Privacy Impact Assessment
for the

Maritime Awareness Global Network (MAGNET)

April 11, 2008

Contact Point
Frank Sisto
Chief, Data Analysis and Manipulation Division
U.S. Coast Guard
202-372-2795

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
703-235-0780

Abstract

The Department of Homeland Security (DHS) United States Coast Guard (USCG) has developed the Maritime Awareness Global Network (MAGNET) system. MAGNET will use information relating to vessels and activities within the maritime environment to accomplish the Coast Guard's missions in the areas of Maritime Safety, Maritime Security, Maritime Mobility, National Defense, and Protection of Natural Resources. MAGNET is a new system that will replace the existing integrated intelligence sharing system known as the Joint Maritime Information Element (JMIE) Support System (JSS). This PIA was completed because MAGNET will process personally identifiable information (PII).

Introduction

The Coast Guard is replacing an existing integrated intelligence sharing system known as the Joint Maritime Information Element (JMIE) Support System (JSS) to fulfill its duties and missions. The new system, Maritime Awareness Global Network (MAGNET) is being developed from this existing data sharing system. When fully operational, MAGNET will replace JMIE/JSS.

The legacy JMIE/JSS provides storage and access to maritime information and provides basic search capabilities either by a person or by vessel. Person searches may be conducted by passport or merchant mariner license number. Vessel searches may be conducted by vessel name, hull identification, or registration number. MAGNET will enhance JMIE/JSS capabilities by adding additional data sources, media storage, access capabilities, and infrastructure to provide rapid, near real-time data to the Coast Guard and other authorized organizations that need it. DHS, Coast Guard, and MAGNET users will have the ability to share, correlate, and provide classified/unclassified data across agency lines to provide Maritime Domain Awareness (MDA) critical to homeland and national security.

Taken together the information in MAGNET establishes MDA. MDA is the collection of as much information as possible about the maritime world. In other words, MAGNET establishes a full awareness of the entities (people, places, things) and their activities within the maritime industry. MAGNET collects the information described above and connects the information in order to fulfill this need.

Coast Guard Intelligence (CG-2)(through MAGNET) will provide awareness to the field as well as to strategic planners by aggregating data from existing sources internal and external to the Coast Guard or DHS. MAGNET will correlate and provide the medium to display information such as ship registry, current ship position, crew background, passenger lists, port history, cargo, known criminal vessels, and suspect lists. CG-2 will serve as MAGNET's executive agent and will share appropriate aggregated data on a need to know basis with other law enforcement and intelligence agencies.

MAGNET could relate to an individual in a few ways. As one example, MAGNET may collect information on individuals associated with ports, port facilities, and maritime vessels. Individuals may be passengers, crew, owners, operators, or any other employees in support of maritime businesses or other activities. The primary collection vehicle for personal information is through the Ships Arrival Notification System (SANS). Certain vessels, as defined in 33CFR160, are required to report arrivals to US ports and included is crew and passenger information. The SANS information is replicated into MAGNET.

MAGNET will also contain information about passenger ships that are required to report arrivals via SANS.

The MAGNET system receives data from several systems within DHS and outside of DHS (see specifically Question 1.2) through electronic transfers of information. These electronic transfers include the use of an Internet Protocol called Secure File Transfer Protocol (SFTP), delivery of data on CDROM or DVD-ROM, system-to-system communications via specially written Internet Protocol socket-based data streaming, database-to-database replication of data, electronic transfer of database transactional backup files, and delivery of formatted data via electronic mail.

Each data source provides its raw data through one of the transfer methods noted above. The data from these transfers are placed into files on the MAGNET Data Interchange Server. Each data source has a process that was designed specifically for that source that transforms the raw data into files that can be ingested by the MAGNET database. These files are then transferred by secure file transfer to the MAGNET Database Server. Various processes on the MAGNET Database Server detect the presence of these files and execute procedures that read the files and load the data into database tables that have been specifically built for each data source. As the data is loaded into the "source" tables, procedures, known as triggers, detect the changes to the "source" table causing the trigger to execute. The triggers then load the data into the various tables of the MAGNET database. During the loading of the data, each record is compared to the data within the MAGNET database and a determination is made on how to connect the records together. This process, known as correlation, allows related data to be logically connected together. MAGNET users only have access to the MAGNET database and do not have access to the "source" tables.

