



The updates to the application form are as follows:

- Added three-year experience requirement to Applicant Requirements section. (Page 2)
- Removed word “primarily” from Infrastructure section. (Page 3)
- Added question to collect applicant’s years of experience with affiliated critical infrastructure (Page 3)
- Driver’s License Number and State fields are now optional, but both fields are mandatory if information is entered in either field. (Page 4)
- Removed “None” checkbox from Employment section and moved up “Are you retired?” question. (Page 6)
- Removed “Are you unemployed?” question from Employment section. (Page 6)
- Removed “Are you a student?” question from Employment section. (Page 6)
- In Criminal History section, updated language in Notice to state that Expunged records should be included in the application. (Page 8)
- Updated language in Other Affiliations section. (Page 8)
- Removed Clearance section. (Page 9)
- Removed “Help Desk Code Word” field. (Page 9)
- Removed “Have you previously been a member of InfraGard?” question. (Page 9)
- Removed “How did you hear about InfraGard?” question. (Page 9)
- Removed “Why do you want to join InfraGard?” question. (Page 9)
- Added language for adhering to the Traffic Light Protocols for information sharing in the InfraGard Information Sharing Policy section. (Page 11)
- In Appeals Process section, changed references from “NIPU” to DMCIU. (Page 14)

INFRAGARD APPLICATION AND MEMBERSHIP AGREEMENTS

APPLICANT REQUIREMENTS

- Applicant must be at least 18 years of age on the date of completion of this Application.
- Applicant must be a U.S. Citizen (U.S. Citizen by birth as defined by 8 USC 1401-1409 or a U.S. Citizen by Naturalization as defined by 8 USC 1421-1459).
- Applicant must be employed or formerly employed in a Critical Infrastructure for at least three years.
- Applicant must complete this InfraGard Membership Application Form in its entirety.
- Applicant must agree with the InfraGard Information Sharing Policy, Privacy Act Statement, Agreements to Hold Harmless and Code of Ethics.
- Applicant must consent to a security risk assessment and to periodic reconfirmation of the security risk assessment. The risk assessment is a membership vetting process completed by the FBI which includes local, state, and federal criminal history and driver's license, citizenship, and other security-related database checks. Note that successful completion of the security risk assessment does not equate to a security clearance (InfraGard members are not given security clearances by the FBI).

INFRAGARD MEMBERSHIP is for the owners, operators, and security directors and their staffs of the 16 U.S. national key asset and critical infrastructure sectors, which includes members of local, state, and federal law enforcement, as well as individuals who are involved in the security of and protected research at educational institutions. A description of the critical infrastructure sectors, and the disciplines included within each one, can be found on the main InfraGard website. The 16 critical Infrastructure sectors as set forth in Presidential Policy Directive (PPD)-21 are as follows:

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials and Waste
- Transportation Systems
- Water and Wastewater Systems

The mission of InfraGard is to promote ongoing dialogue and timely communication between members and the FBI specifically concerning the security of, vulnerabilities in, and threats to critical infrastructure entities. InfraGard members are provided with information to assist them in protecting critical infrastructure assets. In turn, they are encouraged to provide information to the FBI, thereby facilitating its responsibilities to detect, deter, and investigate acts of terrorism and other crimes. Because of the focus and purpose of InfraGard, its members are required to be affiliated with at least one critical infrastructure sector and, as part of the application process, applicants must pick a primary affiliation sector.

INFRASTRUCTURE

With which critical infrastructure sector are you affiliated? (mandatory drop down – choose one)

How many years of experience do you have with your affiliated critical infrastructure? (mandatory drop down – choose one)

PERSONAL AND CONTACT INFORMATION

Full Name (Enter your official full name below, not a nickname.):

First Name (mandatory field)

Middle Name (If you do not have a middle name, enter NMN.) (mandatory field)

Last Name (If you are a “Jr.,” “Sr.,” etc. enter this here as well.) (mandatory field)

Home Address, City, State, Zip (mandatory fields)

Home Phone / Cell Phone (one phone number is required)

Home Email / Confirm Email (home or business email (below) must be provided)

DOB (mandatory field - provide required format mm-dd-yyyy – application should not allow anyone to apply if they are not yet 18 years old.)

