Privacy Impact Assessment

System Name: NFA Applications Suite System

Date: April 1, 2025

1. Overview

The National Futures Association ("NFA") is a not-for-profit membership corporation formed in 1976 and functions as a futures industry self-regulatory organization under Section 17 of the Commodity Exchange Act ("CEA"). The Commodity Futures Trading Commission ("CFTC" or "Commission") has delegated to NFA the authority to perform certain functions and act as custodian of certain CFTC records to support the CFTC's mission of protecting market participants and the public from fraud, manipulation, abusive practices, and systemic risks related to futures and swaps derivatives and to foster transparent, open, competitive, and financially sound markets.

The NFA Applications Suite System ("Applications Suite") is a collection of the NFA databases and applications specifically designed to allow NFA to fulfill the mission and business objectives set forth by the Commission through delegated authority. NFA performs several specific regulatory activities for the Commission through delegated authority as follows:

- reviewing applications for individuals and firms to register to conduct business pursuant to CEA, 7 U.S.C. § 1 *et seq.*, and approving or denying those applications, for individuals, based in part on results of background checks and proof of passing appropriate qualification examinations;
- handling notices of exemption or exclusion or claims for exemption or exclusion from certain CFTC requirements;
- handling other notices and related communications from firms, individuals, or foreign regulators related to CFTC substituted compliance procedures;
- screening to determine fitness to obtain or maintain CFTC registration;
- denying, revoking, suspending, or conditioning registrations;
- maintaining systems for CFTC registrants ("Registrants") to file certain financial statements, disclosures, and other required documentation, and reviewing and auditing such documentation;
- reviewing and analyzing Registrants' financial filings provided in the context of registration applications; and
- maintaining a public-facing website with information about Registrants, including current registration status and any disciplinary action imposed.

The Applications Suite takes in a variety of information from individuals and firms applying for registration to conduct business pursuant to the CEA (7 U.S.C. § 1 *et seq.*), individuals and firms seeking exemption from certain requirements, Registrants, and select market participants (e.g., exchanges) to allow NFA to accomplish the above activities. Though subject to change with future information technology upgrades, this Privacy Impact Assessment ("PIA") covers activities that are currently handled by the following NFA databases and applications[1]:

- Background Affiliation Status Information Center ("BASIC"): a public-facing, web-based, searchable system that contains registration information and regulatory and non-regulatory actions, including disciplinary actions and arbitration decisions made by NFA, the CFTC, and U.S. commodity derivatives exchanges.
- Disclosure Document System ("DDOC"): a web-based system that enables Registrants to file disclosure documents.
- Fingerprint system: a system that allows NFA to store and electronically process fingerprint cards for certain applicants for registration.
- Electronic Filing Cabinet ("EFC"): a system used internally by NFA that contains registration records of Registrants.
- EasyFile: a web-based system that enables Registrants to electronically file a variety of documents, including but not limited to daily, quarterly, and annual statements; foreign exchange currency balances; criminal and regulatory statutory disqualification forms; and other compliance documents.
- Financial Analysis & Audit Compliance Tracking System ("FACTS"): an internal database that stores financial, audit, and other compliance information about Registrants.
- Fitness Image: an internal system that stores images of non-public registration records.
- Compliance Regulatory Exam Software: a system used by NFA to perform inspections of submissions by Swap Dealers and Major Swap Participants pursuant to Commission Regulation 3.10(a)(1)(v)(A)-(B).
- Online Registration System ("ORS"): a web-based registration and processing system. Except for a limited number of forms, NFA no longer accepts hardcopy versions of registration, all of which must be electronically filed using ORS.
- WinJammer™ Online Filing System: a web-based system that allows certain Registrants to enter and transmit FOCUS reports, financial reports for Futures Commission Merchants (Form 1FR-FCM), Segregated Investment Detail Reports ("SIDRs"), notice filings, and other financial statements.
- Exemptions: a web-based system used for filing certain notices of exclusion or exemption from the CFTC's Part 4 requirements.