MAGNET will provide output to the Common Operating Picture (COP) as viewed using the Global Command and Control System, Integrated Imagery and Intelligence (GCCS-I3) platform. The COP is an integrated, or "common", view of the vessels operating in water that is important to the United States government, including geographic positions of the vessels, as well as, characteristics of the vessel. The COP is integrated (or "shared") amongst users of the GCCS-I3, which is commonly used within the USCG and the Department of Defense to monitor areas of operation. The output destined for the COP may be submitted to the Common Intelligence Picture (CIP) for review prior to the data being transferred to the COP. In addition, users will be able to run queries about specific vessels or tracks from a GCCS-I3 workstation and retrieve additional information from the MAGNET database. MAGNET will be able to accept input from the GCCS-I3 environment and process this data into the MAGNET database. This will allow MAGNET to accumulate position reports from the COP.

User Presentation and Use

The user is presented an interface that contains up to six tabs, depending upon the users level of access. The tabs are:

- Port View: Port view provides a specific port visualization of vessels arriving to the port for a specified time period. This will include data such as vessel name, date and time of arrival, registry flag and previous port. See question 1.1 for greater detail.
- Search: Search is for person, vessel, arrival and departure ports and cargo. These basic searches are based upon key words or fields.
- Advanced Search: Advanced search provides the ability to incorporate Boolean[1] searches across multiple fields.

[1] Search terms plus results modifiers of "and", "or", or "not."

- GIS Viewer: GIS Viewer display, in a geospatial presentation, displays vessel location in a user selected area.
- Administration: The administration section is for the creation, deletion and overall management of MAGNET users.
- Coastwatch Vessel Identification and Passenger Reporting (CVIPR): CVIPR is used to support the business processes around vessel and passenger threat assessments such as watchlist check or checking what vessels come from foreign ports.

MAGNET will provide access to the database via workstations located throughout the world. The system will be accessible on multiple networks at different classification levels. It is expected that the workstations, as provided by the user agency, will be equipped to access the appropriate networks with current Internet-style applications and/or browser technology. Users at the workstations will query the system on-line using either pre-stored, parameterized queries or queries built ad hoc by the users. Full Boolean search logic will be supported. Results of database searches will be returned on-line to the users for viewing and/or processing at their workstations.

MAGNET will allow users to create 'alert' profiles expressing interest in particular sets of maritime data and will store, modify, and delete these profiles at user direction. The profiles will be used by the system to automatically monitor incoming data and notify the users when data meeting their interest criteria has arrived.

Capabilities will be provided to view the results of queries and alerts at the workstations in several formats. These will include pre-defined data output forms or reports, spreadsheet formats, and location plots against background shoreline maps. It will be possible to easily retrieve data from the database into any of these presentation formats. Additionally, the system will support the use of local workstation capabilities to allow further manipulation and processing of downloaded information.

MAGNET will support three types of inter-user communications: electronic mail for message exchange, electronic bulletin board for posting of common interest notices, and file transfer for transmission of large volume data.

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

MAGNET collects information on ports, port facilities, and maritime vessels (including their characteristics and cargo), arrival and departure information, and suspicious activity information.

Ports and Port Facilities

Port and facility records consists of information including: location, commodities handled, equipment, certificates, approvals, inspection data, pollution incidents, casualties, and violations of all laws and international treaties, if applicable, and information pertaining to individuals, companies, and organizations associated with those facilities such as owners, operators, managers, and employees (name, company name, position/title at company, and whatever identifying information the company may

provide, for example, passport number, employee identification number, or social security number (if available).

Maritime Vessel Information

Martime vessel information includes vessel information, where the vessels are located (position reports), arrival notifications, departure notifications, cargo manifests, and lists of suspect vessels.

