COSMOS
Navigate the Compliance Universe

31 C.F.R. § 1.36

Systems exempt in whole or in part from provisions of the Privacy Act and this part.

(a) *In general.* In accordance with 5 U.S.C. 552a(j) and (k) and § 1.23(c), Treasury hereby exempts the systems of records identified in paragraphs (c) through (o) of this section from the following provisions of the Privacy Act for the reasons indicated.

(b) *Authority.* The rules in this section are promulgated pursuant to the authority vested in the Secretary of the Treasury by 5 U.S.C. 552a(j) and (k) and pursuant to the authority of § 1.23(c).

(c) *General exemptions under 5 U.S.C. 552a(j)(2).* (1) Under 5 U.S.C. 552a(j)(2), the head of any agency may promulgate rules to exempt any system of records within the agency from certain provisions of the Privacy Act if the agency or component thereof that maintains the system performs as its principal function any activities pertaining to the enforcement of criminal laws. Certain Treasury components have as their principal function activities pertaining to the enforcement of criminal laws. This paragraph (c) applies to the following systems of records maintained by Treasury:

(i) *Treasury-wide.*

Table 1 to Paragraph (c)(1)(i)

No.	Name of system
Treasury .004	Freedom of Information Act/Privacy Act Request Records.

(ii) *Departmental Offices.*

Table 2 to Paragraph (c)(1)(ii)

No.	Name of system
DO .190	Office of Inspector General Investigations Management Information System (formerly: Investigation Data Management System).
DO .220	SIGTARP Hotline Database.
DO .221	SIGTARP Correspondence Database.
DO .222	SIGTARP Investigative MIS Database.
DO .223	SIGTARP Investigative Files Database.
DO .224	SIGTARP Audit Files Database.

DO .303	TIGTA General Correspondence.
DO .307	TIGTA Employee Relations Matters, Appeals, Grievances, and Com plaint Files.
DO .308	TIGTA Data Extracts.
DO .309	TIGTA Chief Counsel Case Files. (also exempt from 552a subsection (d)(5).
DO .310	TIGTA Chief Counsel Disclosure Section Records. (also exempt from 552a subsection (d)(5)).
DO .311	TIGTA Office of Investigations Files.

(iii) *Special Investigator for Pandemic Recovery (SIGPR).*

Table 3 to Paragraph (c)(1)(iii)

No.	Name of system
SIGPR .420	Audit and Evaluations Records.
SIGPR .421	Case Management System and Investigative Records.
SIGPR .423	Legal Records.

(iv) *Office of the Comptroller of the Currency (OCC).*

Table 4 to Paragraph (c)(1)(iv)

No.	Name of system
CC .110	Reports of Suspicious Activities.
CC .120	Bank Fraud Information System.
CC .220	Notices of Proposed Changes in Employees, Officers and Directors Tracking System (not exempt from 552a(c)(4)).
CC .500	Chief Counsel's Management Information System.
CC .510	Litigation Information System.

(v) *Internal Revenue Service.*

Table 5 to Paragraph (c)(1)(v)

No.	Name of system
IRS 46.002	Criminal Investigation Management Information System and Case Files.
IRS 46.003	Confidential Informants, Criminal Investigation Division.
IRS 46.005	Electronic Surveillance and Monitoring Records, Criminal Investigation Division.
IRS 46.015	Relocated Witnesses, Criminal Investigation Division.

IRS 46.050	Automated Information Analysis System.
IRS 90.001	Chief Counsel Management Information System Records (not exempt from (c)(4), (e)(2), (e)(3) or (g)).
IRS 90.003	Chief Counsel Litigation and Advice (Criminal) Records.
IRS 90.004	Chief Counsel Legal Processing Division Records (not exempt from (c)(4), (e)(2), (e)(3) or (g)).
IRS 90.005	Chief Counsel Library Records (not exempt from (c)(4), (e)(2), (e)(3) or (g)).

(vi) *Financial Crimes Enforcement Network.*

Table 6 to Paragraph (c)(1)(vi)

No.	Name of system
FinCEN .001	FinCEN Investigations and Examinations System.
FinCEN .002	Suspicious Activity Reporting System.
FinCEN .003	Bank Secrecy Act Reports System.
FinCEN .004	Beneficial Ownership Information System (not exempt from 552a(e)(3) and (e)(4)(I)).

