



Financial Crimes Enforcement Network
U.S. Department of the Treasury

Washington, D.C. 20220

June 5, 2024

Jennifer Regen
Metropolitan Nashville Police Department
600 Murfreesboro Pike
Nashville, TN 37210
jennifer.regen@nashville.gov

via Electronic Mail

Re: Revised Bank Secrecy Act Access Memorandum of Understanding

Dear Ms. Regen,

As part of the Financial Crimes Enforcement Network's (FinCEN's) ongoing commitment to safeguard the sensitive information reported to the Treasury Department pursuant to the Bank Secrecy Act (BSA), FinCEN has updated the Memoranda of Understanding (MOUs) that govern external agency access to BSA Information (as that term is defined in the MOU). This effort is a priority for FinCEN.

As part of that effort, I am writing regarding access to BSA Information by the Metropolitan Nashville Police Department (Tennessee) (Agency) through FinCEN Query and any related systems. With this letter, FinCEN is providing an updated MOU and accompanying documents, which will replace the existing MOU in place between FinCEN and the Agency and will set forth the terms, conditions, and standards for your Agency's continued access to and use of BSA Information moving forward. Attached please find the following documents:

- (1) Revised BSA Access Memorandum of Understanding
- (2) Re-dissemination Protocols for Bank Secrecy Act Information-November 2023
- (3) Information Access Security Protocols for Bank Secrecy Act Information-November 2023

We ask that you and the appropriate officials from the Agency review these documents carefully. These documents represent FinCEN's current practices regarding safeguarding of BSA Information, consistent with the BSA.

The attached MOU must be signed by an authorized official of the Agency within 30 days of the date of this letter and returned to FinCEN. The signatory from the Agency must be an official at the appropriate level who is authorized to bind the Agency to this MOU. This document should be electronically signed. If you are unable to do so, please let us know. The

Jennifer Regen
Metropolitan Nashville Police Department (Tennessee)
June 5, 2024

MOU should be **returned to FinCEN by replying all to the original transmittal email**. Once FinCEN receives a signed MOU, FinCEN will promptly sign and return a fully executed copy of the document to you.

If you have questions about this requirement or any other questions or concerns regarding these updated documents, please contact FinCEN immediately. Once executed, this MOU will supersede and replace any and all prior MOUs and accompanying documents regarding the Agency's access to BSA Information and will govern the Agency's access to BSA Information going forward.

FinCEN values our partnership with the Agency and also takes its obligation to safeguard BSA Information extremely seriously. Accordingly, failure to respond to this letter within 30 days may result in FinCEN disabling the Agency's access to BSA Information. We look forward to hearing from you and would be happy to discuss any questions you may have.

Sincerely,

Lynda K.
Gammon

Digitally signed by Lynda
K. Gammon
Date: 2024.06.05
16:58:29 -04'00'

Lynda K. Gammon
Office Director
Operational Information and Development
FinCEN Strategic Operations Division

cc: Katherine Ford, Associate Director, FinCEN Strategic Operations Division

Attachments:

1. Revised BSA Access Memorandum of Understanding
2. Re-dissemination Protocols for Bank Secrecy Act Information-November 2023
3. Information Access Security Protocols for Bank Secrecy Act Information-November 2023

**BSA Access MOU – FinCEN and the Metropolitan Nashville Police Department
(Tennessee)
2024**

**Bank Secrecy Act Access Memorandum of Understanding Between
the Financial Crimes Enforcement Network
and the Metropolitan Nashville Police Department (Tennessee)**



This Memorandum of Understanding (MOU) is between the Financial Crimes Enforcement Network (FinCEN), a bureau within the U.S. Department of the Treasury, and the Metropolitan Nashville Police Department (Tennessee) (Agency). This MOU states the terms under which the Agency may obtain direct electronic access to information collected pursuant to the reporting authority contained in the Bank Secrecy Act (BSA), codified at 12 U.S.C. § 1829b, 12 U.S.C §§ 1951-1960, and 31 U.S.C. §§ 310, 5311-5314, 5316-5336, and including notes thereto, with implementing regulations at 31 C.F.R. Chapter X. This MOU includes and incorporates by reference the following documents, which, as set forth herein, may be periodically updated with notice to the Agency: (1) Re-Dissemination Protocols for Bank Secrecy Act Information, included as Attachment A (Re-Dissemination Protocols); and (2) the Information Access Security Protocols for Bank Secrecy Act Information, included as Attachment B (Security Protocols), collectively the “Protocols.” To the extent that FinCEN and the Agency have entered into previous BSA access agreements, this MOU and accompanying Protocols supersede any and all such agreements including the most recent version of their attachments.

- (1) Definitions: For purposes of this MOU, the definitions set forth below apply.

**BSA Access MOU – FinCEN and the Metropolitan Nashville Police Department
(Tennessee)
2024**

(A) Authorized Personnel: All individuals who have been granted access to FinCEN BSA Systems to conduct authorized queries pursuant to this MOU.

Consistent with the requirements set forth in the Security Protocols, Authorized Personnel must be: (1) designated employees of the Agency; or (2) contractors under the supervision of a designated employee of the Agency.

(B) Agency Coordinator: The individual Point of Contact (POC) who represents their Agency in their obligations as specified in this MOU and the Protocols.

(C) FinCEN BSA Systems: The systems through which FinCEN may provide access to the Agency for searching and obtaining BSA Information, as defined in this MOU. For purposes of this MOU, this includes FinCEN Query and any successor to the FinCEN Query System, as well as any other system used to access BSA Information.

(D) Subject: Any person, entity, or transaction that is the basis for a query of the FinCEN BSA Systems system.

(E) BSA Information:¹ Information protected under the BSA, including the following:

- (a) Suspicious Activity Reports (SARs);
- (b) Currency Transaction Reports (CTRs);
- (c) Reports of Foreign Bank and Financial Accounts (FBARs);

¹ This MOU does not cover beneficial ownership information reported to FinCEN pursuant to 31 U.S.C. § 5336.

**BSA Access MOU – FinCEN and the Metropolitan Nashville Police Department
(Tennessee)
2024**

- (d) Reports of International Transportation of Currency or Monetary Instruments (CMIRs);
- (e) Form 8300 Reports of Cash Payments over \$10,000 Filed by a Trade or Business (Form 8300s);
- (f) Information provided in response to any Geographic Targeting Order (GTO);
- (g) Registration forms filed by money services businesses (MSB Registration Forms);
- (h) Forms completed by banks to designate certain persons as exempt from CTR reporting (DOEP Forms);
- (i) Any other information filed with, or obtained by, FinCEN pursuant to its authority under the BSA which FinCEN may make available; and
- (j) Any other information concerning whether any particular person, entity, or transaction is named or referred to in any report filed under the BSA, including the type of form filed, whether the information is a null set, and all query results.

(2) Access to BSA Information. This MOU applies to any access of BSA Information, including whether by examination of screen displays, download to an Agency system, transfer to any electronic or physical media, or otherwise directly through FinCEN BSA Systems. The Agency must designate an Agency Coordinator and provide that individual's contact information to FinCEN.