The vessel information includes the vessel name, vessel identification and registration data, the nationality of the vessel (where the vessel is registered), vessel characteristics (weights, lengths, breadth, depth, etc.), ownership (name, address, telephone number), performance characteristics (number of engines, type of engines, type of hull, fuel type, etc.), cargo carrying characteristics (number of holds, hold capacities, number of cranes, etc.), and other characteristics that help describe the vessel. Vessel information may also associate information. Associate information includes but is not limited to data pertaining to people or organizations associated with vessels, owners, passengers, and crew members. Basic associate information would include location (place of business, address), access or contact (phone and fax numbers) and identification (name). Additional information may be collected on associates during the course of a law enforcement activity to include additional identification information (social security number or passport number).

The vessel position reports include the latitude and longitude of the vessel, the date and time of the position report, the vessel's name and one or more identification numbers, characteristics of the vessel at the time of the report (length, the nationality of the flag it is flying, color of the hull, etc), and other movement information.

The vessel cargo manifests include a list of the commodities that are being imported or exported from a given port, where the cargo originated, the destination of the cargo, the name of the company or person shipping the cargo, the name of the person or company receiving the cargo, the name of the person or company that should be notified when the cargo arrives, the specific amount of the cargo, the port at which the cargo is being shipped, the date and time at which the cargo will be shipped, the container identification number(s) of the container(s) that hold the cargo, and the name of the vessel that will be shipping the cargo.

Arrival and Departure Information

The arrival notifications and departure notifications include the name of the vessel, one or more identification numbers, the port at which the vessel will arrive, the estimated date and time of arrival, the estimated date and time of departure, crew manifest (name, position (job), identification, when and where the crew member boarded the vessel), the passenger manifest (name, identification, when and where the passenger boarded the vessel), points of contact used to verify the information being supplied in the notification, a general description of the cargo that is on board, and a list of any specific dangerous cargo that is on board.

Suspicious Vessel and Person Information

Records involving vessels and associates which are known, suspected, or alleged to be involved in contraband trafficking, illegal migrant activity (smuggling, trafficking, and otherwise), or terrorist activity consists of vessel name, registry flag, home port and vessel identification number (ship control number, vessel registration number or hull number). If known, last port and next port may be included.

Information on individuals, associated with vessels, facilities (including platforms, bridges, marinas, terminals, and factories), and/or Coast Guard activities. This information will include name, nationality, address, telephone number, and taxpayer or other identification number (such as social security number, if available); date of birth, relationship to vessels and facilities; their relationship to other individuals, companies, government agencies, and organizations in MAGNET; their involvement in pollution incidents, and violations of all laws and international treaties. An example of relationship data is if a cook and a captain are reported as crew members on the same notice of arrival, those two people would have a 'relationship'. Information on any casualty associated with a vessel or facility will also be collected. This information will include name and circumstances of death, at a minimum.[2]

MAGNET will also collect the following reports and records:

Reports submitted by Coast Guard crews relating to boardings, over-flights, or other means of surveillance as well as any violations of the United States (U.S.), international law or treaties, along with enforcement actions taken during boarding. Such reports and activities could contain electronic documents, photographic, and video data as well as names of passengers on vessels, owners, crew members and agents (name and address of agent, company represented, and what type of agent it is (co-signee, shipping agent, e.g.).

Records involving vessels, passengers, and associates which are known, suspected, or alleged to be involved in contraband trafficking, illegal migrant activity (smuggling, trafficking, and otherwise), terrorist activity, or other unlawful activity within the maritime domain.

1.2 From whom is information collected?

The MAGNET system receives information from multiple systems operated by the Coast Guard and the Navy, as well as specific reports from a commercial company that provides cargo information to the maritime shipping industry, and the Departments of Motor Vehicles list of registered boats from some of the State governments. It is the intention of the Coast Guard to include additional sources of information that have not yet been identified and to allow users of the system to store textual remarks about the data. This functionality has not been implemented at this time but once implemented this PIA will be updated. At present, MAGNET receives data from the following systems:

U.S. Coast Guard's Ship Arrival Notification System (SANS)

U.S. Coast Guard's Marine Information for Safety for Law Enforcement (MISLE)

U.S. Coast Guard's National Automated Identification System (NAIS)

U.S. Coast Guard's Common Operating Picture (COP)

U.S. Navy's Sea Watch System

U.S. Navy's Merchant Ships Characteristics (MSC) System

U.S. Customs and Border Patrol's Daily Hazardous Cargo Reports

A Commercial Company providing Cargo Manifests (Company name is protected)

[2] Death at sea information is required to be reported by the Center for Disease Control (CDC). CDC may ask for more information if it is available.

