, the MSI effort was accomplished in close coordination with the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the United States Coast Guard (USCG).

The NSI was developed as a result of the 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA) and the 2007 National Strategy for Information Sharing, and is a partnership among Federal, state, local, tribal, and territorial law enforcement. The NSI established a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information that rigorously protects the privacy and civil liberties of Americans. This process is referred to as the SAR process and is critical to sharing information about suspicious activity with a potential nexus to terrorism, which can help prevent terrorist attacks and other related criminal activity from occurring. The ISE-SAR Functional Standard v. 1.5 defines suspicious activity as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." The standard was developed after critical input from several privacy, civil rights, and civil liberties advocacy groups, including the American Civil Liberties Union (ACLU).



Step 2 is an internal process that prepares fact information to be used in Step 3. It is not reflected in this diagram.

Figure 1: Suspicious Activity Report Information Flow Diagram[1]

[1] Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5, available online.

The MSI effort was established to conduct outreach with the maritime community in order to enhance NSI and SAR awareness, identify gaps in SAR information sharing, and develop the necessary training to ensure timely and relevant SAR information is shared with and among law enforcement agencies and other public safety partners. This outreach included critical partners such as NSI Field Liaison Representatives, DHS Intelligence Officers (IOs), DHS Protective Security Advisors (PSAs), FBI Maritime Liaison Agents (MLAs), and State/Major Urban Area Fusion Centers.

To support the overall two-year effort, a team comprised of select individuals from NMIO, the sponsor organization; its partner, the NSI; and the other supporting agencies involved in promoting SAR awareness was formed. The MSI team engaged in a concerted effort that involved development of a maritime SAR training module and extensive outreach to select U.S. ports to promote NSI and SAR awareness.

During the two year initiative, the MSI team learned that a fairly complex SAR process exists at the national level. This process is highly dependent on local suspicious activity reporting and sharing to ensure pertinent information is properly collected, investigated, and analyzed by trained professionals; correctly developed into SARs that meet the accepted functional standard criteria; and promptly shared via the SAR Data Repository (SDR) for follow up investigation and threat analysis. The MSI team also discovered that, for the maritime environment, there are numerous paths for the reporting and processing of SARs and that in general, the maritime community's SAR awareness and understanding of the SAR processes that exist are immature, and as a result, many challenges to effective SAR creation and information sharing exist.

Regardless of what SAR path is followed, the ultimate goal is for all observed suspicious activity to be accurately reported, properly investigated and analyzed, and if warranted, developed into a SAR that meets the NSI SAR functional standard, and is then promptly shared via the SDR. The ability of law enforcement at all levels to preserve public safety and prevent or respond effectively to illegal activity will be greatly enhanced when information, such as suspicious activity reporting, is readily available.

ISE-SAR Functional Standard Details[2]

Common Terrorism Information Sharing Standards (CTISS) are business process-driven, performance-based 'common standards' for preparing terrorism information for maximum distribution and access to enable the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE. One category of common standards formally identified under CTISS is functional standards. Functional standards include set forth rules, conditions, guidelines, and characteristics of data and mission products supporting ISE business process areas.

In particular, an ISE-SAR is a SAR that has been determined, pursuant to a two-part process, to have a potential terrorism nexus. ISE-SAR business, privacy, and civil liberties rules will serve as a unified process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE. In addition to providing specific indications about possible terrorism-related crimes, ISE-SAR can be used to look for patterns and trends by analyzing information at a broader level than would typically be recognized within a single jurisdiction, state, or territory. Standardized and consistent sharing of suspicious activity information regarding criminal activity among state and major urban area fusion centers and Federal agencies is vital to assessing, deterring, preventing, or prosecuting those involved in criminal activities associated with terrorism.

The ISE-SAR Functional Standard is a collection of artifacts that support an implementer's creation of ISE-SAR information exchanges. The basic ISE-SAR information exchange is documented using five unique artifacts giving implementers tangible products that can be leveraged for local implementation. A domain model provides a graphical depiction of those data elements required for implementing an exchange and the cardinality between those data elements. Second, a Component Mapping Template is a spreadsheet that associates each required data element with its corresponding XML data element. Third, information exchanges include the schemas which consist of a document, extension, and constraint schema. Fourth, at least one sample XML Instance and associated style-sheet are included to help practitioners validate the model, mapping, and schemas in a more intuitive way. Fifth, a codified data field values listing provides listings, descriptions, and sources as prescribed by the data fields.

The ISE-SAR Functional Standard is used as the ISE-SAR information exchange standard for all ISE participants (Figure 2). Although the extensibility of this ISE-SAR Functional Standard does support customization for unique communities, jurisdictions planning to modify the ISE-SAR Functional Standard must carefully consider the consequences of customization. Furthermore, messages that

[2] Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5, available online.

