APPENDIX I

FEDERAL MARITIME COMMISSION
PRIVACY IMPACT ASSESSMENT

A. SYSTEM INFORMATION

1. What is the system name?

Closed Circuit Cameras

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

The information is being collected to enhance the security of FMC controlled space by enabling the identification of any individuals entering and exiting such space.

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

To review in the event of a security incident.

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

Yes, it contains the video images of individuals.

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.

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.

The closed-circuit camera system is new to the FMC HQ.

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.)?

All of the above. Anyone entering or exiting FMC controlled space.

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 source of the information is a video recording of an individual entering or exiting FMC controlled space.

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?

A video image of them entering or exiting FMC controlled space.

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?

A video image by definition is accurate.

b. How will data be checked for completeness?

Video images are inherently complete as long as the recording is on.

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 What steps or procedures are taken to ensure the data are not out of date?

Yes. The data are kept for no longer than 20 days.

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

No, the video is stored on a DVR for no longer than 20 days.

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.

None.

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.)

Yes, the individual's video image by date and time at FMC entries and exits.

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?

Yes, when they entered or exited FMC controlled space.

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

By the clarity of the video image.

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

Yes.

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

The information is not being consolidated.

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.

Not applicable.

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 an individual reviewing the DVR recordings.

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

A report could be produced to indicate who entered FMC controlled space by date and time. The use of the report(s) would be to review in the event of a security incident. Access to the reports would be designated FMC staff and/or law enforcemen conducting the investigation or responsible for reviewing the investigation findings.

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?

Not applicable.

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

No longer than 20 days.

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?

The procedure is that the DVR is over-written after two months with new video camera recordings. No reports are created unless created for a specific security incident.

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?

Yes, the FMC has not previously employed closed circuit cameras. This technology enables identification of individuals who enter or exit FMC space.

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

Yes, in so far as a review of the DVR will enable identification of who entered or exited FMC controlled space.

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

Video images.

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

Three individuals in the FMC's Office of Management Services have the ability to monitor. No ongoing monitoring occurs. System access is limited to authorized personnel only.

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

Not applicable.

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

Not applicable.

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?

There is no user access to the data other than those authorized on a need to know basis.

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.

System logs and security training.

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?

Datawatch Systems Inc. designed the system and provides maintenance as necessary. 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. .

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

Not Applicable.

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

No. Law enforcement entities if necessary..

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

Assist in resolution of a security incident.

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.**

   A final determination has not been made whether this is a system of records. Notwithstanding, responses are being provided for question 2 through 4.

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?**

   Given the nature of the collection (video images) it is difficult to identify alternatives to collection and handling as designed. Nonetheless, the controlled access to authorized personnel on a need to know basis is intended to mitigate risks.

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 simplicity of the closed circuit cameras and lack of alternatives, no choices were made regarding the IT collection of information as a result of the PIA. Adequate measures - especially controlled access by authorized personnel only – have mitigated risk. The rationale for the final design choice was that it was essentially the only agency alternative given need and budget.

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
X	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: _____ _____9/30/2013_____
Signature Date

Approval of IT System Risk Assessment

Chief Information Officer: _____ ____9/30/2013_____
Signature Date

Approval of Privacy Assessment and Resulting System Category

Senior Agency Official for Privacy: _____ _____9/30/2013_____
Signature Date