State of California

State of Florida

State of Alaska

State of Delaware

State of Hawaii

The vessel information is obtained from the Coast Guard, the Navy, and the Departments of Motor Vehicles list of registered boats from some of the State governments (not all states choose to provide their information).

The position reports are obtained from the Coast Guard, the Navy, and from information contained within the cargo manifests, arrival notifications, and departure notifications.

The arrival and departure notifications are obtained from the Coast Guard's National Vessel Movement Center (NVMC).

The cargo manifests are obtained from commercial companies that specialize in providing this type of information.

MAGNET users have access to commercial data through the MAGNET interface. The commercial data accessed is provided specifically for MAGNET users to resolve gaps or discrepancies in existing data.

Currently MAGNET also receives information from the Coast Guard and Navy Department. In the future we will like to establish data contributions from other Intelligence Community agencies.

1.3 How is the information being collected?

The MAGNET system receives data from the systems identified in Section 1.2 through electronic transfers of information. These agencies and organizations collect their information either directly from individuals (in the case of States' departments of motor vehicles, or from law enforcement or safety/rescue actions (in the case of USCG, Navy, and CBP). These electronic transfers include the use of an Internet Protocol called SFTP, delivery of data on CDROM or DVD-ROM, system-to-system communications via specially written Internet Protocol socket-based data streaming, database-to-database replication of data, electronic transfer of database transactional backup files, and delivery of formatted data via electronic mail.

1.4 Why is the information being collected?

Coast Guard's mission requires the collection of data associated with maritime security and operations. As Coast Guard replaces the LMIE/JSS), MAGNET will be capable of complex data processing and handling. Coast Guard uses this information to establish MDA. DHS, Coast Guard, and MAGNET users will have the ability to share, correlate, and provide classified/unclassified data across agency lines to provide MDA critical to homeland and national security.

MDA is the collection of as much information as possible about the maritime world, in other words, full awareness of the entities (people, places, things) and their activities within the maritime industry.

1.5 What specific legal authorities/arrangements/agreements define the collection of information?

Maritime information has been critical to this nation's defense and success since its founding. The collection of information for MAGNET is authorized by; 14 U.S.C. 2, 14 U.S.C. 89; 46 U.S.C. 3717; 46 U.S.C. 12501; 33 U.S.C. 1223 The Espionage Act, The Magnuson Act, The Ports and Waterways Safety Act (PWSA), The Maritime Transportation Security Act of 2002 (MTSA), Pub L. 107-295 The Homeland Security Act of 2002, Pub L. 107-296; National Presidential Security Directive 41 (NPSD), United States Coast Guard, 33 CFR Part 160.

1.6 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

The first risk identified was the potential for over-collection of information, that is, to collect more information than is necessary for Coast Guard to complete its mission. MAGNET is designed to provide a total awareness for maritime officers and officials. Fulfillment of this goal requires a large amount of information. However, as indicated in Question 1.1 and the Introduction, information is limited to that information which would be relevant to the maritime sector. This helps to mitigate any risks associated with the collection of a large amount of information.

The second privacy risk identified was the disclosure of PII to unauthorized recipients. To mitigate this risk, access controls were implemented within the system and the database to limit access to the PII data elements. Specifically, the use of Oracle Corporation's Label Security and Fine Grain Auditing products were installed and configured to maintain access control within the database. Oracle Label Security is used to protect PII data by automatically filtering data by user access level. Fine grain auditing is used to record all users and queries that access PII data. All users of the system must sign an agreement to protect the data, and are not granted access until the signed form is provided.