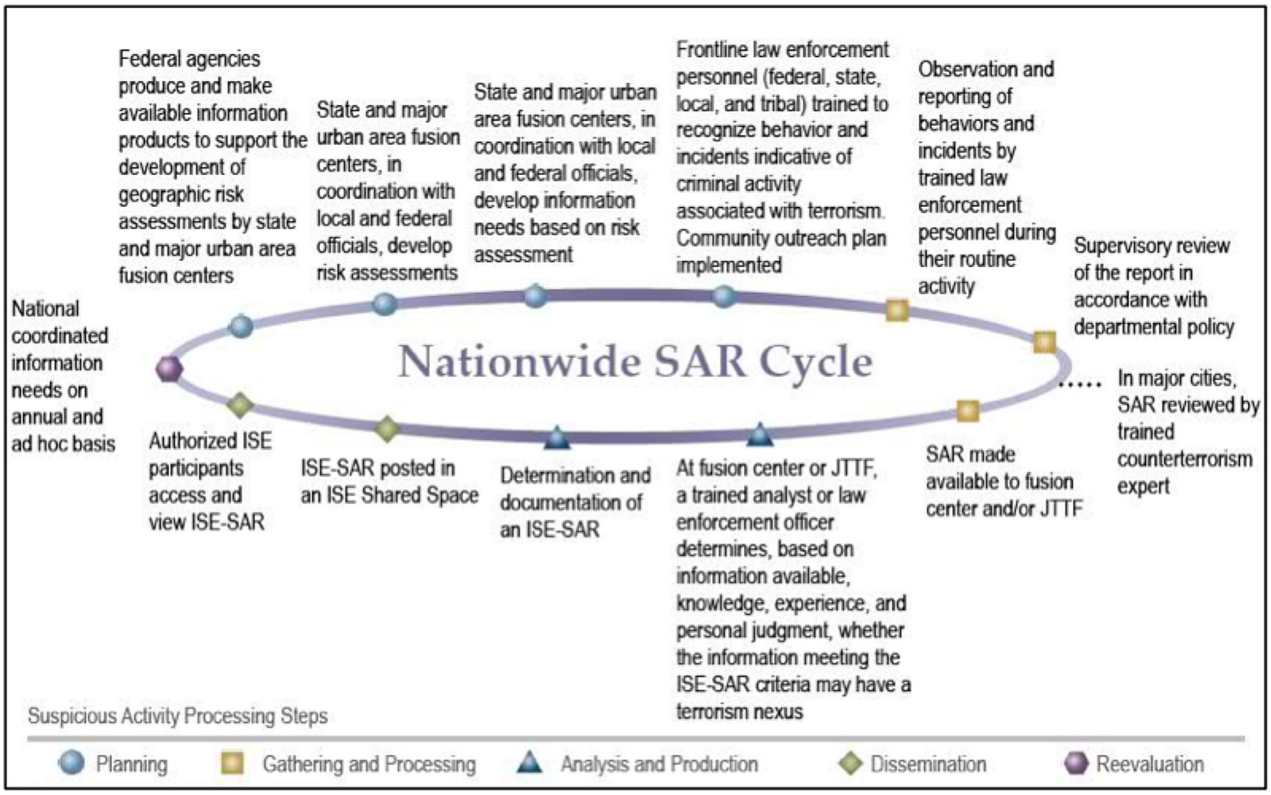

Federal agencies produce and make available information products to support the development of geographic risk assessments by state and major urban area fusion centers
State and major urban area fusion centers, in coordination with local and federal officials, develop risk assessments
State and major urban area fusion centers, in coordination with local and federal officials, develop information needs based on risk assessment
Frontline law enforcement personnel (federal, state, local, and tribal) trained to recognize behavior and incidents indicative of criminal activity associated with terrorism. Community outreach plan implemented
Observation and reporting of behaviors and incidents by trained law enforcement personnel during their routine activity
Supervisory review of the report in accordance with departmental policy
National coordinated information needs on annual and ad hoc basis
Nationwide SAR Cycle
In major cities, SAR reviewed by trained counterterrorism expert
Authorized ISE participants access and view ISE-SAR
ISE-SAR posted in an ISE Shared Space
Determination and documentation of an ISE-SAR
At fusion center or JTTF, a trained analyst or law enforcement officer determines, based on information available, knowledge, experience, and personal judgment, whether the information meeting the ISE-SAR criteria may have a terrorism nexus
SAR made available to fusion center and/or JTTF
Suspicious Activity Processing Steps
● Planning
■ Gathering and Processing
▲ Analysis and Production
◆ Dissemination
● Reevaluation

Figure 2: Overview of Nationwide SAR Process [3]

do not conform to the Functional Standard may not be consumable by the receiving organization and may require modifications by the nonconforming organizations.

MSI Outcomes and Future

As a result of MSI port visits, several fusion center-related recommendations were made in the Final Report which led to the adoption of a resolution by the National Maritime Security Advisory Committee (NMSAC). The NMSAC resolution recommended approving a number of changes to align United States Coast Guard (USCG) policy with the NSI and the MSI's findings. A few of those changes are:[4]

- Ensure that all USCG components provide consistent information to stakeholders on SAR including the prioritization of notifications to be made;
- Encourage SAR training and information sharing for all maritime stakeholders and have training programs (33 Code of Federal Regulations parts: 104.220, 104.225, 105.205, 105.210, and 105.215) include a module on maritime SAR;
- Institute a process to ensure that SAR is bi-directional and those making reports receive feedback;
- Incorporate the use of a standard electronic application (e.g., web-portal, smartphone/tablet app) for reporting; and finally,
- USCG should require that all Area Maritime Security Committee's implement the recommendations and framework contained in the resolution.

The MSI Final Report also specifically recommended that elements of the maritime community responsible for the creation of SARs modify their reporting database to adhere to the ISE-SAR Functional Standard for producing and sharing SARs.[5] Lastly, as the two-year NMIO-led MSI comes to an end, the important work of SAR education and standardization advancement will continue. The USCG Facilities and Compliance office has agreed to promote maritime SAR training and coordinate on-going port visit outreach. The Maritime SAR Training for Hometown Security Partners is freely available online.[6] For additional information regarding the ISE-SAR Functional Standard, please reference the document's full text.[7]

[3] Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5, available online.

[4] National Maritime Security Advisory Committee (NMSAC) Resolution DRAFT 1.1 May 22, 2014

[5] Maritime Suspicious Activity Reporting Initiative (MSI): Final Findings & Recommendations Report, available upon request to NMIO.

[6] http://nsi.ncirc.gov/hsptregistration/maritime/

[7] https://www.ise.gov/sites/default/files/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf