APPENDIX I

FEDERAL MARITIME COMMISSION
PRIVACY IMPACT ASSESSMENT

A. SYSTEM INFORMATION

1. What is the system name?

Datawatch Systems

2. Why is the information being collected (e.g., to determine eligibility)?

The information is being collected to enhance building security. The Datawatch system is a Commercial, Off-The-Shelf (COTS) product that is used to administer physical access authorizations for the Federal Maritime Commission (FMC) Headquarters (HQ), 800 North Capitol St. NW, Washington, DC, identified as a Level IV facility in accordance with the Interagency Security Committee Security Standards Level of Security.

3. What is the intended use of the information (e.g., to verify existing data)?

To issue Proximity Access Cards (cards/fobs) to FMC HQ employees and contractors.

4. Does this system contain any personal information about individuals? (If no, a PIA is not required. Complete a Privacy Impact Analysis.)

There are access control devices or readers to allow entry into FMC HQ spaces. This access is granted via the card/fob or through the use of the employee's Personal Identity Verification Cards (i.e., HSPD-12 cards issued by GSA).

The cards/fobs are identified by unique card/fob numbers, which are assigned to employees or contractors. Cards/fobs are assigned using only employee first and last names and their bureau/office (or identification as "Contractor") assignment. No other personal information (i.e. SSN or Employee Number) is associated with the individual card/fob number. These identifiers are stored for access control only.

The Personal Identity Verification (PIV) card will soon be required for all Federal employees and contractors to gain physical and logical access to government resources. The PIV card will be used for access to secured buildings as well as to access computer resources. PIV cards (issued by GSA) contain personal information within them. However, FMC will only use the employee's (or contractor's) name and bureau/office assignment as authentication for access to FMC facilities.

The following PIA covers only the access control system.

5. What legal authority authorizes the purchase or development of this system/application? (List the statutory provisions or Executive Orders that authorize the maintenance of this information to meet an official program mission or goal.) Also list the OMB Clearance number and expiration date, if applicable.

Executive Order 12977; Executive Order 13286

Homeland Security Presidential Directive 12 (HSPD-12), August 12, 2004

Physical Security Criteria for Federal Facilities. Department of Homeland Security, Interagency Security Committee, 2010.

Use of Physical Security Performance Measures. Department of Homeland Security, Interagency Security Committee, 2009

FAR Subpart 4.13 and FAR 52.204-9 (Clause), *Personal Identity Verification of Contractor Personnel*

6. For new systems, describe how privacy is addressed in documentation related to system development, including as warranted and appropriate, statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and especially, the initial risk assessment.

It is the FMC's responsibility to assure the physical protection of its facilities and the safety of the employees, contractors and visitors to the FMC HQ. Security of federal facilities includes physical security assets such as closed-circuit television cameras, barrier material, and security guards.

The proximity devices/readers are not a new system and have been in place for more than 10 years. However upgrades have been made to the existing system to comply with HSPD 12.

An analysis and assessment of risk has been used to determine the following information:

- What is the FMC protecting: (i.e., personnel, property, & resources)
- Who are potential adversaries: (i.e., the public, related industry, & possible staff)
- How is the FMC vulnerable: (i.e., unlawful, inappropriate access to agency policy decisions, materials, accountable personal property, secure IT systems, etc.)
- What are the FMC's priorities: (i.e., personnel safety, secure property, information & resources control, etc.)
- What can the FMC do to manage physical security: (i.e., obtain security guards, limit & control access, etc.)

B. DATA IN THE SYSTEM

1. What categories of individuals are covered in the system (for example, employee, contractor, public, etc.)?

FMC employees and contractors

2. What are the sources of information in the system?

a. Is the information collected directly from the individual or is it taken from another source? If Information is not collected directly from the individual, describe the source of the information.

The FMC's Office of Human Resources (OHR) provides the first and last name of the employee along with their assigned office/bureau, and a start date. OMS will enter the information into the Datawatch system, designate an access level (based on their office/bureau assignment), and supplies a card/fob to OHR for them to issue to the employee.

Once the employee has been issued a PIV card by GSA, OHR will inform OMS, and provide five-digit PIV card number for OMS to enter into the Datawatch system for activation.

For FMC Contractors, OHR provides the first and last name of the contractor along with the office/bureau the contractor is working with, and a contract start and end date. OMS designates the access level (based on their office/bureau assignment) and supplies a card/fob to OHR for them to issue to the contractor.

b. What Federal agencies provide data for use in the system?

None

c. What state and local agencies provide data for use in the system?

None

d. What other third parties will data be collected from?

None

e. What information will be collected from the employee and the public?

OHR has the responsibility of collecting information from employees. OMS has the responsibility of collecting information from contractors. Name and office/bureau assignment are collected from both employees and contractors.

3. How does the FMC ensure that data are sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations about any individual?

a. How is data accuracy ensured?

OHR has the responsibility of collecting and verifying employee information in accordance with CFR 5, *Administrative Personnel*. OMS has the responsibility of collecting and verifying information from Contractor in accordance with CFR 48, *Federal Acquisition Regulation System*.

b. How will data be checked for completeness?