A third privacy risk is presented by commercial data being available to MAGNET users. This risk is mitigated by several factors. First, commercial data is used to resolve gaps or discrepancies in existing MAGNET data; all searches of commercial data are predicated on existing data and interests. Second, all commercial data accessed by MAGNET users is stored separately and tagged as a commercial data source. This is done to preserve the integrity other USCG information.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

The purpose of MAGNET is to facilitate the sharing of maritime data among its constituents and to cost-effectively optimize the utility of the maritime information in support of the various maritime missions within the USCG, as well as other government agencies. Although specific uses of each piece of information are too numerous to name, the uses can be divided into several categories and sub-categories. These use categories include:

1. **Maritime Safety**
    a. Search and Rescue
    b. International Ice Patrol
2. **Protection of Natural Resources**
    a. Marine Pollution Enforcement & Response
    b. Living Marine Resource Enforcement & Response
3. **Maritime Mobility**
    a. Lightering Zone Enforcement
    b. Foreign Vessel Inspection
4. **Maritime Security – Homeland Security**
    a. Drug Interdiction
    b. General Enforcement of Laws and Treaties
    c. Alien Migrant Interdiction
5. **National Defense**
    a. Homeland Security
    b. General Defense Operations
    c. Maritime Interception Operations
    d. Military Environmental Defense Operations
    e. Port Operations, Security & Defense
    f. Peacetime Military Engagement
    g. Coastal Sea Control

The commercial data accessed is provided specifically for MAGNET users to resolve gaps or discrepancies in existing data.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

As described in the introduction, MAGNET uses a process known as correlation to connect information from more than one source into a single record or set of records. The correlation process involves comparing elements of identification, such as the vessel name or the official registry number, from the information being processed for inclusion into the database to the records already within the database. If the identification information matches, then the incoming information is used to fill in the blanks in the record stored in the database. For example, if new information is received about a person that contains driver's license number, then the driver's license number would be added to the record in MAGNET, if that information was not previously stored. This process allows the MAGNET system to "build up" the information related to a specific ship with having to use resources accessing the information multiple times with multiple queries from multiple users.

The MAGNET system also allows its users to formulate queries into the database. Although the system does not analyze the data directly for unknown areas of note, concern, or pattern, the users may query the system through their ability to formulate queries and the user may personally analyze the results of those queries. The analysis of query results is not automated, and all searches are predicated on a need to know for a relevant or ongoing analysis.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

The MAGNET system does not check the data for accuracy. Because the MAGNET system and its supporting personnel do not interact directly with individuals to collect PII data on individuals, there is no opportunity for MAGNET users to verify accuracy with the individuals.

Data and records within MAGNET subject to the Privacy Act come from a multitude of sources and agencies. Accuracy of the data is solely based on the quality MAGNET sources. Once source systems are updated with new or correct information MAGNET will also be updated.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

MAGNET uses Oracle's Label Security to ensure PII data is only available to appropriate need to know agencies. MAGNET uses Oracle fine grain auditing to record queries run against U.S. persons. Each user of the system is required to sign a user agreement to protect the data. Memorandums of Agreement (MOU's) are established with all of the agencies that provide data to the MAGNET system. As noted in Section 8.0 the user groups and access controls utilized in MAGNET help mitigate the risk of misuse.

Additionally there exists a risk of inaccurate data being used as source data for MAGNET. However, Coast Guard accepts the risk inasmuch as the source systems utilized by MAGNET will be updated once new or more accurate information is obtained. Once the source systems are updated, so will to will MAGNET.

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

Dynamic information on vessel position(s) and movement(s) will be stored for not more than ten (10) years but may be reduced in detail to comply with media storage procedures and requirements. Other information such as characteristics, identification status and associate records is updated to remain current and is retained for twenty (20) years.[3] The requirements supporting the collection and storage of data are

[3] "Associate" record in this response means any person associated with the maritime domain. This includes but is not limited the aforementioned crews, associates, employees, agents, passengers, and persons of interest to law enforcement or intelligence.

reviewed regularly. Records will be kept accessible online for three (3) years then archived offline within MAGNET to support ongoing investigations or law enforcement activities.

