November 2023

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) 14028[4] 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)
[4] See: Executive Order on Improving the Nation's Cybersecurity | The White House

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

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

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

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.