(3) Safeguarding of BSA Information; Unauthorized Disclosures. The safeguarding of BSA Information is critically important, and FinCEN takes this responsibility seriously. In

**BSA Access MOU – FinCEN and the Metropolitan Nashville Police Department
(Tennessee)
2024**

making BSA Information available to the Agency, FinCEN is relying upon the Agency’s commitment to safeguard BSA Information. By signing this MOU, the Agency expressly agrees to safeguard BSA Information made available to the Agency. The Agency expressly agrees to report any unauthorized disclosure of BSA Information to FinCEN immediately. The unauthorized disclosure of SARs, including information that would reveal the existence of a SAR, can be a crime, and FinCEN refers such matters to the Treasury Department’s Office of Inspector General. Given the vital importance of safeguarding BSA Information, the Agency expressly agrees to cooperate in any inquiries from FinCEN, the Treasury Department, or relevant law enforcement authorities involving potential unauthorized disclosures of BSA Information, including by providing any information that FinCEN, the Treasury Department, or relevant law enforcement authorities deem necessary to investigate a potential unauthorized disclosure of BSA Information.

(4) Limitations on Access to BSA Information. Authorized Personnel, acting on behalf of the Agency (including in the Agency’s capacity as a participant in a multiagency task force), may make direct electronic queries to retrieve BSA Information from FinCEN BSA Systems:

- (A) Solely consistent with the legal authority of the Agency; and
- (B) Solely for the following purposes: identification, investigation, or prosecution of possible or actual violations of criminal law that fall within the investigative or prosecutorial jurisdiction of the Agency, including related proceedings such as civil and criminal forfeiture proceedings.
- (C) Limited in scope: BSA Information they obtain through FinCEN BSA Systems should be limited to that BSA Information which is immediately useful

**BSA Access MOU – FinCEN and the Metropolitan Nashville Police Department
(Tennessee)
2024**

in connection with the specific matter prompting the query and narrowing any query as much as possible based on reasonably available information.

(5) Limitations on Retention of Queried BSA Information. The Agency and Authorized Personnel will make best efforts to retain only that BSA Information that is immediately useful in connection with the specific matter prompting the query through which the BSA Information was obtained, and consistent with applicable law enforcement requirements. The Agency and Authorized Personnel will promptly destroy any and all data, documents, or summaries which contain BSA Information that it has obtained, stored, or generated that is not immediately useful in connection with the specific matter prompting the query.

(6) Limitations on Use of Queried BSA Information. Authorized Personnel may retain and use BSA Information if it continues to be consistent with the Agency’s legal authority; and for the identification, investigation, or prosecution of possible or actual violations of criminal law that fall within the investigative or prosecutorial jurisdiction of the Agency, including related proceedings such as civil and criminal forfeiture proceedings.

(7) Limitations on Copying and Storing BSA Information. The Agency and Authorized Personnel will make best efforts to obtain advance approval from FinCEN before copying BSA Information into a format that can be accessed outside of FinCEN BSA Systems, when such copy will contain or consist of 5000 or more unique reports covered by Section 1, or substantially all of the information contained in such reports. Any such copies of BSA Information will be stored and maintained solely on a secure government system (or equivalent). The approval described herein is required whether such copy is an electronic file containing images of the reports, an electronic file containing BSA Information in spreadsheet form, a printed document, or a copy in any other format or medium. In the event of exigent

**BSA Access MOU – FinCEN and the Metropolitan Nashville Police Department
(Tennessee)
2024**

circumstances preventing the Agency from obtaining prior approval, the Agency shall notify FinCEN before the end of the first business day after the copying of records as described in this paragraph. Notwithstanding the foregoing, the following conditions apply:

(A) The Agency will not use BSA Information to develop or contribute to any database not under the control of FinCEN that Agency personnel will be able to search as an alternative to making subsequent direct electronic queries to retrieve BSA Information from FinCEN BSA Systems; and

(B) If the Agency discovers that such a database exists and that it contains BSA Information, the Agency will (i) immediately notify FinCEN; (ii) destroy all BSA Information contained in the database; and (iii) destroy any copies, summaries, or other documents that include or make derivative use of such BSA Information.

(8) Conditions of Access. In addition to requirements set forth in the MOU and Protocols, the Agency agrees that, prior to accessing BSA Information, all Authorized Personnel must: (i) enter into individual user agreements acknowledging the terms and conditions under which they can obtain access to FinCEN BSA Systems; and (ii) fully and accurately complete the FinCEN BSA Systems computer access screens (Access Screens) for the relevant data file, to include the search justification field, conducting any queries or accessing BSA Information.

(9) Continuing Representation and Warranty. Each query under this MOU, including, if applicable, completion of any Access Screen in connection with such query, shall be deemed to constitute a continuing representation and warranty by the Agency that the request for retrieval or use complies with, and any use of retrieved or analyzed information will comply with, the terms of this MOU.

**BSA Access MOU – FinCEN and the Metropolitan Nashville Police Department
(Tennessee)
2024**

(10) Disclaimer of Liability. FinCEN will make all reasonable efforts to make BSA Information available to the Agency upon the Agency's request, consistent with the terms of this MOU. However, FinCEN expressly disclaims any liability for any consequence of the non-availability of BSA Information through FinCEN BSA Systems for whatever reason.

(11) Re-dissemination of BSA Information. No BSA Information may be disseminated to any person outside the Agency except consistent with the provisions of the Re-Dissemination Protocols. This restriction also applies to case-related information, and to statistical or other information that references, summarizes, or may reveal the existence of BSA Information.

(12) Information about Inquiries by the Agency. FinCEN maintains as part of its internal databases information concerning queries made by Authorized Personnel, including without limitation (i) information contained on the Access Screens completed by Authorized Personnel, if applicable, and (ii) a record of the information in the relevant data files searched, retrieved, or both, by such Authorized Personnel.

(13) Networking. FinCEN seeks to facilitate networking among agencies that may be investigating the same matters. If the Subject of a query under this MOU has been or subsequently becomes the Subject of another query to FinCEN by another agency, FinCEN at its discretion and without obtaining prior permission, may concurrently notify the Agencies making the two queries concerning the match of information about the two queries, provided that (i) such concurrent notification will involve only the name of the Subject queried, sufficient additional information about the Subject to demonstrate the fact of the match, and information about relevant officials to contact at the two Agencies; and (ii) no concurrent notification of a match will be made in a particular case to the extent that the Access Screen completed by either

**BSA Access MOU – FinCEN and the Metropolitan Nashville Police Department
(Tennessee)
2024**

relevant Agency with respect to that case is specifically marked to indicate the Agency's decision not to permit concurrent notification.

(14) Reports on Use of BSA Information. Upon FinCEN's request, the Agency will supply FinCEN with a report or reports in a format prescribed by FinCEN on information needed to assess the usefulness and impact of the use of BSA Information and networking. This can include but is not limited to (i) the status or results of investigations and prosecutions relating to inquiries made hereunder, including investigations and prosecutions based on referrals from the Agency in connection with such inquiries; and (ii) such other information, including statistical information about the Agency's use of BSA Information hereunder as FinCEN may reasonably request, provided, however, that the Agency may delay providing information concerning any specific investigation or prosecution until such time after the final resolution of that case as the Agency in the reasonable exercise of its discretion deems appropriate.

(15) Records Relating to Re-Dissemination. The Agency agrees not to re-disseminate or share BSA Information with agencies, entities, organizations, or individuals who do not have independent access to BSA Information through an access MOU with FinCEN, except as provided in the Re-Dissemination Protocols or with the express permission of FinCEN. In the event such sharing is authorized, the Agency agrees to maintain records relating to any dissemination of BSA Information to agencies, entities, organizations, or individuals who do not have independent access to BSA Information through an access MOU with FinCEN, consistent with the requirements and procedures set forth in the Re-Dissemination Protocols. The Agency agrees to retain such files and make them available, upon request or as otherwise required by this MOU and accompanying Protocols, to FinCEN, Treasury, or law enforcement.