SSN (mandatory field – entry of 000-00-0000 or similar string should not be allowed)

POB (City/County (optional short field)/State (optional short field) /Country/Other (optional short field))

DL#/State (optional, but both fields are mandatory if information is entered in either field – DL field must allow for all types of special characters)

CITIZENSHIP

Check the box that reflects your current citizenship status and provide the applicable documentation:

I am a U.S. Citizen or national by birth in the U.S. or a U.S. territory/commonwealth. Do one of the following:

- **Provide your U.S. Passport Number (Current): (optional short field)**
 - o Expired (y/n) o Date issued (mm/dd/yyyy)
- **Appear in person at the nearest FBI office, with a certified copy of your birth certificate and a government photo ID, such as a driver's license. Contact your local InfraGard Coordinator to make an appointment.**

I am a U.S. citizen or national by birth, born outside the U.S. Provide one of the following:

- **U.S. Passport Number (Current): (optional short field) o Expired (y/n) o Date issued (mm/dd/yyyy)**
- **Document Number from State Department Form FS 240, DS 1350, FS 545, etc.: (optional short fields for form type and number) o Date form was completed (optional mm/dd/yyyy) o Place of issuance (optional short field)**

I am a naturalized U.S. citizen. Provide one of the following:

- **U.S. Passport Number (Current): (optional short field) o Expired (y/n) o Date issued (mm/dd/yyyy)**
- **Citizenship Certificate Number (if applicable): (optional short field) o Where was the citizenship certificate issued (City/Court/State)? (optional short field) o Date issued (optional mm/dd/yyyy)**
- **Naturalization Certificate Number (if applicable): (optional short field) o Where was the citizenship certificate issued (City/Court/State)?**

(optional short field) o **Date issued**

(optional mm/dd/yyyy)

EMPLOYMENT

Employer

Are you retired? (y/n) If you are retired, provide the name of your last employer that was related to a critical infrastructure, job title, city, state, and year of retirement.

Employer Name (Mandatory field unless applicant is retired. If self-employed, fill out below contact information and self-employed section.)

Job Title (Mandatory field unless applicant is retired)

Employer Address, City, State, Zip (Mandatory field unless applicant is retired)

Employer Website (optional field)

Business Phone / Cell (Mandatory unless applicant is retired)

Business Email / Confirm Email (home (above) or business email must be provided)

Are you self-employed? (y/n) If you are self-employed, provide a short description of the nature of your business, how it relates to a critical infrastructure, and your website address (if you have one).

MILITARY SERVICE

Have you EVER served in the US Military or US Merchant Marine? (y/n)

- If “yes,” which branch and what were your dates of service? (optional short field)
- Have you EVER received a discharge that was not honorable? (y/n)
 - o If “yes”, provide an explanation about the discharge, making sure to include information that you feel would assist us in making a membership decision. (paragraph field)

CRIMINAL HISTORY

Have you ever been arrested for, charged with, or convicted of a felony, misdemeanor, Driving Under the Influence (DUI), or Driving While Intoxicated (DWI)? Exclude minor parking and traffic violations such as parking and non-reckless speeding tickets, but do not exclude reckless driving or other major moving violation arrests, charges, or convictions. (y/n)

- If “yes,” enter an explanation of the occurrence(s), making sure to include dates, law enforcement agencies involved, and any additional information that you feel would assist us in making a membership decision. (paragraph field)

If you were in the military, have you been subject to court martial or disciplinary proceedings under the Uniform Code of Military Justice? (y/n)

- If “yes,” enter an explanation of the occurrence(s) making sure to include dates, military branch of service and/or agencies involved, and any additional information that you feel would assist us in making a membership decision. (paragraph field)

Notice: If you check “no” for either of the above questions and the criminal history check reveals information to the contrary, including DUI/DWI’s or records that you thought had been expunged, such omission will be grounds for your application to be automatically disqualified. Please report arrests, charges, or convictions that you believe to have been expunged as records you believe to be expunged may not be, and/or they may still appear in your criminal history. Please consider this in your responses, as apparent omissions on your part will be grounds for your application to be automatically disqualified.

