

Financial Crimes Enforcement Network

Privacy Impact Assessments

Pursuant to the E-Government Act of 2002, federal agencies are required to conduct Privacy Impact Assessments (PIA) for electronic information systems and collections and, in general, make them publicly available “through the website of the agency, publication in the Federal Register, or other means.” The PIA is an 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.”

Until such time that the PIA conducted for each of the following systems is posted on this Web page, copies of these documents may be obtained by contacting the FinCEN Disclosure Officer listed below.

FinCEN Project	Description	Contact for a Copy of the PIA	Address	Office Phone/Fax
1. 314(a) SISS: Secure Information Sharing System	The 314(a) Major Application (MA) provides financial institutions the capability to electronically access subject lists submitted by federal law enforcement and to electronically indicate positive matches on any person or business	Disclosure Officer	PO Box 39, Vienna, VA 22183	(Office) 703-905-5034 (Fax) 703-905-3684

	<p>on that subject list through a secure Internet network. 314(a) also provides a secure messaging system that allows FinCEN to communicate and disseminate information such as advisories and reports on the latest trends in money laundering or terrorist financing to the financial industry.</p>			
<p>2. 314(b) VISP: Voluntary Information Sharing Program</p>	<p>The Section 314(b) information sharing program allows financial institutions to share information with one another for the purpose of detecting and reporting terrorist financing or money laundering activity by providing a safe harbor from liability pertaining to such</p>	<p>See Above</p>	<p>See Above</p>	<p>See Above</p>

	communication.			
3. Bank Secrecy Act (BSA) E-Filing System (formerly known as Patriot Act Communications System, PACS)	(1) A system that provides financial institutions the capability to electronically file their BSA data through a secure Internet network. (2) A secure messaging system that allows FinCEN to communicate and disseminate information such as advisories and reports on the latest trends in money laundering or terrorist financing.	See Above	See Above	See Above
4. Egmont	(1) Provides a secure online mechanism for communication among Egmont Group members from various foreign governments Financial Intelligence Units (FIUs). (2) Provides	See Above	See Above	See Above

	a secure web-based mechanism for Egmont Group members to view online reference documents.			
5. FinCEN Database	FinCEN Database is part of FinCEN's General Support System (GSS) to support FinCEN's efforts to provide a multi-source intelligence and analytical network to support the detection, investigation, and prosecution of domestic and international money laundering and other financial crimes, and other domestic and international criminal, tax, and regulatory matters.	See Above	See Above	See Above
6. ITI - Information Technology Infrastructure	The ITI GSS supports and provides	See Above	See Above	See Above

	telecommunication, network services, and Data Center services to support the FinCEN mission.			
7. Secure Outreach	A Web portal that permits federal and other law enforcement real-time access to data in FinCEN's Money Laundering Coordination Center and the Internal Revenue Service (IRS) Detroit Computing Center (DCC).	See Above	See Above	See Above