**BSA Access MOU – FinCEN and the Metropolitan Nashville Police Department
(Tennessee)
2024**

(16) Records of Queries of BSA Information. The Agency shall ensure that appropriate documentation is maintained for FinCEN with respect to the Agency's compliance with this MOU. Such documentation shall include a written record of the purpose for which every query was conducted that coincides with the query justification noted in the database. A contemporaneous investigative file relating to a Subject will satisfy the requirement to prepare such a written record. The Agency agrees to make such files regarding justification for queries of BSA Information available to FinCEN, Treasury, or law enforcement, upon request by FinCEN.

(17) Agency's Compliance. To ensure the Agency's compliance with the terms of this MOU, FinCEN may (i) request the Agency provide internal review and certification of their compliance; and/or (ii) arrange for and conduct onsite and/or electronic inspections of the Agency's access of FinCEN BSA Systems. The Agency agrees to cooperate and respond timely to all requests and actions initiated by FinCEN to ensure compliance and understands that failure to do so may result in the termination of its access to FinCEN BSA Systems.

(18) Periodic Updates to Protocols. FinCEN reserves the right to revise and supplement the Protocols at any time. Revised Protocols automatically become part of this MOU upon receipt by the Agency. In addition, FinCEN reserves the right to issue additional BSA Information safeguards in connection with this MOU in the future as necessary. The Agency also agrees that any such future safeguards will also automatically become part of this MOU upon receipt by the Agency.

(19) Security; Authorized Personnel. The Agency agrees to follow the steps outlined in the Security Protocols, including confirming that all Agency employees acting as Authorized Personnel (or proposed by the Agency for Authorized Personnel status) are the subject of a

**BSA Access MOU – FinCEN and the Metropolitan Nashville Police Department
(Tennessee)
2024**

satisfactory background investigation completed in accordance with the Agency’s policies, have taken all required training, and met all other requirements specified in the Security Protocols.

The Agency must immediately revoke access privileges of Authorized Personnel when they no longer require access to FinCEN BSA Systems. This includes authorized users who (i) are no longer employed by the agency; (ii) have changes in employment status or undergo changes in job duties and responsibilities such that they no longer require access to BSA information; (iii) are subject to personnel actions that implicate matters pertaining to honesty, integrity, or security; or (iv) are the subject of any criminal charges that become known to the Agency.

(20) Control of Records; Open Information and Privacy Laws. BSA Information, or any records thereof, are exempt from search and disclosure under the Freedom of Information Act (FOIA). *See* 31 U.S.C. § 5319. Further, BSA Information “may not be disclosed under any State, local, tribal, or territorial ‘freedom of information’, ‘open government’, or similar law.”

Id. The Agency shall promptly notify FinCEN of any FOIA or similar request implicating BSA Information and coordinate any response to such a request with FinCEN FOIA Office.

Similarly, the Agency shall promptly notify FinCEN of any Privacy Act or similar request as well as any subpoena implicating BSA Information and coordinate any response to such a request with FinCEN FOIA Office.

(21) Costs. The Agency is responsible for costs to the Agency that may arise in connection with its compliance with this MOU, its use of BSA Information consistent with this MOU, and its receipt of training as contemplated by this MOU, including but not limited to travel expenses of Authorized Personnel for the purpose of receiving training. FinCEN imposes no charges for access to BSA Information hereunder and no charges with respect to the travel

**BSA Access MOU – FinCEN and the Metropolitan Nashville Police Department
(Tennessee)
2024**

expenses of FinCEN personnel for the purposes of exercising FinCEN’s inspection rights or providing training as contemplated by this MOU.

(22) Authority to Sign. The persons identified below as signing on behalf of FinCEN and the Agency have the authority to commit FinCEN and the Agency to the undertakings contained in this MOU for the period during which this MOU is effective.

(23) Effective Date; Termination. This MOU is effective as of the first Monday following the date on which it is signed on behalf of FinCEN (Effective Date). This MOU expires five (5) years from the Effective Date. This MOU may be renewed on the same terms for additional five (5) year terms upon mutual written agreement of the parties. This MOU may be terminated by either party upon written notice to the other, effective 30 days from the date that notice of termination is sent (Termination Date). The Agency’s access rights to BSA Information under this MOU will terminate on the Termination Date. FinCEN reserves the right without notice, to suspend the Agency’s access to data files containing BSA Information if, in FinCEN’s sole discretion, such suspension is necessary for reasons of security or for failure to observe the terms of this MOU. If the Agency’s access to BSA Information is terminated or suspended, the Agency shall continue to use and safeguard BSA Information consistent with the terms of this MOU and shall continue to cooperate with FinCEN’s efforts to ensure the Agency’s compliance in that regard.

(24) Material Changes. The Agency is required to notify FinCEN immediately of any material changes to the Agency’s organization, mandate, or structure, that would alter the Agency’s ability to comply with any provision of this MOU.

**BSA Access MOU – FinCEN and the Metropolitan Nashville Police Department
(Tennessee)
2024**

(25) For all required communications referenced in this MOU, FinCEN communications shall be routed to the FinCEN employee assigned as your point of contact or to DataAccessManagement@fincen.gov.

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

**BSA Access MOU – FinCEN and the Metropolitan Nashville Police Department
(Tennessee)
2024**

Accepted and agreed to:

FINANCIAL CRIMES ENFORCEMENT NETWORK

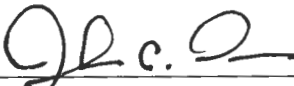
By:

Katherine E. Ford
Associate Director, Strategic Operations Division

Date:

METROPOLITAN NASHVILLE POLICE DEPARTMENT (TENNESSEE)

By:



John Drake
Chief of Police

Date: 7-15-24

Attachments:

- Tab A: Re-dissemination Protocols for Bank Secrecy Act Information
- Tab B: Information Access Security Protocols for Bank Secrecy Act Information
(Security Protocols)



RE-DISSEMINATION PROTOCOLS FOR BANK SECRECY ACT INFORMATION

I. Purpose

These Re-Dissemination Protocols for Bank Secrecy Act (BSA) Information (Re-Dissemination Protocols) set forth requirements on the use and dissemination by any Agency of information provided by the Financial Crimes Enforcement Network (FinCEN), a bureau within the U.S. Department of the Treasury, pursuant to any Memorandum of Understanding (MOU) for access to information filed with FinCEN pursuant to the BSA, codified at 12 U.S.C. § 1829b, 12 U.S.C §§ 1951-1960, and 31 U.S.C. §§ 310, 5311-5314, 5316-5336, and including notes thereto, with implementing regulations at 31 C.F.R. Chapter X.

Because BSA Information generally consists of personal and/or sensitive financial data, the dissemination of such information is subject to strict control. Each Agency with access to BSA Information has an obligation to safeguard such information and to prevent the unauthorized disclosure of such information, consistent with the terms of the MOU, these Re-Dissemination Protocols, the Security Protocols, and the BSA.

FinCEN notes, in particular, that the unauthorized disclosure of Suspicious Activity Reports (SARs), a type of BSA Information, is a violation of law subject to both criminal and civil penalties.