2. Data Collected and Stored Within the System

2.1. What information is collected, used, disseminated, or maintained in the system?

NFA collects, uses, disseminates, and maintains in the Applications Suite, or system, a variety of information used for identification and regulatory purposes. This information includes:

[1] NFA maintains its own business activities separate from its activities for the CFTC by delegated authority. This PIA only covers those NFA activities performed for the CFTC by delegated authority.

Personally Identifiable Information ("PII") Categories	Is collected, processed, disseminated, stored, and/or accessed by the system
Name	X
Date and/or Place of Birth	X
Citizenship	X
Social Security Number (9 digits)*	X
Taxpayer Identification Number	X
Legal Entity Identifier	X
Photographic Identifiers	X
Driver's License	X
Biometric Identifier (Fingerprint)**	X
Physical Characteristics	X
Mother's Maiden Name	X
Mailing Address	X
Phone and Fax Numbers	X
Financial Account Information	X
Trader Information:	X
Options Account Information	X
Futures Account Information	X
Special Account Reporting Number	X
Certificates	X
Legal Documents	X
Web Uniform Resource Locator	X
Internet Protocol ("IP") Address	X
Authentication Information	X
Email Address	X
Education Records	X
Military Status	X
Employment Records	X
Foreign Activities	X
NFA ID Number	X
Central Registration Depository ("CRD") ID Number	X
Investment Adviser Registration Depository ("IARD") ID Number	X
Record of Arrest and Prosecution Sheet ("RAP")	X
Commodity interest related regulatory and non-regulatory actions taken by NFA, CFTC, & U.S. Exchanges	X

*Requested on the Federal Bureau of Investigation ("FBI") fingerprint card and CFTC Forms 8-R and 8-W. Providing a Social Security number assists NFA in identifying individuals and ensuring it assigns only one NFA ID number per person, thereby expediting the processing of these forms. On Forms 8-R and 8-W, a Social Security number also may be used pursuant to the Debt Collection Improvement Act of 1996 to facilitate collection and reporting on any debt owed to the U.S. Government, including civil monetary penalties. Also, the last four digits of the Social Security number are collected for Sole Proprietors who file notices of exemption through NFA's Exemptions system.

**The FBI provides fingerprint identification services for the positive identification of certain individuals with common names and to facilitate fitness reviews of Registrants on spot and periodic bases.

2.2. What are the sources of the information in the system?

Applicants for registration, Registrants, firms and individuals filing notices of exemption or exclusion or claims for exemption or exclusion, and select market

participants (e.g., exchanges) are the primary sources of the collected information. Information also may be provided by foreign government authorities related to substituted compliance procedures. While conducting cross reference, background checks, or fitness investigations, additional sources that provide information to NFA may include the FBI, Financial Industry Regulatory Authority ("FINRA") Central Registration Depository ("CRD®"), court documents, Public Access to Court Electronic Records ("Pacer"), World-Check™, Interpol, and regulators.

2.3. Why is the information collected, used, disseminated, or maintained?

NFA uses this information both to perform the duties delegated to it by the CFTC and to oversee its Members. For example, NFA thoroughly screens all applicants for registration. Individual applicants must meet stringent fitness requirements, provide fingerprint cards for FBI background checks, and pass comprehensive proficiency testing requirements. NFA exercises the delegated authority to deny, revoke, suspend, or condition registration, with certain appeal rights to the CFTC. In addition, NFA collects certain notices and handles related communications concerning exemptions or exclusions from CFTC requirements and CFTC substituted compliance procedures.

Information is collected, used, disseminated, and maintained in accordance with CFTC regulations and NFA Member rules. These rules and regulations dictate the type of information that is required in order for NFA to fulfill its CFTC delegated responsibilities.

2.4. How is the information collected by NFA?

NFA collects the information in electronic format through online portals, emails, and secure connections as well as in the form of paper, fingerprint cards, faxes, and/or mail.

