



**Egmont Secure Website (ESW)
Privacy Impact Assessment (PIA)**

Version 1.6

FINAL

December 5, 2012

Revision History

Change Record				
Revision Number	Document ID	Description of Change	Change Effective Date	Change Entered By

Table of Contents

1. Privacy Impact Assessment ESW.....	4
A. CONTACT INFORMATION	4
B. SYSTEM APPLICATION/GENERAL INFORMATION	5
C. DATA IN THE SYSTEM.....	6
D. ATTRIBUTES OF THE DATA.....	7
E. MAINTENANCE AND ADMINISTRATIVE CONTROLS.....	9
F. ACCESS TO DATA.....	10

1. Privacy Impact Assessment Template

Name of Project: Egmont Secure Website (ESW)
Bureau: Financial Crimes Enforcement Network (FinCEN)
Project's Unique ID: 015-04-01-14-02-1006-00-115-047
Name of the system: Egmont
Unique System Identifier: 015-04-01-14-02-1006-00-115-047

A. CONTACT INFORMATION

- 1) **Who is the person completing this document?** (Name, title, organization and contact information).
Name: Fielding Johnson
Organization: TSSD
Email: fielding.johnson@fincen.gov

- 2) **Who is the system owner?** (Name, organization and contact information).
Name: Richard Whitney
Organization: TSSD
Email: richard.whitney@fincen.gov

- 3) **Who is the system manager for this system or application?** (Name, organization, and contact information).
Name: Amy Taylor
Organization: TSSD – CIO
Email: amy.taylor@fincen.gov

- 4) **Who is the IT Security Manager who reviewed this document?** (Name, organization, and contact information).
Name: Quentin Robinson
Organization: FinCEN
Email: Quentin.Robinson@fincen.gov

- 5) **Who is the Bureau/Office Privacy Officer who reviewed this document?** (Name, organization, and contact information).
Name: Gayle Rucker
Organization: FinCEN
Email: Gayle.Rucker@fincen.gov

- 6) **Has organizational privacy management information previously been provided with another PIA?**
 Yes No N/A Enclosed Reference
Details* _____

- 7) If so, has any of this information changed since the previous PIA was submitted? If NO, please provide the title & date of the previous PIA and proceed to Section B of the questionnaire.

Yes Partial No N/A Enclosed Reference

Details* _____

ESW is modernizing system security by employing new access control technologies.

- 8) Who is the Reviewing Official?

Name: Gayle Rucker

FinCEN Privacy Program Manager

Email: Gayle.Rucker@fincen.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION

- 1) Does this system contain any information about individuals?

Yes Partial No N/A Enclosed Reference

Details*

- a. Is this information identifiable to the individual¹¹?
Yes, basic contact information for administrative purposes only
- b. Is this information about individual members of the public?
No, only Financial Intelligence Unit (FIU) representatives/employees
- c. Is this information about employees?
Yes, FIU employees only.

- 2) What is the purpose of the system/application?

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' Financial Intelligence Units (FIU)s. This service consists minimally of secure electronic mail.
- Provide a secure web-based mechanism for Egmont Group members to view online reference documents.

- 3) What legal authority authorizes the purchase or development of this System/application?

The Egmont Charter and its Group Principles of Information Exchange mandate the need for the system.

¹¹ "Identifiable Form" - This means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

C. DATA IN THE SYSTEM

What categories of individuals are covered in the system?

Financial Intelligence Units (FIU) employees who have been approved by their respective FIU authorities will have access to the data.

1) What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

Yes Partial No N/A Enclosed Reference

Details

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

Yes Partial No N/A Enclosed Reference

Details*

The system may contain all or some of the contact information below of the US FIU head:

- (i) Name
- (ii) Physical and Post Office Addresses
- (iii) Public e-mail addresses
- (iv) Title
- (v) Phone

c. Will Tribal, State and local agencies provide data for use in the system?

Yes Partial No N/A Enclosed Reference

Details*.

d. Will data be collected from other third party sources?