For employees, OHR checks for completeness in accordance with CFR 5, *Administrative Personnel*. For contractors, OMS checks in accordance with CFR 48, *Federal Acquisition Regulation System*.

c. Are the data current? What steps or procedures are taken to ensure the data are not out of date?

OMS runs routine reports to ensure that employee and/or contractor information is up to date, and removes any employees or contractors no longer eligible for access to FMC facilities.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

No, the data elements are outlined per the Datawatch Systems' requirements for card/fob activation. Reports are prepared based on dates and/or time frames, or by names or numbers. Offices and bureaus may request reports on their physical areas and reports are provided in PDF format for this purpose.

e. How will data collected from sources other than FMC records be verified for accuracy?

For employees, OHR will verify data for accuracy in accordance with CFR 5, *Administrative Personnel*. For contractors, OMS verifies in accordance with CFR 48, *Federal Acquisition Regulation System*.

4. Describe what opportunities individuals have to decline to provide information (that is, where providing information is voluntary) or to consent to particular uses of information (other than required or authorized uses), and how individuals can grant consent.

OHR has the responsibility for collecting employee information and will take appropriate action if/when employees decline to provide required information.

Contractors declining to provide any required information can be deemed ineligible for participation in FMC acquisitions.

C. ATTRIBUTES OF THE DATA

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

The data collected is both relevant and necessary to ensure the security of the FMC HQ facility. It is the Federal Government's responsibility to assure the physical protection of its facilities and the safety of employees and visitors in their Federal space.

2. Will the system derive new data or create previously unavailable data about an individual through the aggregation of information collected? (If no, skip to D.3.)

No

3. Will the new data be placed in the individual's record?

No

b. Can the system make determinations about employees or the public that would not be possible without the new data?

No

c. How will the new data be verified for relevance and accuracy?

NA

4. Do the records in this system share the same purpose, routine use, and security requirements?

Yes. All data is used to allow access to FMC HQ facilities based on an access level, and to protect FMC assets and reduce the impact of their potential loss. Included among the assets of FMC HQ facilities are the physical safety and peace of mind of the occupants, the value of the structure itself, and the importance of the mission of the bureaus/offices housed at FMC HQ.

a. If the data are being consolidated, what technical, management, and operational controls are in place to protect from unauthorized access or use? Explain.

Data is accessed, entered or modified only by an authorized user of the Datawatch System. The Datawatch system is a password-protected portal only for authorized users within FMC. The Director of OMS is charged with providing authorized access to the Datawatch system.

b. If processes are being consolidated, are the proper technical, management, and operational controls remaining in place to protect the data and prevent unauthorized access? Explain.

No processes are being consolidated.

5. How will the data be retrieved? Can a personal identifier be used to retrieve data? Are personal identifiers used to retrieve data on a routine, occasional, or ad hoc basis? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Data is retrieved only through the Datawatch system, a password-protected portal. No personal identifiers, other than those identified above (name and office/bureau), are stored in or can be retrieved through Datawatch.

Reports may be prepared on a routine, occasional, or ad hoc basis to identify employees and contractors, by name and badge number, entering portals or areas secured by the proximity card readers.

6. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

Reports prepared on individuals include name, card/fob number, and access level. The use of the reports will be for identifying/verifying users of the system. OMS will have access to these reports. Reports can be prepared to identify entry by card number, employee name, reader (portal), or panel.

D. MAINTENANCE OF ADMINISTRATIVE CONTROLS

1. If the system is hosted and/or used at more than one site, how will consistent use of the system and data be maintained at all sites?

The system is hosted offsite by Datawatch, and not by FMC.

2. What are the retention periods of the data in this system?

Currently, there is no retention period of the data.

3. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

There are no defined procedures for disposition of data. Reports produced are kept for varying lengths of time.

4. Is the system using technologies in ways that the FMC has not previously employed (for example, monitoring software, CallerID)? If yes, how does the use of this technology affect public/employee privacy?

No. FMC has used the Datawatch System since occupying the HQ building at 800 North Capitol Street, NW, e.g., since August 1992.

5. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

The system will provide the capability to identify badges used for entry at secured portals throughout FMC HQ. There is no capability to locate and monitor individuals prior to the badge swipe at the portal. The system is utilized to secure FMC resources, not monitor the movement of individuals.

a. What kinds of information are collected as a function of the monitoring of individuals?

NA

b. What controls will be used to prevent unauthorized monitoring?

Datawatch is a password-protected system. Only the System Coordinator, or individuals authorized by the Director of OMS have access to the system.

6. Under which Privacy Act systems of records notice does the system operate? Provide name and number.

NA

7. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

NA

E. ACCESS TO DATA

1. Who will have access to the data in the system (for example, contractors, users, managers, system administrators, developers, other)?

Only the System Coordinator, or individuals authorized by the Director, OMS, will have access to the system.