Should I be approved as an InfraGard member, I agree to self-report any arrests, charges, or convictions for criminal activity, including DUI/DWI incidents, while an InfraGard member to the local InfraGard Coordinator. I understand that minor parking and traffic violations such as parking and non-reckless speeding tickets do not need to be reported, but reckless driving or other major moving violations do need to be reported.

OTHER AFFILIATIONS

List other professional, community or social organizations that are you affiliated with that promote/advance the security of critical infrastructure: (optional paragraph field)

INFRAGARD CHAPTER

Choose Chapter (drop down)

Have you applied to InfraGard before? (y/n)

- If “yes,” and you were not accepted for membership, what was the reason provided for your not being accepted? (paragraph field)

INFRAGARD CODE OF ETHICS

As an InfraGard member I will do all of the following:

- Promote the protection of the critical infrastructure of the United States of America.
- Cooperate with others in the interchange of knowledge and ideas for mutual protection, and participate in local, regional, and national InfraGard events to the best of my ability.
- Support the education of members and the general public about the importance of the security of and threats to the U.S. critical infrastructure.
- Serve the interests of InfraGard and the general public in a diligent, loyal, and honest manner, and not knowingly be a party to any illegal or improper activities that endanger the U.S. critical infrastructure.
- Maintain the confidentiality, and prevent the use for competitive advantage at the expense of other members, of information obtained in the course of my involvement with InfraGard, which may include information concerning the business of a fellow member or company and information identified as proprietary, confidential, or sensitive.
- Not commercially exploit InfraGard or use it as a forum to market products or services.
- Not use my affiliation with InfraGard to elicit special privileges.
- Act in a manner consistent with the InfraGard National Members Alliance (INMA) Bylaws and the local InfraGard Members Alliance (IMA) Bylaws, understanding that the Bylaws may be amended from time to time, as well as any other duly enacted national or local requirements of InfraGard.
- Protect and respect the privacy rights, civil rights, and physical and intellectual property rights of others.

I agree to abide by the InfraGard Code of Ethics and understand that not doing so may result in the revocation of my membership in InfraGard. (mandatory check box)

INFRAGARD INFORMATION SHARING POLICY

InfraGard members may receive information that is sensitive and not publicly available. This information may be provided by or through the FBI, the InfraGard National Members Alliance, a local InfraGard chapter, another InfraGard member, partners of InfraGard, or other sources. All members must adhere to the “Traffic Light Protocol” for sharing/disseminating information. Note that members are not obligated as a condition of InfraGard membership to disclose any information to the FBI, the InfraGard National Members Alliance, or any InfraGard chapter, member or partner; however, the key mission of InfraGard is the effective exchange of information in order to protect the nation’s critical infrastructure and such a goal cannot be optimally achieved if InfraGard members do not choose to share information.

All members must understand and agree to the following terms regarding information received or provided through InfraGard:

- **Non-Disclosure:** Information obtained through InfraGard shall not be released beyond its intended scope of disclosure, as established or understood, formally or informally.
- **FBI Disclaimer:** The FBI provides information to InfraGard members as a service and for informational purposes only. While the FBI strives to make this information as timely and accurate as possible, it cannot provide any warranties, and expressly disclaims liability, for the accuracy of information disseminated through InfraGard. The member acknowledges that he/she must use his/her own judgment in assessing the nature and accuracy of all InfraGard-related information and agrees to assume all risk for taking, or not taking, any action(s) based on such information.
- **Submission in Good Faith:** Applicant agrees that he/she will submit information only to further the purpose of InfraGard and will not submit information which he/she knows to be false.
- **Protection of Information from Disclosure:** To the extent appropriate, reasonable, and allowed by law, the FBI agrees that proprietary information received from InfraGard members and marked as “trade secrets” or “proprietary information” shall be protected from mandatory agency disclosure under 5 USC 552(b)(4) (“Exemption 4”), the Freedom of Information Act (“FOIA”), and from publication, divulgence, or release in any other manner pursuant to 18 USC 1905, the Trade Secrets Act.

I understand and agree to the InfraGard Information Sharing Policy and understand that not following such a policy may result in the revocation of my membership in InfraGard. (mandatory check box)

PRIVACY ACT STATEMENT

Authority: Collection of the information on this form is authorized under 28 USC 534 and 28 CFR 0.85.