These Re-Dissemination Protocols and the requirements set forth herein are to be read in conjunction with the MOU between FinCEN and the Agency. All defined terms in the MOU are hereby incorporated by reference. As stated in the MOU, the requirements set forth in these Re-Dissemination Protocols supersede any prior re-dissemination protocols that may have been published by FinCEN. As set forth in the MOU, FinCEN reserves the right to revise and supplement these Re-Dissemination Protocols at any time. Revised Re-Dissemination Protocols automatically become part of this MOU upon receipt by the Agency.

II. General Authorization to Re-Disseminate with MOU Holders

Subject to the following conditions, the Agency may disclose BSA Information to another Federal, State, local, tribal, or territorial government Agency with an MOU with FinCEN in support of financial institution examinations, criminal, tax, or regulatory investigations, risk assessments, or proceedings; or intelligence or counterintelligence activities, including analysis, to protect against terrorism, without first obtaining the approval of FinCEN.

Any BSA Information shared by an Agency must be accompanied by the warning statement affixed as Appendix II.

Both the sharing and the receiving Agencies are required to implement appropriate safeguards for sharing and transmitting BSA Information, consistent with the terms of the MOU,

these Re-Dissemination Protocols, the accompanying Security Protocols.

III. Recordkeeping Requirements and Obligations for Sharing BSA Information

An Agency may, under certain circumstances, share BSA Information with any agency, individual, or entity that does not have an active MOU with FinCEN. The circumstances under which such sharing is permitted, and the necessary requirements for such sharing, are set forth in Sections IV-V below.

In addition to the procedures set forth below, any such sharing of BSA Information with an entity that does *not* have an active MOU with FinCEN is subject to the following conditions, notice, and record-keeping requirements:

- (1) The disclosing Agency shall maintain a record of each disclosure of BSA Information, to include the written acknowledgment obtained from the receiving Agency at the time of disclosure reflecting the receiving Agency's understanding that the further dissemination of such information is prohibited without the prior approval of FinCEN. This written acknowledgement shall take the form of the Acknowledgement Form contained at Appendix I to these Re-Dissemination Protocols; and
- (2) The disclosing Agency shall ensure that any BSA Information shared prominently contains the warning statement set forth in Appendix II to these Re-Dissemination Protocols.

IV. Authorization to Share BSA Information with Foreign Partners

With prior written approval from FinCEN, an Agency may share BSA Information in the following situations:

A. Unclassified Sharing with Foreign Partners

FinCEN approval is required prior to re-disseminating BSA Information to foreign partners. FinCEN strongly encourages sharing or re-dissemination of BSA Information contained in an unclassified report or product to occur via Egmont Group channels when the recipient country's financial intelligence unit is a member of the Egmont Group, which may include requests for further dissemination to additional government components (e.g., federal police, sanctioning authority) of a country.

To request that FinCEN share or re-disseminate BSA Information included in an unclassified report via Egmont Group channels, contact FinCEN's Egmont Support Team at CMSEgmontSupportTeam@fincen.gov to request the current Spontaneous Disclosure template. A Spontaneous Disclosure includes the following information: (1) the FIU recipient name; (2) any additional foreign government components the Agency may wish to further share with; (3) a subject line; and (4) the BSA information you are seeking to share.

To seek authorization from FinCEN to share or re-disseminate BSA Information included in an unclassified report outside of Egmont Group channels, contact FinCEN at frc@fincen.gov. In your request to share with foreign partners outside of Egmont Group channels, you must provide the following: (1) the name of the requestor, phone number, office, and organization; (2) a justification for sharing; (3) the proposed method of sharing: hard copy, electronic (e.g., via encrypted email), verbal, etc.; (4) the foreign recipient(s), specifying the country and government authority or authorities receiving the information (e.g., Canada, Royal Canadian Mounted Police);

and (5) a justification for the need to share outside of Egmont channels.

B. Classified Sharing with Foreign Partners

To seek permission from FinCEN to share or re-disseminate BSA Information included in a classified report or product, or that is being shared for classified reasons, contact infoshare@treasury.gov or infoshare@treasury.ic.gov. All requests must include the following: (1) name of requestor, phone number, office, organization; (2) justification for sharing; (3) method of sharing: hard copy, electronic, verbal; (4) classification at which the information will be shared; (5) proposed language to be shared; and (6) the country and government authority or authorities receiving the information. Do not include classified information if sending a request to infoshare@treasury.gov.

V. Other Dissemination of BSA Information

Except as authorized elsewhere in these Re-dissemination Protocols, neither an Agency nor any of its employees may share BSA Information without first obtaining the approval of FinCEN. Any such request for approval must be made via written request to FinCEN via email at frc@fincen.gov. FinCEN requests at least five business days to process such requests, absent exigent circumstances. With respect to requests for sharing of BSA Information, the following requirements apply:

A. Requests from Other Agencies Not Otherwise Authorized

An Agency seeking to share BSA Information with an Agency that is not otherwise authorized under these Re-Dissemination Guidelines, must submit a written request clearly setting forth the following: (1) the particular BSA Information sought to be disclosed; (2) the identity of the Agency or Person to whom the information would be disclosed; and (3) the purpose for the disclosure. The written request also must provide a point of contact, with an email address and phone number, at the Agency seeking to re-disseminate the BSA information.

B. Requests from Third Parties in Connection with Litigation

An Agency that receives requests for BSA Information in litigation, through the process described in their *Touhy* regulations or other authorities, should submit the request to DataAccessManagement@fincen.gov and provide: (1) the name of the requestor, phone number, office, and organization; (2) a justification for sharing; and (3) the proposed method of sharing, such as hard copy, encrypted email, verbal, etc. In addition, the Agency should contact FinCEN's Office of Chief Counsel at (703) 905- 3590 before acting on the request. If the request seeks BSA information from a SAR filed by a bank, the agency receiving the request also should contact the filing bank's primary federal regulator.

C. Requests to Share with the Public

An Agency seeking to share BSA Information or analysis derived from BSA Information with members of the public must submit a written request that includes the following: (1) intended the recipient(s) (e.g., general public, public-private Bank conference); (2) a copy of the unclassified report, product, or language that includes BSA Information or analysis derived from BSA Information; (3) description of how the BSA Information or analysis derived from BSA Information will be used (e.g., public press release, PowerPoint with BSA statistics); and (4) requested suspense date. Note that BSA Information is exempt from disclosure under the FOIA in accordance with 5 U.S.C. § 552(b)(3) and 31 U.S.C. § 5319. As required by the MOU, an

Agency shall promptly notify FinCEN of any FOIA, Privacy Act, subpoena or similar request implicating BSA Information and coordinate any response to such a request with FinCEN FOIA office at FOIA@fincen.gov. These requirements do not apply to information that FinCEN has already made public on their website.

VI. Handling BSA Information That is Not Shared with Foreign Partners

BSA Information or analysis derived from BSA Information that is re-disseminated must be bannered as UNCLASSIFIED//NOFORN//LAW ENFORCEMENT SENSITIVE. Each paragraph of derivatively reported BSA Information, meaning BSA Information extracted from a source document (e.g., a SAR) and incorporated into a subsequent report, product, or correspondence, must be portion marked as (U//LES-NF).

