



EXECUTIVE ORDER No. 2026-002

SENSITIVE INFORMATION AND ASSOCIATION INFORMATION SECURITY DURING INTERNATIONAL TRAVEL

Date of Issuance: September 15, 2026

Effective Date: Immediately

Article I. Purpose

To protect the information security of the members, officers, administrators, employees, volunteers, partners, and the New York Firearms Association, Inc. ("NYFA") itself, and to prevent sensitive information from being obtained, accessed, copied, detained, disclosed, transferred, or misused without authorization during international travel or other cross border activities, as well as to address potential security threats involving foreign governments, foreign intelligence services, agents of foreign governments, and other foreign-based entities or actors, this Administrative Order is hereby issued.

Article II. Scope

This Administrative Order applies to all people who represent NYFA, perform duties on behalf of NYFA, participate in NYFA activities, or possess NYFA authorized equipment, information, or materials, including but not limited to:

1. The President and Vice Presidents, including Honorary Officers;
2. Directors and senior administrative officers;
3. Department heads;
4. NYFA employees and staff;
5. Volunteers and representatives authorized by NYFA to perform official duties; and
6. Any other person is formally authorized by NYFA to access sensitive NYFA information.

Article III. Restricted Travel Jurisdictions

Any person subject to this Order who travels to a foreign jurisdiction falling within any of the following categories shall comply with the information security requirements established herein:

1. Jurisdictions designated by the U.S. Department of State as subject to elevated or higher travel advisory levels;
2. Jurisdictions for which the U.S. Government has issued security warnings concerning arbitrary law enforcement, exit restrictions, government seizure or detention, or other special security risks;

3. Other jurisdictions determined by the NYFA Office of the President to present significant information security risks; and
4. The NYFA Office of the President may issue or update a list of applicable jurisdictions based on the latest U.S. Government security information and prevailing security conditions.

Article IV. Sensitive Information

For purposes of this Order, "Sensitive Information" includes, but is not limited to:

1. NYFA membership rosters and members' personal information;
2. Member identities, contact information, and other personal identifiable information;
3. Firearms licenses, permits, and related application information of NYFA members;
4. Legal records, background-investigation information, and case-related information concerning members;
5. NYFA internal meeting and administrative information;
6. Non-public NYFA policies, plans, and administrative documents;
7. NYFA security procedures, event-security plans, and internal security information;
8. Non-public information concerning partner organizations and partner personnel;
9. NYFA account information, login credentials, passwords, and other information-system security information; and
10. Any information marked "Confidential," "Restricted," "Internal Use Only," or otherwise designated as having an equivalent level of sensitivity.

Article V. Prohibition on Transportation and Storage

Unless prior written approval is obtained from the President of NYFA or a senior officer designated by the President, no person subject to this Order shall:

1. Carry NYFA Sensitive Information into a restricted travel jurisdiction;
2. Store NYFA Sensitive Information on personal electronic devices;
3. Store NYFA Sensitive Information on external storage devices not approved by NYFA;
4. Upload NYFA Sensitive Information to cloud services not approved by NYFA; or
5. Transmit NYFA Sensitive Information through unauthorized personal accounts.

Article VI. Travel Devices

People traveling to restricted travel jurisdictions should, whenever practicable, use travel-dedicated devices that do not contain NYFA Sensitive Information.

NYFA personnel shall not, for personal travel, family visits, business activities, or other non-NYFA purposes, remove NYFA member information or confidential internal NYFA information from the United States.

Article VII. Special Authorization

When it is genuinely necessary to carry Sensitive Information in connection with an official NYFA assignment, the individual must obtain written authorization from the Office of the President before departure.

Such authorization shall consider the necessity of the information, the purpose of the travel, the risks associated with the destination, and the information security measures available to mitigate those risks.

Article VIII. Security Incident Reporting

If an NYFA person experiences the loss of a device, detention or inspection of a device, unauthorized or unusual account access, suspected copying of information, or any other circumstance that may result in the disclosure or compromise of NYFA information while traveling abroad, the individual shall, when reasonably safe to do so, immediately report the incident to the Office of the President.