Principal Purpose and Routine Uses: The information collected on this form will be used for the principal purpose of conducting security risk assessments on InfraGard applicants and members. As part of this assessment, the collected data may also be used to assist in determining approval, denial, revocation, or renewal of access to the IG Network and the authorization to receive information through InfraGard. The information provided will be protected and used in strict compliance with the Privacy Act and the routine uses most recently published in the Federal Register for the FBI's Central Records System (Justice/FBI-002) and the FBI's Blanket Routine Uses (Justice/FBI-BRU).

Social Security Account Number: Your Social Security Account Number (SSAN) is requested to check criminal, immigration, national security, and other electronic databases. It will be used to facilitate accurate identification and to help eliminate the possibility of misidentification.

Effects of Non-disclosure or Falsification: Completion of this application and provision of your SSAN is voluntary. However, failure to provide the requested information may result in your application being rejected. Knowingly falsifying or concealing information requested on this form will result in your application being rejected or your membership revoked. In addition, 18 USC 1001, provides that knowingly falsifying or concealing a material fact may under certain circumstances constitute a felony resulting in fines and/or imprisonment.

I understand and agree with the Privacy Act Statement. (mandatory check box)

AGREEMENTS TO HOLD HARMLESS

Agreement to Hold Harmless the U.S.: The applicant agrees not to institute, initiate, prosecute, or in any way aid in any demand, action, suit, or other claim, legal or otherwise, against the FBI, the Department of Justice, or the United States, or the officers, employees, agents, representatives, task force members, contractors/subcontractors, consultants, or advisors thereof, on account of any damage, loss, injury, or expectation arising from, in connection with, or in any way pertaining to the reporting, non-reporting, or use of information in accordance with this agreement.

Agreement to Hold Harmless Other InfraGard Members: The applicant agrees not to institute, initiate, prosecute, or in any way aid in any demand, action, suit, or other claim, legal or otherwise, against any other InfraGard member on account of any damage, loss, injury, or expectation arising from, in connection with, or in any way pertaining to the reporting, non-reporting, or use of information in accordance with this agreement, and the member further expressly agrees to hold harmless and indemnify the same against loss from any and all claims that may hereafter be brought against the same by applicant arising out of the reporting, non-reporting, or use of information.

I understand and agree to the Agreements to Hold Harmless.

APPEALS PROCESS

An applicant who is denied InfraGard membership will be notified via e-mail. Should the applicant wish to request additional information and/or appeal the decision, he/she must send a letter to the Data Management and Critical Infrastructure Coordination Unit (DMCICU) at FBI Headquarters via postal mail within 60 days of having received the e-mail. The e-mail will contain specific instructions about what to include in the letter, as well as the DMCICU mailing address. A letter of appeal must address the specific reason(s) for denial. All subsequent communications regarding the membership decision will be exchanged via postal mail.

I understand the Appeals Process.

CONSENT

By completing an InfraGard Membership Application Form, I hereby authorize the FBI to obtain and verify any information relevant to assessing my suitability to access, possess, use, receive, or transfer information obtained through InfraGard. I further authorize the FBI to disclose information obtained in connection with my security risk assessment to appropriate national security and law enforcement partners in order to determine my suitability for membership in InfraGard. I understand that the FBI will use all information provided on this application and through the record checks completed during the security risk assessment to make a decision on my membership. I also understand that, should I be approved for membership, the FBI will utilize the information I have provided herein to conduct periodic reassessments of my suitability to remain an InfraGard member.

I understand that the FBI retains sole authority and discretion to accept, deny, or revoke the membership of any InfraGard member. I understand that I may cancel my membership at any time upon written notice to the local InfraGard Coordinator or National Membership Coordinator.

I understand that this is a legally binding document and false statements provided by me are violations of federal law and could lead to criminal prosecution or other legal action. To the best of my knowledge and belief, I affirm that I meet all of the requirements to apply to be an InfraGard member and that the information I have provided herein is true, complete, and correct.

I consent to the security risk assessment and to periodic reassessments.
(mandatory check box)

Provide option for applicant to either print or save completed application.