

## **THE DHS INFORMATION SHARING AGREEMENTS PROCESS AND TOOLS – IMPLEMENTING THE “ONEDHS” POLICY**

By Irene Hoffman Moffatt, Senior Policy Analyst, U.S. Coast Guard Maritime Domain Awareness and Information Sharing Staff - with major contributions from the DHS Office of Intelligence and Analysis, Information Sharing and Collaboration Branch

### **INFORMATION SHARING POLICY OVERVIEW**

The DHS mission to detect, interrupt and prevent international and domestic threats to homeland security is ever critical. As such, timely, broad, and unfettered, sharing and access to terrorism, homeland security, law enforcement, intelligence information and/or data between DHS Components is one of the high priorities for the Department. As stated by DHS Secretary Napolitano’s congressional testimony, earlier this year, “It is important that we develop an identity for DHS that is centered on the department’s mission and that we build a ‘one DHS’ culture among the different components of the department.”

So then, notwithstanding statutory or other legal prohibitions to the contrary, whenever DHS personnel, acting on behalf of a Component in furtherance of the DHS mission, has satisfactorily demonstrated an authorized need to obtain and access certain information and/or data, of which another DHS Component has stewardship, such information and/or data shall be disseminated without delay to the requestor. This is known as the *DHS Policy for Internal Information Exchange and Sharing*, commonly referred to as the “One DHS” policy, issued in 2007.

In a nutshell, the OneDHS policy is an acknowledgement that while DHS is comprised of multiple Components, it is nevertheless a single unified entity wherein all relevant information generated and received by individual entities within DHS is to be accessible to and shared amongst and between all other DHS Components that have a demonstrated need to know.

The “One DHS” policy replaces the former “need to know” criterion for information and intelligence sharing with the new “responsibility to share,” providing DHS personnel a powerful resource and establishing DHS as a leader in the information-sharing efforts vital to protecting the nation.

The “One DHS” policy has transformed the information-sharing policy landscape by declaring, “DHS personnel must have timely access to all relevant information they need to successfully perform their duties” and that “[n]o DHS component should consider another DHS component to be a separate agency for information-sharing purposes.” In this regard, the OneDHS policy applies most obviously to the Information Sharing Access Agreements.

### **INFORMATION SHARING ACCESS AGREEMENTS**

Information Sharing and Access Agreements (ISAAs), the primary vehicle used to exchange, receive and share information from external parties (i.e. non DHS), are arrangements, policies, standard operating procedures, practices, understandings, etc. that are memorialized on behalf of DHS in formal official documents such as Memorandums of Understanding, Memorandums of Agreement, Letters of Intent, to name a few.

### ***ISAA OneDHS Policy Compliance Review***

All ISAAs are subject to mandatory review by the Information Sharing Coordination Council (ISCC), comprised of action officers from various DHS Components, for compliance with the OneDHS Policy. Compliance is achieved if the terms of the ISAA do not limit dissemination of the information/data received for an authorized purpose or use.

ISAAs that have not been through OneDHS policy compliance review and/or that conflict with the OneDHS policy cannot be executed or signed. It is important to note that OneDHS review is just one of multiple potential mandatory reviews for ISAAs. Therefore, OneDHS is not the only step that must be satisfied before ISAA execution or signature is authorized. USCG-specific review and clearance steps for ISAAs will be published and disseminated to the USCG field units upon release of the highly anticipated revised ISAA Methodology Guidebook, which is discussed below.

During the OneDHS policy compliance review, the ISCC action offices circulate the ISAA throughout their respective organizations for a review to determine if access to the information that is the subject of the ISAA is in anyway limited or otherwise trespassed upon.

If there are no OneDHS policy objections, the ISAA is deemed OneDHS compliant. If there are OneDHS policy objections, then the ISAA must be changed or modified to achieve OneDHS policy compliance before it can be executed. Please note that a finding of OneDHS policy compliance may be delayed where and if issues concerning privacy, civil rights and civil liberties, and other general legal considerations are identified. Therefore, it is important to engage the DHS and USCG Privacy Offices, Offices of Civil Rights and Civil Liberties, and Offices of General Counsel at the outset minimize delays.