The following citation styles must be used for citing BSA Information:

A. Standard BSA Forms Citation Style for Analytical Products

(U//LES-NF) TREASURY | Access Method (e.g., FinCEN Query, XXXXXX) | BSA ID Number | Filing Date of Record (two-digit day, three letter month, two-digit year) | (U//LES-NF) BSA ID XXXXXXXXXXXXXXXX | Cite portion classified UNCLASSIFIED//LES NOFORN | Overall document classified UNCLASSIFIED//LES NOFORN

B. Standard BSA Collections Data Citation Style for Analytical Products

(U//LES-NF) TREASURY | Access Method (e.g., FinCEN Query, C2BSA) | BSA records collected between Month Year and Month Year | Date Analyst Pulled the information (two-digit day, three letter month, two-digit year) | Cite portion classified UNCLASSIFIED//LES NOFORN | Overall document classified UNCLASSIFIED//LES NOFORN

VII. Reporting Obligations & Auditing

The Agency must retain a record of all disclosures of BSA Information to any agency, individual, or entity that does not have an active MOU with FinCEN. The Agency must provide a list of all such disclosures on an annual basis including the following: (1) date of disclosure; (2) receiving agency, individual, or entity; (3) description of BSA Information disclosed; (4) copy of authorization from FinCEN, where applicable, to share such BSA Information, consistent with these Re-Dissemination Protocols; and (5) a copy of the signed certification provided in Appendix II that accompanied each such disclosure.

VIII. Miscellaneous Provisions

A. Compliance

Failure to comply with these Re-Dissemination Protocols may result in the suspension of the Agency's and/or Authorized Personnel's access to the System. Additionally, criminal, and civil penalties may apply to the misuse of Federal data and resources. Such criminal and civil penalties may be pursued against Authorized Personnel or any other individual who violates applicable law.

B. Unauthorized Disclosure

No current or former government officer, employee, or contractor may disclose a SAR to any person involved in a reported transaction, or otherwise reveal any information that would reveal that the transaction has been reported, other than as necessary to fulfill their official duties.

November 2023

31 U.S.C. § 5318(g)(2). Under FinCEN’s regulations, the disclosure of a SAR to any person except for official purposes is unlawful and subject to criminal and civil penalties. 31 CFR § 1010.950(e). Federal law provides for civil penalties of up to \$100,000 for each violation, 31 U.S.C. § 5321, 31 CFR § 1010.820, and criminal penalties including up to five years imprisonment and fines of up to \$250,000, 31 U.S.C. § 5322, 31 CFR § 1010.840(b). Criminal penalties may increase to include up to ten years imprisonment and fines of up to \$500,000 if the violation occurs “while violating another law of the United States.” 31 U.S.C. § 5322(b), 31 CFR § 1010.840(c).

Any suspected unauthorized disclosure of BSA Information will be referred to the appropriate officials for inquiry and/or investigation. **The Agency expressly agrees to report any unauthorized disclosure of BSA Information to FinCEN immediately by emailing DataAccessManagement@fincen.gov.**

C. Effective Date, Rights & Obligations

As set forth in the MOU, FinCEN reserves the right to update these Re-Dissemination Protocols as appropriate. Any revised versions of the Re-Dissemination Protocols shall become effective and binding on the Agency as of the date of transmission to the Agency.

APPENDIX I - ACKNOWLEDGMENT FORM

TO BE USED BY AGENCY FOR DISCLOSURE OF BSA INFORMATION TO OTHER AGENCIES

I understand that any Bank Secrecy Act (BSA) Information provided to me by the [insert name of disclosing agency here] (“Disclosing Agency”) is being made available to me in my capacity as an employee of [insert name of receiving Agency] (“Receiving Agency”) and for use exclusively in support of financial institution examinations, criminal, tax, or regulatory investigations, risk assessments, or proceedings; or intelligence or counterintelligence activities, including analysis, to protect against terrorism. This Acknowledgement Form is to be signed by a representative of the Receiving Agency with sufficient authority to bind the Receiving Agency with respect to the treatment and handling of BSA Information shared pursuant to this Acknowledgement Form.

I further understand that the unauthorized disclosure of SARs, including information that would reveal the existence of a SAR, can be a crime, and FinCEN refers such matters to the Treasury Department’s Office of Inspector General. Given the vital importance of safeguarding BSA Information, Receiving Agency agrees to cooperate in any inquiries from FinCEN or the Treasury Department involving potential unauthorized disclosures of BSA Information, including by providing any information that FinCEN, the Treasury Department, or relevant law enforcement authorities deem necessary to investigate a potential unauthorized disclosure of BSA Information.

I further understand that this BSA Information is being provided by the Disclosing Agency to the Receiving Agency, consistent with the terms of the MOU between the Disclosing Agency and FinCEN. By signing this Acknowledgement, the Receiving Agency agrees to be bound by the terms and conditions set forth in the MOU, as well as the Re-Dissemination and Security Protocols, including, but not limited to the following:

- The Receiving Agency may use BSA Information solely consistent with the legal authority of the Receiving Agency for the following purposes: identification, investigation, or prosecution of possible or actual violations of criminal law that fall within the investigative or prosecutorial jurisdiction of the Receiving Agency.
- The Receiving Agency must make best efforts to obtain and maintain only that BSA Information which is of value in connection with the specific matter at issue. The Receiving Agency must promptly destroy any and all data, documents, or summaries which contain BSA Information that it has obtained, stored, or generated that is not of value for the specific matter at issue.
- The Receiving Agency must maintain any copies of BSA information appropriately; BSA Information must be stored and maintained solely on a secure government system (or equivalent). The Receiving Agency may not use BSA Information to develop or contribute to any database not under the control of FinCEN that Agency personnel will be able to search as an alternative to making subsequent direct electronic queries to retrieve BSA Information from FinCEN Systems.

I agree not to use this information for other purposes, nor to disclose this information outside of my Agency without prior approval from FinCEN.

Appendix I – Acknowledgement Form for Disclosing and Receiving Agencies

Signature and Title of Receiving Official	Date
Name of Receiving Agency	

Signature and Title of Disclosing Official	Date
Name of Disclosing Agency	

APPENDIX II

WARNING STATEMENT TO BE AFFIXED TO BSA REPORT INFORMATION DISCLOSED TO OTHER AGENCIES

The enclosed information was collected and disseminated under provisions of the Bank Secrecy Act (BSA) and regulations implementing the BSA, codified at 12 U.S.C. § 1829b, 12 U.S.C §§ 1951-1959, and 31 U.S.C. §§ 310, 5311-5314, 5316-5336, and including notes thereto, with implementing regulations at 31 C.F.R. Chapter X. The information is sensitive in nature and is to be treated accordingly. The information may be used only for a purpose related to a criminal, tax, or regulatory investigations, risk assessments, or proceedings; or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against terrorism. See 31 U.S.C. § 5311.

This information – referred to herein as “BSA Information” cannot be further released, disseminated, disclosed, or transmitted except as specified in FinCEN’s Re-Dissemination Protocols.

FinCEN notes, in particular, that the unauthorized disclosure of Suspicious Activity Reports (SARs), a type of BSA Information, is a violation of law subject to both criminal and civil penalties.

Suspicious activity reports (SARs) filed under the BSA must be treated with particular care given that they contain unsubstantiated allegations of possible criminal activity, akin to confidential informant tips. Such reports, or the fact they have been filed, may not be disclosed to any person by any government officer, employee, or contractor except for official purposes. 31 CFR § 1020.320(e); 31 U.S.C. 5318 (g)(2)(ii).