Yes Partial No N/A Enclosed Reference

Details*

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

The system may collect all or some of the contact information below of the Egmont FIU heads:

- (i) Name
- (ii) Physical and Post Office Addresses
- (iii) Public e-mail addresses
- (iv) Title
- (v) Phone

3) Accuracy, Timeliness, and Reliability

- a. **How will data collected from sources other than FinCEN records are verified for accuracy?**

Details: The registered user approval process involves the vetting and verification of personal contact information regarding accounts and contact information by contacting actual account holders.

- b. **How will data be checked for completeness?**

Contact data validations are performed by the individuals themselves once systems access is granted. System administrators confirm and verify account specific information prior to connection. All account holding FIU's go through a rigorous assessment process as part of the membership requirements to the Egmont Group. Only when this exhaustive assessment process is complete and ratified by the Heads of FIU are accounts created for that FIU's representative.

- c. **Is the data current?**

Yes Partial No N/A Enclosed Reference

Details* Quarterly review of accounts is performed for accuracy as well as each time a support call is initiated by the member FIU.

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

Yes Partial No N/A Enclosed Reference

Details*

D. 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?**

Yes Partial No N/A Enclosed Reference

Details*

The Egmont Charter and its Group Principles of Information Exchange mandate that the system:

- Provide a secure online mechanism for communication among Egmont Group members from various foreign governments' Financial Intelligence Units (FIU)s. This service consists minimally of secure electronic mail.
- Provide a secure web-based mechanism for Egmont Group members to view online reference documents.

This data is necessary to ensure users are uniquely authenticated.

- 2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

Yes Partial No N/A Enclosed Reference

Details*

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

Yes Partial No N/A Enclosed Reference

Details* The system contains audit, identity management, access control, and role based security. The only records created are the system accounts themselves

4) Can the system make determinations about employees/public that would not be possible without the new data?

Yes Partial No N/A Enclosed Reference

Details* The system contains audit, identity management, access control, role based security, network security and security zones.

5) How will the new data be verified for relevance and accuracy?

Contact data validations are performed by the individuals themselves once systems access is granted. System administrators confirm and verify account specific information prior to connection. All account holding FIU's go through a rigorous assessment process as part of the membership requirements to the Egmont Group. Only when this exhaustive assessment process is complete and ratified by the Heads of FIU are accounts created for that FIU's representative.

Quarterly review of accounts is performed for accuracy as well as each time a support call is initiated by the member FIU.

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

N/A

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

Yes Partial No N/A Enclosed Reference

Details*.

8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Yes Partial No N/A Enclosed Reference

Details* The System is only used a transmission medium. E-mails sent between the FIU's are encrypted when stored temporarily and cannot be searched until an analyst gathers the data. Only addressees who are authorized account holders who have their own private key can decrypt the data to view.

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

Routine system audit reports are generated for system and account administration purposes

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

Yes Partial No N/A Enclosed Reference

Individuals have the right to decline basic contact information for general contact information purposes; however for account holding purposes a minimum amount of personally identifiable information is required:

The system will collect the following Basic Contact Information including:

- (i) Name
- (ii) Physical and Post Office Addresses

- (iii) Public e-mail addresses
- (iv) Title
- (v) Phone

All PKI certificates are based on account id, individual name, and secure e-mail address.

- 11) Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?
 Yes Partial No N/A Enclosed Reference

Specific information is required to create PKI certificates and accounts as specified previously. The following notice to each user is displayed prior to login:

This system is for the use of authorized Egmont users only in support of the Egmont Group mission. It is inappropriate to intentionally access a computer without authorization or in excess of authorized access. To protect the Egmont user community, FinCEN will periodically monitor the system security controls at a system-wide level to detect and prevent unauthorized access by third parties and any malicious activity. FinCEN does not monitor the content of message traffic between authorized Egmont users. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of inappropriate activity, the matter will be referred to the Egmont Committee for appropriate sanctions.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS

- 1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

N/A

- 2) What are the retention periods of data in this system?
Backup are stored for disaster recovery purposes only, per the record retention schedule.

