FINANCIAL CRIMES ENFORCEMENT NETWORK
PRIVACY IMPACT ASSESSMENT

Pursuant to Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Chapter 36), the following organizational privacy management information is provided in this Privacy Impact Assessment (PIA) analysis of how information is handled: (a) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (b) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (c) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

- **NAME OF SYSTEM**

Egmont

- **UNIQUE SYSTEM IDENTIFIER (or Systems of Records Notification)**

SECTION A CONTACT INFORMATION

Director, FinCEN
P.O. Box 39, Vienna, VA 22183-0039
E-mail: InfoAssure@fincen.gov

SECTION B SYSTEM APPLICATION/GENERAL INFORMATION

This section of the Privacy Impact Assessment (PIA) describes the application and the method used to collect, process, and store information. Additionally, it includes information about the business functions the system supports.

The mission of the Egmont Group is to support and strengthen domestic and international anti-money laundering, counter terrorist financing efforts, and to foster global cooperation to that end, through information collection, analysis and sharing, and technological assistance.

The Egmont Secure Web is a network that the Egmont Group members are joining to further improve the efficiency of their information request and dissemination process. This project is designed to provide two primary services to users:

- Provide a secure online mechanism for communication among Egmont Group members from various foreign governments FIUs. This service consists minimally of secure electronic mail.
- Provide a secure web-based mechanism for Egmont Group members to view online reference documents.

SECTION C DATA IN THE SYSTEM

N/A. The System is only used a transmission medium. Data is stored temporarily in the in the email until an analyst gathers the data. There is no structure to the email received. Data is encrypted within the email. The data collected is entered into case reports into the FinCEN Database. Information is not stored within this system, but stored in the FinCEN Database.

SECTION D ATTRIBUTES OF THE DATA

N/A. The System is only used a transmission medium. Data is stored temporarily in the in the email until an analyst gathers the data. There is no structure to the email received. Data is encrypted within the email.

SECTION E ACCURACY, TIMELINESS, AND RELIABILITY

N/A. The System is only used a transmission medium. Data is stored temporarily in the in the email until an analyst gathers the data. The data is dependant on the information received by the FIU's.

SECTION F MAINTENANCE AND ADMINISTRATIVE CONTROLS

The System is only used a transmission medium. Data is stored temporarily in the in the email until an analyst gathers the data. Data can be stored for as little as a few minutes to few days. Firewalls and Intrusion Detection Systems (IDS)'s are in place to monitor any infrastructure anomalies. The email system it self does not have any capability to monitor individuals or groups. The Secure Web is anonymous once a user has RAS'd into ESW. E-mails sent between the FIU's are encrypted. Only authorized FIU's analysts can decrypt the data to view.

SECTION G ACCESS TO DATA

Financial Intelligence Units (FIU) who have been approved by FinCEN have access to the data. Each FIU is responsible for approving who can have access to the system. This is usually a Manager or the Director of that FIU. Other agencies can provide/receive or share data, but they have to request the information through FinCEN. No outside agency (ex: FBI, DHS) can directly access the system.

Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?

N/A.

SECTION H BUSINESS PROCESSES AND TECHNOLOGY

Will the conduct of this PIA result in circumstances that will require changes to the current business processes involving this system? If so, explain. No.

Will the completion of this PIA potentially result in technology changes for the system? If so, explain.

No. This system will not use technology in a new way. It is currently going through an upgrade but the same technologies used in the old system (as far as security goes) will be used