The unauthorized disclosure of a SAR is unlawful and subject to criminal and civil penalties. Federal law provides for civil penalties of up to \$100,000 for each violation (31 U.S.C. § 5321 and 31 CFR § 1010.820), and criminal penalties that include fines of up to \$250,000 and/or imprisonment of up to 5 years (31 U.S.C. § 5322 and 31 CFR § 1010.840). Criminal penalties may increase to include fines of up to \$500,000 and/or imprisonment of up to 10 years if the violation occurs “while violating another law of the United States.” (31 U.S.C. § 5322(b)).

Any suspected unauthorized disclosure of BSA Information will be referred to the appropriate officials for inquiry and/or investigation.



INFORMATION ACCESS SECURITY PROTOCOLS FOR BANK SECRECY ACT INFORMATION

I. PURPOSE

These Bank Secrecy Act (BSA) Information Access Security Protocols (Security Protocols) set forth the security features required to ensure that BSA Information accessed through the Financial Crimes Enforcement Network (FinCEN), a bureau within the U.S. Department of the Treasury, is safeguarded appropriately. These Security Protocols apply to, and must be followed by, any Agency that has access to BSA Information pursuant to any Memorandum of Understanding (MOU) for access to information filed with FinCEN pursuant to the BSA, codified at 12 U.S.C. § 1829b, 12 U.S.C §§ 1951-1960, and 31 U.S.C. §§ 310, 5311-5314, 5316-5336, and including notes thereto, with implementing regulations at 31 C.F.R. Chapter X.

Because BSA Information generally consists of personal and/or sensitive financial data, the dissemination of such information is subject to strict control. Each Agency with access to BSA Information has an obligation to safeguard such information and to prevent the unauthorized access to and disclosure of such information, consistent with the terms of the MOU, these Security Protocols, the BSA, and its implementing regulations.

FinCEN notes, in particular, that the unauthorized disclosure of Suspicious Activity Reports (SARs), a type of BSA Information, is a violation of law subject to both criminal and civil penalties.

These Security Protocols and the requirements set forth herein are to be read in conjunction with the MOU between FinCEN and the Agency. All defined terms in the MOU are hereby incorporated by reference. As stated in the MOU, the requirements set forth in these Security Protocols supersede any prior Security Protocols or guidelines that may have been published by FinCEN. As set forth in the MOU, FinCEN reserves the right to revise and supplement these Security Protocols at any time. Revised Security Protocols automatically become part of this MOU upon receipt by the Agency.

II. PERSONNEL SECURITY

A. General Security Principles

Given the sensitivity of BSA Information, access is restricted to Authorized Persons who are in good standing with their respective Agencies and who meet the criteria set forth below. The Agency has an ongoing and continuing obligation to ensure that Authorized Users (and those employees and/or contractors submitted by the Agency to become Authorized Users) meet these

criteria. Any questions that the Agency has concerning standards of suitability for Authorized Personnel regarding access to BSA Information should be addressed to the FinCEN Application Helpdesk at fincenappshd@fincen.gov.

B. Screening of Authorized Personnel

Before an Agency may propose a person for Authorized Personnel status, the Agency must have determined that the proposed Authorized User meets all of the following criteria:

1. Every authorized user must be an employee or contractor of the Agency in good standing, meaning that the Authorized User's employment with the Agency has not been suspended or terminated for any reason, the Authorized User is not on probation with, or under any investigation by, the Agency, law enforcement, or any inspector general;
2. Every Authorized User must have been the subject of a satisfactory background investigation by the Agency (or any agent retained by the Agency for this purpose). Satisfactory background checks of federal employees completed under U.S. Office of Personnel Management guidelines are deemed to meet this standard. Otherwise, a background investigation under this provision must include, at a minimum, the following components:
 - a) Criminal history checks of National Crime Information Center (NCIC), state and local indices; and
 - b) Verification of the individual's identity, including full name, date of birth, and social security number, based on official documentation that is sufficient to form a reasonable belief as to the individual's identity; and
3. Every Authorized User must be a citizen or permanent resident alien of the United States.¹

After determining that an employee or contractor meets the criteria for becoming an Authorized User, the Agency Coordinator shall submit the user's profile to FinCEN for review and approval in order for the employee and/or contractor to be granted access to FinCEN BSA Systems as an Authorized User.

C. Ongoing Obligation to Ensure Eligibility of Authorized Users

The Agency must immediately revoke access privileges of Authorized Personnel when they no longer require access to FinCEN BSA Systems. This includes authorized users who (i) are no longer employed by the agency; (ii) have changes in employment status or undergo changes in job duties and responsibilities such that they no longer require access to BSA information; (iii) are subject to personnel actions that implicate matters pertaining to honesty, integrity, or security; or (iv) are the subject of any investigation or criminal charges that become known to the Agency. The Agency must revoke access privileges of the Authorized User and notify FinCEN immediately by contacting their respective FinCEN agency liaison via email or the FinCEN Applications Help

¹ FinCEN may waive this requirement on a case-by-case basis in extenuating circumstances.

Desk at fincenappshd@fincen.gov.

III. PHYSICAL & SYSTEM SECURITY

A. System Connections

Access to BSA Information must be limited to Authorized Personnel. The Agency must take reasonable precautions to ensure that Authorized Personnel do not connect to FinCEN BSA Systems in areas readily accessible to persons other than Agency employees or contractors (e.g., public spaces, including hallways or foyers of Agency offices subject to uncontrolled public access). In the event an Authorized User needs to access FinCEN BSA Systems outside of the Agency's controlled areas for work consistent with both the Agency's mission and the authorized use of BSA Information, extreme caution should be exercised to maintain the security of the BSA Information.

If connections are made via a wireless network, connections should be limited to encrypted wireless networks utilizing strong WPA2 or AES (or successors) encryption.² FinCEN BSA Systems may not be accessed in any uncontrolled or unencrypted shared internet access point. Further, FinCEN BSA Systems should not be accessed from a publicly available or widely accessible computer or other device (e.g., retail stores, business establishments, hotels, or cyber cafés).

B. Additional Physical Security Measures

Authorized Personnel must make reasonable efforts to protect BSA Information. Reasonable efforts in this context include, but are not necessarily limited to, the following: equipment in use must not be left unattended at any time without utilizing a password-protected screensaver, logging out, removing tokens or fobs and/or if appropriate, implementing additional physical security measures.

C. Authorized User Access

FinCEN provides Authorized Users with access to FinCEN BSA Systems on the following terms:

1. FinCEN must approve Authorized Personnel before FinCEN BSA Systems access will be granted to them;
2. FinCEN requires that all Authorized Personnel have a unique username and unique authentication method (e.g., password, PIV-mediated credentials, or similar) for accessing FinCEN BSA Systems that are unique to the individual user. Authorized Personnel will receive a username, temporary password, and instructions for setting up a certificate and establishing a unique authentication method from FinCEN when their User Account is created; Authorized Personnel must not share their unique passwords or other authentication methods such as PIV cards, PIN numbers, or tokens, with anyone, including, but not limited to, other Authorized Personnel. The Authorized Personnel to whom passwords or similar

² For more information, please consult the National Institute of Standards and Technology (NIST) Special Publication 800-153 revision 1, [Guidelines for Securing Wireless Local Area Networks \(WLANs\)](#). WEP and WPA are not acceptable protocols.

unique user authentication credentials are issued are responsible for all queries made using their username and user authentication method;

3. The user account for any Authorized Personnel that do not access the FinCEN BSA Systems for a period of 90 days or more will be automatically suspended, and access can only be granted upon request to FinCEN. After a period of 365 days of inactivity, the user account will automatically be permanently disabled. Once an account is permanently disabled, the Agency will be required to submit a new application for the user to obtain access; and

4. Authorized Users are required to comply with all instructions from FinCEN regarding continued access, including in connection with periodic changes to passwords or similar user authentication methods and recovering lost passwords or similar user authentication methods. Questions regarding Authorized User access should be directed to the FinCEN Portal Application Helpdesk at fincenappshd@fincen.gov to reset their login credentials.