### ***Initiating the OneDHS Policy Compliance Review Process***

To initiate mandatory OneDHS policy compliance review of an ISAA, DHS Components, including Coast Guard must submit the ISAA, along with a brief background summary about the agreement, and other supporting documentation, to the Office of Intelligence and Analysis, Information Sharing and Collaboration Branch at [ISAA@dhs.gov](mailto:ISAA@dhs.gov).

Upon receipt, IS&C staff will determine if an ISAA already exists pertaining to the subject and with the named external party by checking the ISAA Interim Repository

(more information below about the repository below) and if there is none, will proceed to prepare the ISAA for review by the ISCC. The review process takes about 10 business days.

After the review period, the IS&C generates a OneDHS Policy Compliance Review Result document for the ISAA originator. This document advises about whether an ISAA has been determined to be compliant with the OneDHS policy and details the nature and origin of ISCC comments.

As previously stated, a finding of OneDHS policy compliance by the ISCC clears the way for execution and signing of the ISAA, absent any other clearance requirements unrelated to the OneDHS policy. Once an ISAA has been signed, the ISAA originator is responsible for submitting a copy of the signed document to the IS&C so that it can be added to the ISAA interim Repository.

### ***ISAA Repository***

The ISAA Interim Repository is a database of legacy and recent domestic and international ISAAs – over 700 – between DHS and its external partners, maintained and managed by the IS&C Branch. The Repository is a useful resource for exploring the breadth of existing DHS external partnerships, identifying existing agreements that satisfy current data needs or as templates for future agreements. Access to the Repository is gained through the IS&C, whose staff is available to perform searches using multiple terms. Search requests should be sent to the IS&C at [ISAA@dhs.gov](mailto:ISAA@dhs.gov).

In FY 2010, Components will have the ability to perform searches independently using the Data Architecture Repository (DAR) within the DHS Enterprise Architecture Information Repository (EAIR). This web-based application, will house the ISAAs, along with other data assets, providing a searchable and updateable tool for the entire Department. Expect to hear more information about the DAR in the near future, to include training information. Until then, the IS&C remains available to assist with ISAA search requests.

### ***OneDHS Policy and ISAA Resources***

The most current comprehensive resource about ISAAs and the OneDHS policy is *ISAA Methodology Guidebook*, issued February 2008. The purpose of the ISAA Guidebook is to present appropriate policies, responsibilities and procedures, and other necessary information needed to develop, coordinate, approve, execute, catalogue, and negotiate disputes involving all ISAAs, in a, user-friendly manner. It sets forth definitions of relevant terms, a description of steps to take to develop, draft, and archive an ISAA, ISAA templates, and information about special circumstances such as OneDHS policy compliance exemptions and handing classified ISAAs. To obtain a copy of the *ISAA Methodology Guidebook*, contact the DHS Office of Information and Analysis, Information Sharing and Collaboration (IS&C) Branch at [issa@dhs.gov](mailto:issa@dhs.gov) or call (202) 282-9400. ***NOTE: The current Guidebook is currently being revised to more***

*effectively communicate the ISAA process, but remains the prevailing guidance until further notice.*

## **COAST GUARD IMPLEMENTATION OF THE “ONEDHS” REQUIREMENTS – ISAA REVIEW PROCESS**

Coast Guard guidance regarding the OneDHS ISAA review and implementation process will be addressed in the COMDTINST 5216.18 “Memoranda of Understanding/Agreement”. The modifications to the Commandant Instruction are underway, and will be finalized once revisions to the Guidebook have been completed.

### **ABOUT THE AUTHOR**

Ms. Hoffman-Moffatt is an attorney admitted to practice law in New York and Florida and holds a current USCG Merchant Mariner Credential (Masters License). Ms. Hoffman Moffatt has held a position in the USCG Headquarters Vessel Traffic Services Division and is currently a member of the Maritime Domain Awareness and Information Sharing Staff at USCG Headquarters.

### **KEY WORDS**

Information Technology, Interagency, Information Sharing, Agreements