2.5. Is the system using technologies in ways that NFA has not previously employed (e.g., monitoring software)?

No. All software and technologies used are common to NFA's current infrastructure.

2.6. What specific legal authorities authorize the collection of the information?

In 1974, Congress passed the Commodity Futures Trading Commission Act, establishing the CFTC as a federal regulatory agency with jurisdiction over commodity futures trading. The same legislation authorized the creation of "registered futures associations," giving the futures industry the opportunity to create a nationwide, self-regulatory organization. NFA began its regulatory operations in 1982. Since then, NFA has continued to accrue responsibilities under authority delegated to it by the CFTC, including but not limited to processing registrations; reviewing submissions by Swap Dealers and Major Swap Participants pursuant to Commission Regulation 3.10(a)(1)(v)(A); collecting, reviewing, and analyzing notices and related communications concerning exemptions or exclusions from CFTC requirements and CFTC substituted compliance procedures; reviewing and analyzing financial statements filed by Registrants; reviewing and approving disclosure documents; and accepting notices of disciplinary actions in accordance with Commission Regulation 9.11.

3. Data and Records Retention

3.1. For what period of time data collected by this system is maintained and in what form is the data retained?

The records are maintained in accordance with CFTC records disposition schedules approved by the National Archives and Records Administration. The schedules are available at http://www.cftc.gov. CFTC and NFA are revising the records disposition schedules that apply to records covered by this PIA.

3.2. What are the plans for destruction and/or disposition of the information?

To the extent possible, taking into account system and data integrity requirements for linked records, NFA disposes of PII in accordance with CFTC retention requirements. Deletion and destruction techniques vary depending on the medium in which the information is stored.

4. Access to and Sharing of the Data

4.1. Who has access to the information in the system (internal and external parties), and with whom is data shared? If contractors, are the Federal Acquisition Regulation ("FAR") clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)?

CFTC regulations require that certain registration information is made publicly available. NFA generally makes available to the public on NFA website(s) firm directories, business addresses, telephone numbers, registration categories, supplemental biographical information (except for any confidential information on supplementary attachments to the forms), effective dates of registration, registration status, and disciplinary actions taken concerning Futures Commission Merchants, Introducing Brokers, Commodity Pool Operators, Commodity Trading Advisors, Swap Dealers, Major Swap Participants, and Retail Foreign Exchange Dealers and their Associated Persons. NFA also will release records or portions of records to any member of the public if such records or portions are ‘‘public’’ or ‘‘publicly available’’ under Commission Regulations 1.10(g) or 145.0.

Applicants for registration, Registrants, individuals and firms seeking exemption or exclusion from CFTC requirements, and exchanges have access to certain types of non-public information in the Applications Suite, as authorized by the CEA and CFTC regulations.

Authorized NFA staff have access to non-public information in the system on a need-to-know basis. Information is shared with the CFTC and other regulatory agencies and may be shared as required or permitted by law, which can include law enforcement and foreign government authorities. Contractors that may have access to this information are contractually required to maintain the confidentiality of non-public information either through FAR terms and conditions or other terms and conditions containing similar protections and restrictions on the use of information.

4.2. If the data is shared outside NFA's network, how is the data transferred or shared?

Certain information in the Applications Suite is publicly available in accordance with the CEA and/or CFTC regulations. Information that is not publicly available and is

shared outside the NFA network is provided via secure channels in a manner designed to prevent the unnecessary and/or unauthorized disclosure of sensitive information. Such methods may include encryption of electronic information (e.g., Secure File Transfer Protocol ("SFTP")) or hand delivery of documentation.

4.3. If the data is released to the public, consultants, researchers, or other third parties, is it aggregated or otherwise de-identified (i.e., anonymized)? If yes, please also explain the steps that NFA takes to aggregate or de-identify the data.

Some information that is not publicly available may be provided in accordance with the SORN. Unless otherwise required by regulations, rules, laws, or other legally binding agreements, NFA will anonymize non-public data to be released to the public by aggregating the data to de-identify specific individuals.