D. Password/Data Compromise or Loss

1. If Authorized Personnel passwords or user authentication methods are compromised or lost, Authorized Personnel must **immediately** notify the FinCEN Portal Application Helpdesk at fincenappshd@fincen.gov.

2. Authorized Personnel must **immediately** notify the FinCEN Portal Application Helpdesk upon the receipt of information concerning any apparent, threatened, or possible BSA data compromise or loss.

IV. SECURITY OF BSA INFORMATION

A. Privacy and Appropriate Use

FinCEN BSA Systems are official government systems, and all Authorized Personnel acknowledge prior to logging into the FinCEN BSA Systems that no user has any expectation of privacy concerning use of FinCEN BSA Systems. The Agency is responsible for monitoring the use of FinCEN BSA Systems by their Authorized Personnel. The Agency must take reasonable precautions to ensure that Authorized Personnel avoid and prevent unauthorized use of the FinCEN BSA Systems. Any unauthorized use will result in suspension or termination of the Agency and/or Authorized Personnel's access to FinCEN BSA Systems and/or BSA Information.

B. Maintenance and Destruction of BSA Information

As set forth in the MOU, the Agency and Authorized Personnel are required to limit the BSA Information they obtain through a query to that BSA Information which is immediately useful in connection with the specific matter prompting the query. The Agency will take reasonable precautions to ensure that Authorized Personnel promptly destroy all BSA Information not of value for the specific matter queried that the Agency has obtained or generated, consistent with the Agency's applicable record retention requirements.

Where BSA Information is retained by the Agency, the Agency must take reasonable precautions to ensure the safety and security of BSA Information and materials (electronic or hard

copy) containing BSA Information. BSA Information must not be left unsecured or left unattended in a working area to which persons other than Authorized Users have access.

All electronic files containing such BSA Information must be deleted in accordance with National Security Agency (NSA) guidelines on computer media sanitization.³ Hard copies of all such BSA Information must be destroyed by shredding, burning, or similar means.

C. Standards for Electronic Transmission of BSA Information

If it is necessary to transmit BSA Information, either within the Agency or to a third party consistent with the MOU and the Re-Dissemination Protocols, the BSA Information shall only be transmitted as encrypted Data in Transit (DIT) following current NIST and Executive Order (EO) 14028⁴ protocols. FinCEN provides the FinCEN Portal Secure Mail System as one means for electronic transmission of BSA Information.

D. Standards for Electronic Storage and Processing of BSA Information

The Agency must utilize electronic systems which have implemented a security program and protocols with established current security standards such as NIST 800-53 at the appropriate impact baseline control levels. NIST 800-53 addresses security control families such as Access Control, Audit and Accountability, Identification and Authentication, Media Protection, System and Communication Protection, System and Information Integrity, and others. The Agency must establish a policy and procedure to approve the use of removable media on an exception basis only. While the use of removable media should be limited, when is approved to be used by exception only basis, the current security standards for removable devices should be followed. EO 14028 includes encryption requirements to ensure that Authorized Personnel use of portable computing devices and portable electronic storage media intended to contain BSA Information enable strong cipher algorithm such as AES-256, and that encryption is used when Authorized Personnel store BSA Information on such media.

E. Standards for Physical Transmission of BSA Information

If it is necessary to physically transmit BSA Information, either within the Agency or to a third party consistent with the MOU and the Re-Dissemination Protocols, the Agency and/or Authorized Personnel must use the following methods: (1) certified or registered U.S. mail; or (2) courier service, such as UPS, Federal Express, or authorized USG courier personnel for purposes of intraoffice delivery.

V. REPORTING, INSPECTIONS & AUDITS

A. Participation in Audits and Inquiries

The Agency and Authorized Personnel are required to cooperate in any audits by or inquiries from FinCEN, the Treasury Department, or relevant inspectors general or law enforcement authorities regarding use of FinCEN BSA Systems, unauthorized disclosure of BSA Information, or otherwise related to the access to and use of the information described in the MOU. Failure to provide such cooperation will result in suspension or termination of access to FinCEN BSA Systems and/or BSA Information by the Agency and/or Authorized Personnel. Any suspected

³ See: [Media Destruction Guidance \(nsa.gov\)](https://www.nsa.gov/Policy/Security%20Guidance/Information%20Security/Information%20Security%20Guidance/Information%20Security%20Guidance%20-%20Media%20Destruction%20Guidance%20(nsa.gov).pdf)

⁴ See: [Executive Order on Improving the Nation's Cybersecurity | The White House](https://www.whitehouse.gov/the-press-office/2013/05/01/eo-13526-improving-the-nations-cybersecurity)

unauthorized disclosure of BSA Information should be referred to FinCEN immediately and will be referred to the appropriate officials for inquiry and/or investigation.

B. Authorized Personnel Certifications

On at least an annual basis, FinCEN will supply the Agency Coordinator with a report containing the names of all the Agency's Authorized Users for the purposes of controlling and monitoring access to BSA Information. The Agency must have a process in place to immediately disable the accounts of any authorized users that no longer require access to BSA Information. The Agency must certify to this practice on an annual basis.

C. Monitoring and Audits

FinCEN retains the right to monitor and audit the Agency and Authorized Personnel relating to the use of FinCEN BSA Systems, as well as the use of BSA Information accessed via FinCEN BSA Systems.

FinCEN will request Agency internal review and annual certification to MOU compliance and conduct annual inspections to ensure that the Agency and Authorized Personnel are using the FinCEN BSA Systems and BSA Information appropriately. FinCEN reserves the right to request additional Agency reviews and/or conduct inspections at any time if FinCEN has reason to suspect that FinCEN BSA Systems or BSA Information may be misused. FinCEN reserves the right to inspect Agency's internal systems, including any systems where BSA Information or materials that may rely on or incorporate BSA Information may be stored, to determine if misuse of the FinCEN BSA Systems has occurred.

These requests and inspections may include contacting the Agency for verification that the queries by Authorized Personnel were conducted for authorized purposes and with the approval of their supervisor(s). Such inspections may also include on-site visits to the Agency's office and access to the Agency's relevant records.

VI. MISCELLANEOUS PROVISIONS

A. Compliance

Failure to comply with these Security Protocols may result in the suspension of the Agency's and/or Authorized Personnel access to the FinCEN BSA Systems. Additionally, criminal and civil penalties may apply to the misuse of Federal data and resources. Such criminal and civil penalties may be pursued against Authorized Personnel or any other individual who violates applicable law.