Audit records, maintained to document access to information relating to specific individuals, are maintained for five (5) years or the life of the MAGNET whichever is longer. Access to audit records will only be granted to authorize personnel.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

The MAGNET Records Management Disposition schedule (SF115) was drafted and submitted by the USCG Records Officer to NARA for review and approval. The schedule has been registered under N1-026-08-1 and is currently being appraised by NARA. No records will be destroyed until the records schedule is approved by NARA.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

Information is needed for the period specified to continuously analyze data. Maintaining this data as directed allows for trend analyses. The periods described above aligns with not only MAGNET's mission requirements but also the policy that information retention should be kept to the minimum necessary to fulfill mission duties.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

The information collected by and maintained in MAGNET may be shared with all component agencies within DHS on a need to know basis consistent with the component's mission. This may include any information listed in the Introduction and Section 1.0 of this PIA. USCG currently shares information within Coast Guard (internally). As MAGNET grows we are expected to make our database available to other DHS agencies including but not limited to Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), and Intelligence and Analysis (I&A). Any organization that has a need for maritime information will be evaluated; normally, however, records containing PII will only be shared with organizations with law enforcement authority, i.e. MAGNET data may be shared with Customs and Border Protection (CBP) once a need to know has been established. An official MOU is in place for sharing with CBP however sharing has not commenced.

4.2 For each organization, what information is shared and for what purpose?

General information pertaining to the maritime domain detailed in Question 1.1 may be shared with any organization as defined in Question 4.1, for homeland and national security. More frankly, if a sharing partner establishes a need to know information within MAGNET the information may be shared. Normally, however, records containing PII may only be shared with organizations with law enforcement authority.

4.3 How is the information transmitted or disclosed?

Information is shared and disclosed via secure web-based browser over the classified Secret Internet Protocol Routed Network (SIPRNet).

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

In order to mitigate the privacy risks of PII being inappropriately used, the information is shared only with DHS personnel who have a need to know the information as part of the performance of their official employment duties. Internal DHS access to USCG data is controlled by USCG through the use of strict access controls for the users, passwords, background checks for individuals accessing the data, as well as system audits that track and report on access to the data. Additionally, any individual with access has gone through privacy training.

Section 5.0 External Sharing and Disclosure

5.1 With which external organizations is the information shared?

Externally MAGNET currently shares information with the Navy Department. As MAGNET grows it is expected that the database will be made available to other agencies. In the future MAGNET will share information with any U.S. law enforcement or intelligence organization (Federal, state, or local) that has an official need for maritime information. Records containing PII, however, will only be shared with organizations with law enforcement authority. Additionally, any sharing of PII will be compatible with the purpose stated in the MAGNET system of records notice.

5.2 What information is shared and for what purpose?

General information pertaining to the maritime domain detailed in Question 1.1 may be shared with any organization that has a need for maritime information. Records containing PII will normally only be shared with organizations with law enforcement authority for homeland and national security purposes. Any additional sharing of PII will be compatible with the purpose and routine uses stated in the MAGNET system of records notice.

5.3 How is the information transmitted or disclosed?

Information is shared and disclosed via secure web-based browser or secret internet protocol routed network.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

A MOU is in place with the Navy for access on the SIPRNet. The SIPRNet is a system of interconnected computer networks used by the U.S. Department of Defense and the U.S. Department of State to transmit classified information (up to and including information classified SECRET) by packet switching over the TCP/IP protocols in a "completely secure" environment. It also provides services such as hypertext documents and electronic mail.

5.5 How is the shared information secured by the recipient?

Specific operating rules to ensure compliance with national policy are reflected in each site's Standard Operating Procedures. These rules include specifications to access records containing information on U.S. persons are as follows:

1. Only authorized personnel may access such records.
2. These records are used only for official business.
3. Each access to such records will be entered into audit records which are maintained for five (5) years or the life of the system, whichever is longer.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

No training is required for any users outside of USCG.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

Within the MAGNET system, the only privacy risk identified was the disclosure of PII to unauthorized recipients. To mitigate this risk, access controls were implemented within the system and the database to limit access to the PII data elements. Specifically, the use of Oracle Corporation's Label Security and Fine Grain Auditing products were installed and configured to maintain access control within the database. PII data within MAGNET is shared with users outside of DHS, and access to the data is restricted using the access control features described above.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