Article IX. Security Measures Upon Return to the United States

The Office of the President may require individuals returning from restricted travel jurisdictions to undergo necessary security checks concerning their devices, accounts, and information.

When necessary, NYFA may require the individual to change account passwords, revoke access privileges, reconfigure devices, or implement other appropriate information-security measures.

Article X. Enforcement and Disciplinary Measures

NYFA officers and administrators at all levels shall be responsible for ensuring compliance with this Order.

Any person who violates this Order may, depending on the circumstances, be subject to:

1. A warning;
2. Suspension of information-access privileges;
3. Revocation of official authorization or assigned responsibilities;
4. Termination of an internal NYFA position or assignment;
5. Other appropriate administrative measures; or
6. Where the conduct may involve a violation of applicable law, NYFA reserves the right to take further action as permitted by law.

Article XI. Prohibition on Providing Funds to Foreign Governments and Restricted Entities

Except where expressly permitted by law and approved in advance in writing by the Office of the President, no person acting on behalf of NYFA shall, in the name of NYFA or through NYFA funds, assets, or membership resources, directly or indirectly provide to a foreign government, an entity owned or controlled by a foreign government, a foreign intelligence or security agency, or another foreign entity determined by NYFA to present a significant security risk:

1. Donations;
2. Funding;

3. Financial support;
4. Equipment, supplies, services; or
5. Other resources have material economic value.

Any cooperation, donation, funding arrangement, or financial transaction involving a foreign government agency or government affiliated entity shall comply with applicable U.S. law and NYFA's internal review procedures.

Article XII. Prohibition on Accepting Donations from Foreign Governments and Related Entities

To protect the independence, transparency, and information security of NYFA, NYFA shall not, directly or indirectly, accept, except as expressly permitted by applicable law and subject to review and prior approval by the Office of the President and, where necessary, legal counsel, any of the following from a foreign government, foreign government department, diplomatic or consular institution, foreign military or intelligence agency, or an entity directly or indirectly controlled by, acting on behalf of, or effectively controlled by any such entity:

1. Donations;
2. Funding;
3. Financial assistance;
4. Government grants or funds;
5. Membership dues or other forms of financial support; or
6. Equipment, supplies, services, or other benefits are of economic value.

If NYFA discovers that funds, property, or other benefits already received may have originated from any of the entities described above, NYFA shall immediately suspend the use of the relevant assets, preserve records concerning the transaction and source of the funds or property, and take appropriate steps, as permitted or required by applicable law, including return, segregation, disclosure, reporting, or other appropriate disposition.

Article XIII. Prohibition on Assisting Foreign Actors in Targeting NYFA Members and Related Persons

No person shall use an NYFA position, membership information, internal information, event information, or other NYFA resources to assist any foreign government, foreign intelligence agency, agent of a foreign government, or other foreign-based actor in:

1. Monitoring, tracking, harassing, threatening, or intimidating NYFA members, officers, employees, volunteers, or partners;
2. Unauthorized collection, organization, analysis, or transmission of personal information concerning such people;
3. Attempting to obtain members' identities, contact information, family information, employment information, legal information, or other Sensitive Information;
4. Conducting cross border retaliation, coercion, threats, or other malicious conduct against such people; or
5. Assisting foreign actors in conducting unauthorized intelligence activities or other security threats against NYFA or its members.

NYFA shall take appropriate protective, documentation, reporting, and assistance measures concerning suspected incidents described above, consistent with applicable law and the circumstances of the incident.

Article XIV. Protection and Disclosure Restrictions Concerning Member Personal Information

Without the individual's consent, a legal requirement, or formal authorization from NYFA, no person shall publicly disclose, publish, sell, transfer, or provide NYFA member personal information to an unrelated third party.