(2) The Department hereby exempts the systems of records listed in paragraphs (c)(1)(i) through (vi) of this section from the following provisions of the Privacy Act, pursuant to 5 U.S.C. 552a(j)(2): 5 U.S.C. 552a(c)(3) and (4), 5 U.S.C. 552a(d)(1), (2), (3), (4), 5 U.S.C. 552a(e)(1), (2) and (3), 5 U.S.C. 552a(e)(4)(G), (H), and (I), 5 U.S.C. 552a(e)(5) and (8), 5 U.S.C. 552a(f), and 5 U.S.C. 552a(g).

(d) *Reasons for exemptions under 5 U.S.C. 552a(j)(2).* (1) 5 U.S.C. 552a(e)(4)(G) and (f)(l) enable individuals to inquire whether a system of records contains records pertaining to them. Application of these provisions to the systems of records would give individuals an opportunity to learn whether they have been identified as suspects or subjects of investigation. As further described in the paragraphs (d)(2) through (12) of this section, access to such knowledge would impair the Department's ability to carry out its mission, since individuals could:

(i) Take steps to avoid detection;

(ii) Inform associates that an investigation is in progress;

(iii) Learn the nature of the investigation;

(iv) Learn whether they are only suspects or identified as law violators;

(v) Begin, continue, or resume illegal conduct upon learning that they are not identified in the system of records; or

(vi) Destroy evidence needed to prove the violation.

(2) 5 U.S.C. 552a(d)(1), (e)(4)(H) and (f)(2), (3) and (5) grant individuals access to records pertaining to them. The application of these provisions to the systems of records would compromise the Department's ability to provide useful tactical and strategic information to law enforcement agencies.

(i) Permitting access to records contained in the systems of records would provide individuals with information

concerning the nature of any current investigations and would enable them to avoid detection or apprehension by:

(A) Discovering the facts that would form the basis for their arrest;

(B) Enabling them to destroy or alter evidence of criminal conduct that would form the basis for their arrest; and

(C) Using knowledge that criminal investigators had reason to believe that a crime was about to be committed, to delay the commission of the crime or commit it at a location that might not be under surveillance.

(ii) Permitting access to either on-going or closed investigative files would also reveal investigative techniques and procedures, the knowledge of which could enable individuals planning crimes to structure their operations to avoid detection or apprehension.

(iii) Permitting access to investigative files and records could, moreover, disclose the identity of confidential sources and informants and the nature of the information supplied and thereby endanger the physical safety of those sources by exposing them to possible reprisals for having provided the information. Confidential sources and informants might refuse to provide criminal investigators with valuable information unless they believe that their identities will not be revealed through disclosure of their names or the nature of the information they supplied. Loss of access to such sources would seriously impair the Department's ability to carry out its mandate.

(iv) Furthermore, providing access to records contained in the systems of records could reveal the identities of undercover law enforcement officers who compiled information regarding the individual's criminal activities and thereby endanger the physical safety of those undercover officers or their families by exposing them to possible reprisals.

(v) By compromising the law enforcement value of the systems of records for the reasons outlined in paragraphs (d)(2)(i) through (iv) of this section, permitting access in keeping with these provisions would discourage other law enforcement and regulatory agencies, foreign and domestic, from freely sharing information with the Department and thus would restrict the Department's access to information necessary to accomplish its mission most effectively.

(vi) Finally, the dissemination of certain information that the Department maintains in the systems of records is restricted by law.

(3) 5 U.S.C. 552a(d)(2), (3) and (4), (e)(4)(H), and (f)(4) permit an individual to request amendment of a record pertaining to him or her and require the agency either to amend the record, or to note the disputed portion of the record and to provide a copy of the individual's statement of disagreement with the agency's refusal to amend a record to persons or other agencies to whom the record is thereafter disclosed. Since these provisions depend on the individual having access to his or her records, and since these rules exempt the systems of records from the provisions of the Privacy Act relating to access to records, for the reasons set out in paragraph (d)(2) of this section, these provisions should not apply to the systems of records.