- 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 system contains audit, identity management, access control, role based security data. The System is only used as a transmission medium. Data is stored temporarily on-line in an encrypted format until an account holder gathers the data. Data can be stored on-line for as little as a few minutes to few days. Backup are stored for disaster recovery purposes only, per the record retention schedule.

- 4) Is the system using technologies in ways that the FinCEN has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

Yes Partial No N/A Enclosed Reference

Details*:

ESW is modernizing system security by employing new access control technologies.

- 5) How does the use of this technology affect public/employee privacy?

This technology secures the level of access to specific content through Role Based Access Control (RBAC) and Attribute Based Access Control (ABAC). User privacy will also be protected with this model in a secure non-restricted /secure restricted environment.

- 6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

Yes Partial No N/A Enclosed Reference

Details* The identity management, access control and audit logging components of the system, will provide an audit trail of the user's access to the system.

- 7) **What kinds of information are collected as a function of the monitoring of individuals?**
The system captures only basic access information. This includes login attempts, access granted to the user, and connection time and duration.

- 8) **What controls will be used to prevent unauthorized monitoring?**

Access controls are used to prevent unauthorized access to monitoring component of the system. System controls are implemented in a role-based 'least access' manner. Firewalls and Intrusion Detection Systems (IDS)'s are in place to monitor any infrastructure anomalies.

- 9) **Under which Privacy Act systems of records notice does the system operate? Provide number and name.**

ESW does not constitute a system of records under the Privacy Act.

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

Yes Partial No N/A Enclosed Reference

Details*

ESW does not constitute a system of records under the Privacy Act.

F. ACCESS TO DATA

- 1) **Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, tribes, other)**

Financial Intelligence Units (FIU) employees who have been approved by their respective FIU authorities will have access to the data.

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

Initial user access and account creation is granted by the Egmont Secretariat on the request of a Head of FIU. The extent of initial user access to data is determined by the user's role (owner or member) which is assigned by the user's FIU. Any given FIU or the individual account holders under that FIU are responsible for making accessible to other users any data that is transmitted by that FIU or the individual account holders, either on the FIU's or account holders' own initiative or pursuant to a request from another FIU, via secure email exchange.

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

Access to records in the system is limited to authorized personnel whose official duties require such access, i.e., on a "need to know" basis. Electronic data is protected through application of required security control baselines. Security measures establish different access levels for different types of users. User's access will be restricted to their data only. The registered user will have access to his/her own profile information. FinCEN system administrator will have access to all users profile information.

- 4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)**

Security measures and controls and consistent application of United States Federal Government Federal Information Security Management Act (FISMA) security control baselines.

- 5) Are contractors involved with the design and development of the system and 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?**

Yes Partial No N/A Enclosed Reference

Details: Only FinCEN FTEs are designated as designers and developers of the ESW system and are also required to have appropriate security clearances. Contractors provide end-user support and client installation services (Help Desk). Their contracts include non-disclosure agreements and agreements to comply with all applicable FinCEN policies and laws, including the Privacy Act.

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

Yes Partial No N/A Enclosed Reference

Details:

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

The Egmont Secretariat and the requesting Head of an FIU are responsible for protections as required by the Egmont Charter and its Group Principles of Information Exchange.

- 8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?**

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. Profile data is the only information stored on the system

9) How will the data be used by the other agency?
N/A

10) Who is responsible for assuring proper use of the data?
The Egmont Secretariat and the requesting Head of an FIU are responsible for protections as required by the Egmont Charter and its Group Principles of Information Exchange.

The Following Officials Have Approved this Document

1) System Manager owner

 / S / (Signature) 12/5/12 (Date)
Name *Richard Whitney*
Title *Project manager*

2) IT Security Manager

 / S / (Signature) 12-5-12 (Date)
Name *Quentin Robinson*
Title *ISSO*

3) Privacy Officer

 / S / (Signature) 12/5/12 (Date)
Name *Gayle Rucker*
Title *Privacy Program Manager*

4) Reviewing Official

 / S / (Signature) 5 Dec 12 (Date)
Name *Amy L. Taylor*
Title *CIO*