Protected information includes, but is not limited to:

1. Name;
2. Address;
3. Telephone number;
4. Email address;
5. Date of birth;
6. Identification-document information;
7. Firearms license or permit information;
8. Application information;
9. Family information;
10. Employment information; and
11. Other information capable of identifying an individual.

Any public disclosure of NYFA member information that could reasonably expose a member to harassment, threats, stalking, retaliation, or other security risks shall be treated as a significant information security incident.

Article XV. Security Incidents Suspected of Involving Foreign Actors

If NYFA has reasonable grounds to believe that NYFA, its members, officers, employees, volunteers, or partners may be affected by unauthorized intelligence activities, cross border threats, harassment, coercion, surveillance, theft of information, or other malicious conduct by a foreign government, foreign intelligence or security agency, agent of a foreign government, or other foreign based actor, NYFA shall promptly take reasonable security measures.

To the extent permitted by applicable law and warranted by the circumstances, NYFA shall preserve relevant evidence, communications records, device information, and other information that may have investigative value and shall not knowingly delete, alter, or destroy such information.

Article XVI. Reporting to and Cooperation with U.S. Federal Law Enforcement Agencies

If NYFA discovers or receives credible information indicating the possible existence of espionage, unlawful intelligence collection, cross border threats, data theft, cyberattacks, threats, coercion, or other conduct potentially violating U.S. federal law and involving a foreign government, foreign intelligence agency, agent of a foreign government, or other foreign based actor, NYFA shall, based on the nature of the incident and applicable law, report the matter to an appropriate U.S. federal law-enforcement or security agency.

Where an incident involves suspected foreign intelligence activity, threats associated with a foreign government, or other security matters within federal jurisdiction, NYFA may report the matter to the Federal Bureau of Investigation (FBI) and cooperate with an investigation to the extent permitted by law and requested by the appropriate authorities.

If a foreign government or related entity attempts to provide funding to NYFA through a third party, individual, company, foundation, or other intermediary for the purpose of influencing NYFA policies, obtaining member information, establishing a special relationship, or pursuing another undisclosed objective, NYFA shall conduct an internal review or investigation based on the nature of the matter and applicable law and, where appropriate, report the matter to the FBI or another appropriate federal authority.

NYFA shall, to the extent reasonably possible and legally required, assist federal investigations, including providing relevant documents, communications records, electronic data, and other evidence lawfully requested by the appropriate authorities.

Article XVII. Prohibition on Retaliation and Interference with Reporting

No NYFA person shall retaliate against, threaten, intimidate, demote, remove from office, or otherwise take adverse action against any member, employee, volunteer, or other related person for making a good faith report concerning suspected foreign interference, information-security breaches, threats, harassment, or other security incidents.

No person shall knowingly conceal, destroy, alter, or obstruct information or an investigation relating to such security incidents.

Article XVIII. Supremacy of Federal Law and Authority of Government Agencies

This Administrative Order constitutes an internal NYFA information security and administrative management policy and does not replace, restrict, or limit the lawful authority of federal, state, or local government agencies.

If any provision of this Order conflicts with applicable law, a federal government requirement, or a lawful order issued by a competent governmental authority, applicable law and the lawful government order shall control.

Article XIX. Interpretation and Updates

The Office of the President may periodically review and update this Administrative Order based on travel security, cybersecurity, counterintelligence, sanctions, and other relevant security information issued by the U.S. Government.

The terms “foreign government,” “foreign intelligence agency,” “agent of a foreign government,” and other related concepts used in this Administrative Order shall be interpreted in accordance with applicable U.S. federal law and the official definitions or guidance issued by the appropriate federal authorities.

Article XX. Effective Date and Continuing Effect

This Administrative Order shall take effect on September 15, 2026.

Unless formally amended, superseded, or revoked by the Office of the President of NYFA, this Administrative Order shall remain in full force and effect.



Authorization Person Name Print Ranghan Lin

Date 09/15/2016

Authorization Person Name Signature Ranghan Lin