4.4. Do the recipients of the aggregated or de-identified information have another dataset, or is there a publicly available dataset that could be used to re-identify NFA information?

NFA is not aware of any dataset that could be used to re-identify the information. NFA will anonymize any non-public data to be released to the public by aggregating the data.

4.5. Describe how NFA tracks disclosures of information that are shared with outside entities. The Privacy Act requires that NFA record the date, nature, and purpose of each disclosure of a record to any person or to another agency.

CFTC regulations require that most information collected is publicly available. For requests for information in PII-form, when such information is not publicly releasable, NFA confirms its legal authority to release such information and tracks such disclosures to outside entities by documenting which person or organization made the request, the date and nature of the request, the decision made to disclose or not disclose the data and by whom, and any restrictions on further dissemination of the requested information. Requests for information can be handled by NFA General Counsel, Compliance, or Registration staff. Privacy Act and Freedom of Information Act ("FOIA") requests are also logged.

4.6. Do other systems share the information or have access to the information in this system? If yes, explain who is responsible for protecting the privacy rights of the individuals affected by the interface (e.g., system administrators, system developers, and system managers)?

Yes. The Applications Suite shares certain information with the CFTC via an SFTP connection and a secure encrypted connection. NFA also shares certain information with the FBI via Simple Mail Transfer Protocol ("SMTP"). NFA is also working to make certain information available to FINRA via SFTP protocols. NFA Information Systems owners and Information Technology staff are responsible for protecting the privacy rights of individuals affected by the interface.

5. Notice, Consent, and Access for Individuals

5.1. What notices are provided to individuals about the collection, use, sharing, and other processing of their personal data?

Notice about the collection, use, and sharing of personal data is provided through various means, including NFA's "Disclaimer and Privacy Policy" on its website; the certifications in firm and individual applications, including Privacy Act notices; system use notification messages; and associated CFTC published SORN CFTC-12. In addition, this PIA will be posted on both CFTC and NFA websites.

5.2. What opportunities exist for an individual to decline to provide information or consent to particular uses of the information? If opportunities exist, how is this notice given to the individual and how can an individual grant consent?

Individuals are required by law to provide certain information in order to apply, register, and/or participate in activities governed by the CEA, and they are given an opportunity to consent to the collection, use, maintenance, and/or dissemination of their PII when they submit their applications for registration. For example, CFTC registration application forms contain language whereby an individual consents to the collection and use of certain PII. Individuals may decline to provide some information that is not specifically required, such as Social Security numbers.

5.3. What procedures exist to allow individuals to gain access to their information and request amendments/corrections, and how are individuals notified of these procedures?

Individuals may access much of the information maintained about them by NFA through the public interface of the BASIC application, i.e., the BASIC website. NFA's "Disclaimer and Privacy Policy" directs individuals requesting access, amendment, or correction to their information to contact NFA by email at information@nfa.futures.org. In addition, Individuals may amend some of their information by logging into applications accessible on the NFA website, including ORS.

Requests for information also can be handled by NFA General Counsel, Compliance, or Registration staff. For details, please see NFA Rule 701, Disclosure of Information From Registration Records Maintained by NFA, and Rule 4-1, Disclosure of Information from CFTC Records, Other than Registration Records, Maintained by NFA.

6. Maintenance of Controls

6.1. What controls are in place to prevent the misuse of the information by those having authorized access and prevent unauthorized access, use, or disclosure of the information?

NFA follows the National Institute of Standards and Technology Special Publication 800-53 Revision 5 “Security and Privacy Controls for Information Systems and Organizations” ("NIST Special Publication 800-53") in adopting appropriate controls to safeguard information. The information is protected from misuse and unauthorized access through various administrative, technical, and physical security measures. Administrative measures include policies and procedures that require appropriate treatment of personal information and mandatory completion of annual privacy and security training. Technical security measures include limiting access to authorized individuals, requiring the use of strong passwords that frequently change, encrypting data at rest and during transfers, and regularly reviewing security procedures and best practices to enhance security. NFA's website also utilizes various security measures such as firewalls, encrypted data transmissions, and other security techniques to

protect users' personal data. In addition, the CFTC accesses NFA information and data through secure means. For example, email communications between NFA and the CFTC are generally encrypted, at present, through transport layer security ("TLS") technology, and CFTC staff members can directly access certain NFA applications through secure web portals. Physical measures include restricting access to building and office space to authorized individuals and maintaining records in locked data centers, network equipment rooms, offices, and filing cabinets.