2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

The only way to access the system is by having a registered user name/password with Datawatch Systems. The Director of OMS provides authorization to Datawatch Systems for an individual to obtain a user name/password. One must follow the user name/password set-up procedures on the Datawatch web site. Only FMC employees may register as users of the system.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.

Only authorized OMS personnel will have access to the data on the system.

4. What controls are in place to prevent the misuse (for example, unauthorized browsing) of data by those having access? List procedures and training materials.

Currently, only two individuals have access to the system. By limiting access to these two trusted individuals, misuse concerns are mitigated. Additionally, very limited information is available in the system.

5. Are contractors involved with the design and development of the system and/or will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

The Datawatch system is a COTS product, designed, developed and maintained by Datawatch Systems, Inc. Datawatch System's GSA Contract contain both FAR 52.224-1 - PRIVACY ACT NOTIFICATION (APR 1984), and 52.224-2 - PRIVACY ACT (APR 1984) clauses.

6. Do other systems share data or have access to the data in the system? If yes, explain.

No. Datawatch is a "stand alone" system, and does not share data with any other system.

7. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

NA

8. Will other agencies share or have access to the data in this system? If yes, list agencies.

No other agencies will have access to the data in the system. Currently there are no other agencies that share data in this system; however, as FMC does not occupy all space on floors secured by access panels, in the event another federal agency occupies proximate space, OMS will be responsible for collecting the information on the employee or contractor requiring access and will issue them an access card/fob.

9. How will the data be used by the other agency?

Agencies may request access reports of employees' or contractors' within their agency only.

10. Who is responsible for ensuring proper use of the data?

The Director of OMS will be responsible for ensuring proper use of other agency's data.

APPENDIX II

FEDERAL MARITIME COMMISSION
PRIVACY IMPACT ANALYSIS

SYSTEM OF RECORDS IDENTIFICATION

1. **Is a system of records being created under the Privacy Act, 5 U.S.C. 552a? If no, skip questions 2 through 4.**

   Yes

2. **Have privacy and IT risk assessments been conducted that consider the alternatives to collection and handling as designed and the appropriate measures to mitigate risks identified for each alternative?**

   The HSPD-12 is mandated across the Federal Government pursuant of Homeland Security Presidential Directive 12 (HSPD-12), August 12, 2004. While there is no Government wide SORN there are numerous agency SORN's (e.g. Department of Justice, Department of Homeland Security, Department of Agriculture) all assuring HSPD-12 compliance with Privacy Act requirements.

3. **What impact will this system have on an individual's privacy? (Consider the consequences of collection and flow of information and identify and evaluate threats to individual privacy.)**

   There should be essentially no impact because the system of records is not used but in rare circumstances where there may be a security concern related to a specific incident where access to information on an individual may have to be reviewed. Even in these rare instances individual privacy would be protected given the limited access to the system and use only on a need to know basis.

4. **As a result of the PIA, what choices have been made regarding the IT system of collection of information? Have adequate measures been designed and implemented to mitigate risk? What is the rationale for the final design choice or business process?**

   Given the mandate to institute HSPD-12 the agency went with the only viable alternative at its disposal given the need to get the best possible system at the best possible price under numerous constraints.

APPENDIX III

FEDERAL MARITIME COMMISSION
SYSTEM DEVELOPMENT LIFE CYCLE
PRIVACY REQUIREMENTS WORKSHEET

A. CONTACT INFORMATION

1. Person who completed the Privacy Impact Assessment document

Name: Peggy J. Wright
Title: Contract Specialist
Bureau/Office: Office of Management Services
Phone number: 202-523-5711

2. System Owner

Name: Michael H. Kilby
Title: Director, OMS
Phone number: 202-523-5900

3. Chief Information Officer

Name: Anthony Haywood
Title: CIO
Phone number: 202-523-0001

4. Senior Agency Official for Privacy

Name: Austin L. Schmitt
Title: Director of Strategic Planning and Regulatory Review
Phone number: 202-523-1266

B. PRIVACY IMPACT ASSESSMENT SUMMARY

	System Category (Check all categories that apply)	**Requirement**
	System of Records	Publish System of Records Notice
	Website available to the public	Publish Privacy Impact Assessment
	Website or information system operated by a contractor on behalf of the FMC for the purpose of interacting with the public	Publish Privacy Impact Assessment
	New or significantly altered information technology investment administering information in an identifiable form collected from or about members of the public	Conduct Privacy Impact Assessment
X	New or significantly altered information technology investment administering information in an identifiable form collected from or about FMC employees	Conduct Privacy Impact Assessment

	Contains medical information	Determine if system is subject to HIPAA
	Other	
	None of the above	Privacy Impact Assessment not required

C. PRIVACY IMPACT ASSESSMENT APPROVAL

Approval of Privacy Impact Assessment accuracy and completeness.

System Owner: _____ _____
Signature Date

Approval of IT System Risk Assessment

Chief Information Officer: _____ _____
Signature Date

Approval of Privacy Assessment and Resulting System Category

Senior Agency Official for Privacy: _____ _____
Signature Date