MAGNET's data and records are a compilation of many sources. MAGNET and its supporting personnel do not interact directly with individuals to collect PII data. However, through the publication of this PIA and the MAGNET System of Records Notice (SORN) to be published in the Federal Register and the legacy Privacy Act data regarding JMIE/JSS (59 FR 40402, August 8, 1994) notice has been provided.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

No. MAGNET does not collect information directly from individuals rather it receives data from databases/sources which are the primary collectors.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

No. Individuals may address consent issues with the source systems that collect information but MAGNET itself does not provide a mechanism for consent to use. However, MAGNET is confined to the uses described in this PIA and the relevant SORN.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

MAGNET is not a primary collector of information and is not in the best position to give notice of collection. This PIA and the SORN covering MAGNET provide notice that DHS operates this system of records.

Section 7.0 Individual Access, Redress and Correction

7.1 What are the procedures which allow individuals to gain access to their own information?

The JMIE/JSS SORN provides instructions for someone to access their record(s) of information. Legacy Privacy Act data regarding JMIE/JSS can be found in 59 FR 40402, August 8, 1994.

The JMIE/JSS SORN will be replaced by the MAGNET SORN and Notice of Proposed Rulemaking (NPRM) which will be published in the Federal Register concurrently with this PIA being published on www.dhs.gov/privacy.

7.2 What are the procedures for correcting erroneous information?

As detailed in the SORN and NPRM, MAGNET is exempted of certain provisions of the Privacy Act. Nonetheless, USCG will examine each separate request on a case-by-case basis, and, after conferring with the appropriate component or agency, may waive applicable exemptions in appropriate circumstances and where it would not appear to interfere with or adversely affect the law enforcement or national security purposes of the systems from which the information is recompiled or in which it is contained. Individuals should write to the following address with information requests: Department of Homeland Security United States Coast Guard (MAGNET Executive Agent), Intelligence Directorate, Office of ISR (CG-26), 2100 2nd Street, SW, Washington, DC 20593-0001.

7.3 How are individuals notified of the procedures for correcting their information?

The SORN and this PIA provide notice of the procedures.

7.4 If no redress is provided, are alternatives available?

As noted above, USCG will review any information request on a case-by-case basis.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

MAGNET is not in the best position to give redress for inaccurate information or provide access to records because is not a primary collector of information and is a sensitive but unclassified (SBU) to Top Secret system. As noted in Section 2.0 MAGNET is regularly updating information received from information sources. This ensures that MAGNET has the most accurate information available to its sources.

However, this means that the sources systems noted above and not MAGNET are in the best position to change information. Information changes in the sources systems will affect change in MAGNET.

MAGNET is also exempted from certain provisions of the Privacy Act regarding access and redress. Nonetheless, USCG will examine each separate request on a case-by-case basis, and, after conferring with the appropriate component or agency, may waive applicable exemptions in appropriate circumstances and where it would not appear to interfere with or adversely affect the law enforcement or national security purposes of the systems from which the information is recompiled or in which it is contained.

Section 8.0 Technical Access and Security

8.1 Which user group(s) will have access to the system?

Within the structure of the database, users will be added to one of two user groups, Law Enforcement (LE) and Intelligence Community (IC). Determination as to which group a use is added is based upon the organization from which the user is requesting access and the function of the position. Users performing National Intelligence work will be in the IC user group, all other will be in the LE.

MAGNET is unique in that it has been designed to store its information within multiple security levels for SBU, Confidential, Secret, and Top Secret data. MAGNET will provide users with the appropriate security clearances and with a need to know access to the data at the highest level for which their security clearance will allow, and will merge the data at higher security levels with data provided at lower security levels, such that any user of the system will only need to access the system at a single point in order to have access to all of the data to which they are entitled. The multiple levels of security provide a more robust set of information to the users of the system.

8.2 Will contractors to DHS have access to the system?

Yes.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes, the MAGNET system uses Oracle database roles and the features of Oracle Label Security to apply those roles to the users of the system. The roles established in the system have been designed to control whether or not a user may see PII data or not. Additional roles have been established for operating and maintaining the MAGNET system that include access to all of the information within the system. These "system" level roles are strictly controlled by the staff that operates the MAGNET system.