6.2. While the information is retained in the system, what are the requirements for determining if the information is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

Various administrative, technical, and physical security measures are in place to help ensure that the information entered into the Applications Suite continuously reflects over time original and amended information. NFA conducts regular audits, reviews, and spot checks of its systems to validate the integrity of information. Also, individuals may access much of the information held by NFA through the BASIC website to confirm the accuracy, relevance, timeliness, and completeness of the information and may contact NFA to request amendment.

6.3. Does this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

No. Although the system contains addresses and other contact information, it does not allow NFA to monitor an individual's real-time movements or actions.

6.4. Does this system comply with Federal Information Security Management Act ("FISMA") requirements to help ensure that information is appropriately secured?

Yes. NFA follows NIST Special Publication 800-53, which was developed to support the implementation of and compliance with FISMA. A security assessment of the Applications Suite is regularly conducted by NFA security staff and reviewed by the CFTC Division of Data ("DOD") Security Team.

6.5. Describe the privacy training provided to users either generally or specifically relevant to the program or system.

All NFA personnel are subject to NFA's company-wide procedures for safeguarding PII and completing privacy and security training at least annually.

7. Privacy Act

7.1. Can the data in the system be retrieved by a personal identifier in the normal course of business? If yes, explain.

Yes. NFA ID numbers, names, and Social Security numbers are used in the Applications Suite as means to identify individuals or companies and retrieve information about them.

7.2. Is the system covered by an existing Privacy Act SORN? Provide the name of the system and its SORN number, if applicable.

The Applications Suite is currently covered by SORN CFTC-12, "National Futures Association (NFA) Applications Suite System" (84 FR 17811), which is available at https://www.cftc.gov/Privacy/SORN/index.htm.

8. Privacy Policy

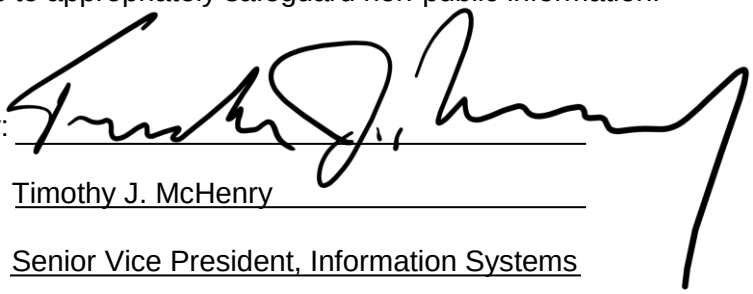
8.1. Confirm that the collection, use, and disclosure of the information in this system have been reviewed to ensure consistency with the NFA's Privacy Policy on https://www.nfa.futures.org/.

Yes. NFA's "Disclaimer and Privacy Policy" reflects the collection, use, and disclosure of information.

9. Privacy Risks and Mitigation

9.1. What privacy risks are associated with the collection, use, dissemination, and maintenance of the data? How have those risks been mitigated?

NFA is working to minimize the collection of PII to the minimum necessary to carry out its obligations delegated by the CFTC. Occasionally, however, NFA may receive more information from individuals than requested. To mitigate associated privacy risks, NFA maintains a comprehensive information security plan with security and privacy controls designed to safeguard NFA's networks and systems and has adopted the protections identified in Section 6.1, above, and other preventive measures to appropriately safeguard non-public information.

Approved By: 

Name: Timothy J. McHenry

Capacity: Senior Vice President, Information Systems