B. Unauthorized Disclosure

No current or former government officer, employee, or contractor may disclose a SAR to any person involved in a reported transaction, or otherwise reveal any information that would reveal that the transaction has been reported, other than as necessary to fulfill their official duties. 31 U.S.C. § 5318(g)(2). Under FinCEN's regulations, the disclosure of a SAR to any person except for official purposes is unlawful and subject to criminal and civil penalties. 31 CFR § 1010.950(e). Federal law provides for civil penalties of up to \$100,000 for each violation, 31 U.S.C. § 5321, 31 CFR § 1010.820, and criminal penalties including up to five years imprisonment and fines of up to \$250,000, 31 U.S.C. § 5322, 31 CFR § 1010.840(b). Criminal penalties may

November 2023

increase to include up to ten years imprisonment and fines of up to \$500,000 if the violation occurs “while violating another law of the United States.” 31 U.S.C. § 5322(b), 31 CFR § 1010.840(c).

Any suspected unauthorized disclosure of BSA Information should be referred to FinCEN immediately and will be referred to the appropriate officials for inquiry and/or investigation.

C. Effective Date, Rights & Obligations

As set forth in the MOU, FinCEN reserves the right to update these Security Protocols as appropriate. Any revised versions of the Security Protocols shall become effective and binding on the Agency as of the date of transmission to the Agency.

APPENDIX I
DEPARTMENT OF THE TREASURY
FINANCIAL CRIMES ENFORCEMENT NETWORK (FinCEN)

Bank Secrecy Act and Other Information Access User Acknowledgment

FinCEN BSA Systems are for use by persons authorized by FinCEN (Authorized Personnel) for purposes consistent with the Bank Secrecy Act (BSA), codified at 12 U.S.C. § 1829b, 12 U.S.C §§ 1951-1960, and 31 U.S.C. §§ 310, 5311-5314, 5316-5336, and including notes thereto, with implementing regulations at 31 C.F.R. Chapter X.

For purposes of this User Acknowledgement, BSA Information includes all records and reports collected by FinCEN under the BSA. The term “FinCEN BSA Systems” includes all systems and services accessible for use by Authorized Personnel to access such BSA Information or other information controlled by FinCEN.

BSA Information is sensitive but unclassified and is to be used exclusively in support of financial institution examinations, criminal, tax, or regulatory investigations, risk assessments, or proceedings; or intelligence or counterintelligence activities, including analysis, to protect against terrorism. Use of FinCEN BSA Systems will be monitored by FinCEN or its delegees for security and administration purposes. Accessing FinCEN BSA Systems constitutes consent to such monitoring. Any unauthorized access to or unauthorized use of the information provided in or accessible through FinCEN BSA Systems is prohibited and may be subject to criminal and civil penalties under federal law.

FinCEN BSA Systems are for the sole use of Authorized Personnel for official business only, and there is no expectation of privacy when using FinCEN BSA Systems. Users are advised that FinCEN or its delegees may provide evidence of possible abuse or misuse of FinCEN BSA Systems to appropriate officials for further action.

USER ACKNOWLEDGEMENT

As a user of FinCEN BSA Systems, I acknowledge my responsibility to conform to the following requirements and conditions and, the Re-Dissemination Protocols for Bank Secrecy Act Information (Re-Dissemination Protocols) and the Information Access Security Protocols (Security Protocols).

1. I understand that failure to agree to this User Acknowledgement and all terms contained herein will result in denial of access to FinCEN BSA Systems.
2. I am a citizen or permanent resident alien of the United States of America or have received the appropriate waiver from FinCEN to access FinCEN BSA Systems.
3. I acknowledge and agree that I am not currently under investigation or pending judicial proceedings for any criminal offense. I further acknowledge that I am an employee in good standing with the Agency, with an active and valid security clearance, and not the subject of any suspension, disciplinary action, or investigation. I am of good character, worthy of

Appendix I – Annual User Acknowledgement

trust and confidence. Further, I understand that any change in this status could result in the suspension or termination of my access to FinCEN BSA Systems.

4. I acknowledge that FinCEN BSA Systems are to be used for official business only, and I agree to use the FinCEN BSA Systems and any information accessed through those systems only for the official business for which I am responsible.
5. I will not access FinCEN BSA Systems unless I have the proper clearances necessary for access to these systems. I understand that FinCEN BSA Systems are not capable of supporting classified queries. I agree that I will not use FinCEN BSA Systems for queries of classified information.
6. I understand the need to protect my FinCEN BSA System passwords and similar unique user authentication credentials. I certify that I will NOT share any of my passwords or similar unique user authentication credentials with anyone, including, but not limited to, other Authorized Personnel. I understand that help desk personnel or system administrators will not request any of my passwords or unique user authentication credentials; however, they may request that I change a password or unique user authentication credential. I will change my passwords or unique user authentication credentials for FinCEN BSA Systems as prompted by FinCEN BSA Systems or as required by FinCEN.
7. I certify that I will not access FinCEN BSA Systems from devices that do not meet the security requirements of the BSA Information Access Security Protocols, such as a personally owned computer or laptop, a publicly available computer (e.g., retail stores, business establishments, cyber cafes) or a computer or laptop offered by a private entity other than my organization (e.g., hotel computer at a convention or conference), except pursuant to a written waiver of this element of the Security Protocols.
8. I acknowledge, understand and agree that I am responsible for all actions taken under my account. I certify that I will not attempt to “hack” the FinCEN BSA Systems (e.g., by using penetration tests or password cracking techniques, executing Ping or tracer commands, or engaging in tampering to circumvent FinCEN security policy and protections), or attempt by any means to gain access to BSA Information or other information controlled by FinCEN for which I am not specifically authorized.
9. I understand that FinCEN may establish limits on the number of records that I am permitted to transfer out of the FinCEN BSA Systems environment by download or other mechanism at any one time. I agree that I will not attempt to obtain records in violation of FinCEN policies pertaining to such limits. I understand that FinCEN routinely monitors download activity and that downloading records in excess of established limits may constitute a violation of the terms of any agreement under which FinCEN grants me access to FinCEN

Appendix I – Annual User Acknowledgement

data, including this User Acknowledgement and any applicable Memorandum of Understanding.

10. I will store any materials containing BSA Information in conformity with the Security Protocols.
11. I understand my responsibility to report all incidents of compromised or lost FinCEN BSA System passwords or similar unique identification credentials or of any apparent, threatened, or possible loss of BSA Information to the FinCEN Portal Application Help Desk.
12. I certify that I will not load additional software and updates onto official or contractor-owned Portable Electronic Devices (PEDs) that are approved to process or connect to FinCEN BSA Systems unless authorized by and coordinated with the FinCEN Information System Security Officer (ISSO).
13. I will not connect any PEDs or any peripherals for a PED to any FinCEN system (classified or unclassified, including but not limited to FinCEN BSA Systems) while in a FinCEN-controlled facility unless appropriately authorized. This includes connection via MODEM and data ports.
14. I further acknowledge my responsibility to conform to the requirements of all conditions of access imposed by FinCEN in connection with my use of FinCEN BSA Systems. I also acknowledge that failure to comply with any such conditions may constitute a security violation resulting in denial of access to FinCEN BSA Systems and that such violation may be reported to appropriate authorities for further actions as deemed appropriate, including disciplinary, civil, or criminal penalties.
15. I understand and agree that I have no expectation of privacy on FinCEN BSA Systems. I consent to inspections by authorized FinCEN personnel or their delegees, at any time, and agree to make any passwords or user authentication credentials available for investigation and review by authorized FinCEN personnel upon request. I further consent to FinCEN monitoring my use of FinCEN BSA Systems for inspection, law enforcement or other purposes.
16. I acknowledge and understand that this User Acknowledgement may be updated from time to time and that continued agreement to its terms and conditions is required for access to FinCEN BSA Systems.