8.4 What procedures are in place to determine which users may access the system and are they documented?

A "new user" request form is used by prospective users to request access to the system. The "new user" request form is available through the MAGNET Graphical User Interface, which has been

implemented as a web-site. The "new user" request form is a read-only PDF that must be downloaded and printed by any interested party wanting access to MAGNET. Once the party fills out the request, the form is faxed to the MAGNET customer service office. The customer service office will verify via a phone call all information on the request and create a user account according to the needs of the party. There is a two person review of the information contained on the form by their management and MAGNET staff prior to granting access to MAGNET. Only person with a need to know and who have the appropriate background check, security clearance and have completed the annual privacy training will be granted access.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

The roles and rules used within the MAGNET system were verified during system testing prior to each release of the system. The assignment of the roles is verified by the MAGNET staff prior to granting access to MAGNET. Accounts are reviewed on a regular basis to ensure users are re-vetted and are active users. USCG analysts and officers leaving duty where MAGNET access is required have their accounts immediately deactivated.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

Oracle's Label Security is used to control access to PII data (whether or not a user can view the data). Oracle database roles are used to control read-write access to the database (whether or not a user can change the data). Oracle's Fine Grain Auditing is used to track queries run against PII data and who makes changes to this data.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

The MAGNET Project does not provide training specific to the use of this system. The Coast Guard provides general training for Coast Guard personnel users which consist of security and privacy training, among other law enforcement and intelligence specific training.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. MAGNET received an Authority to Operate on July, 28, 2006 for its classified operations per the System Security Authorization Agreement and Department of Defense Information Technology Security Certification and Accreditation Process. The unclassified version of MAGNET is currently undergoing accreditation and anticipates an ATO approximately May, 2008.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Within the MAGNET system security, one privacy risk identified was the disclosure of PII to unauthorized recipients. To mitigate this risk, access controls were implemented within the system and the database to limit access to the PII data elements. Specifically, the use of Oracle Corporation's Label Security and Fine Grain Auditing products were installed and configured to maintain access controls within the database.

Another privacy risk identified was unauthorized access to the system. The controls detailed in Section 8.0 mitigate much of the risk of unauthorized access to MAGNET. By controlling access to MAGNET and categories of information within MAGNET, Coast Guard can ensure that unauthorized access and misuse of data are significantly mitigated.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

The MAGNET system was developed from the ground up using a combination of system software, database management software and custom written software. The uniqueness of the system and the community it serves eliminated the possibility of purchasing the system off-the-shelf.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

The MAGNET system is intended to exist within multiple security domains. As such, the integrity of the data, the ability to see the PII data, and the security of the system has been integral throughout all stages of system development. Although no specific procedures were used to ensure compliance with the requirements for handling PII data, the MAGNET system was designed, developed and tested to be operated with classified data, which includes rigorous testing of data access control measures.

9.3 What design choices were made to enhance privacy?

Oracle Label Security, Oracle Fine Grain Auditing, and data base roles were used to protect the data. This PIA was conducted prior to the move from Joint Regional Information Exchange System (JRIES) into the full MAGNET package to ensure MAGNET's operational capacity and privacy safeguards were reviewed.

Conclusion

As the Nation's primary maritime law enforcement agency, the Coast Guard has statute authority and responsibility for (1) Maritime Safety, (2) Maritime Mobility, (3) Maritime Security, (4) National Defense, and (5) Protection of Natural Resources. This Program is designed to support and coordinate these five missions and in particular, new homeland security requirements enacted after the events of September 11, 2001. In choosing whether to update/upgrade the existing JMIE/JSS infrastructure the choice was simple. Due to technological obstacles and new system requirements, it was quickly established that the legacy system could not support today's needs. Newer technology allows for better, broader, and more near real-time support to the personnel (internal/external to the Coast Guard) tasked with securing the Nation through the maritime domain.

Responsible Officials

Frank Sisto
Chief, Data Analysis and Manipulation Division

Approval Signature Page

Original signed and on file with the DHS Privacy Office

Hugo Teufel III

Chief Privacy Officer
Department of Homeland Security