**SUPPORTING STATEMENT**

**1110-0049 COLLECTION**

***INFRAGARD APPLICATION AND MEMBERSHIP PROFILE QUESTIONNAIRE***

A. Justification.

1. Necessity of Information Collection

This collection, the member profile questionnaire, is authorized by 28 U.S.C. Sec. 533, which directs the Attorney General and its Justice Department entities, including the FBI, to detect and prosecute crimes against the United States.

For ongoing participation in InfraGard, members must complete the member profile questionnaire providing information that indicates respondents’ knowledge, skills, and abilities, to be used by FBI representatives to query the membership. This profile stores member information on business type and size, professional associations/certifications, and areas of expertise and interests. This information is necessary to categorize the respondents into groups based on their industry, expertise, knowledge and skills. Moreover, because access to InfraGard information is role-based and granted on a need-to-know basis, this collection is necessary to ensure that members are given access only to information relevant to their expertise and necessary for their roles.

InfraGard is a Public/Private Alliance that operates 7 days a week, 24 hours a day (7 X 24) on-line (real-time), controlled-access communications and information sharing data repository that is owned by the Federal Bureau of Investigation (FBI) Cyber Division (CyD). The purpose of the InfraGard program is to share intelligence and criminal information between the FBI and the private sector about cyber threats and infrastructure vulnerabilities. InfraGard is accessed by vetted and authorized entities using industry-standard personal computers equipped with any standard Internet browser who access a secure website, where members can communicate securely. It provides an internet accessible focal point for electronic Sensitive but Unclassified (SBU), For Official Use Only (FOUO), Unclassified, and Law Enforcement Sensitive (LES) communications and information sharing for the InfraGard members.

As part of its mission, the FBI conducts outreach and information sharing with the public and private-sector owners and operators of critical infrastructures. The InfraGard Program establishes a mechanism for two-way information sharing about intrusion incidents and system vulnerabilities and provides a channel for the FBI to disseminate analytical threat products to the private sector. The InfraGard secure website was designed to provide InfraGard members information about intrusions and infrastructure protection measures, access to original research issues, and the capability for members to communicate with each other about similar security interests through secure channels. InfraGard also supports anti-terrorism, intelligence, law enforcement, criminal justice, and public safety communities nationwide.

The InfraGard system was developed in concert with the FBI and the Information Analysis and Infrastructure Protection Directorate (IAIP) of the Department of Homeland Security to address cyber and physical threats within the United States. The FBI in conjunction with representatives from the private industry, the academic community, and the public sector, further developed the InfraGard initiative to expand direct contacts with the private sector infrastructure owners and operators and to share information about cyber intrusions, exploited vulnerabilities, and infrastructure threats. All 56 field offices of the FBI have opened an InfraGard chapter.

A revision of this currently approved collection is requested in addition to a 3-year extension.

The revisions on the existing form are:

* + - PAGE #1

Date Change

5/01/2014

Seals Added

The FBI and InfraGard seals were added.

Opening

The document previously with the beginning of the application, it now begins with the Applicants Requirements which have also changed to reflect the following statements:

Previously collection advised **-** At least 18 years of age on the date of completion of this Application; Consent to a records check that yields a satisfactory result as determined by the FBI in its sole discretion; Consent to periodic re-confirmation of membership requirements; Agree to and complete this InfraGard Membership Application Form; Any further requirements (if more restrictive) mandated by the local chapter and approved by the FBI.

Changed **-** 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 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 re-confirmation 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.)

All personal identifiable information (PII) will be collected and maintained by the FBI and is strictly used for identification purposes only during the vetting process. This information will be held in a secure repository on the InfraGard Network and will not be provided to outside entities under any circumstances. Based on the information provided, members will be vetted for membership, assigned to critical infrastructure sectors and provided access to “for official use only” (FOUO) and law enforcement sensitive information regarding their sector assignment.

* + - PAGE #2

Previously there was no page #2, a page has been added to advise members of the InfraGard program as follows:

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

The FBI utilizes the SSAN of the InfraGard member applicant for two specific operational reasons: 1. To make specific identification of the individual during the background check to determine the eligibility of the individual to join the InfraGard program. As a national-level program, InfraGard membership applicants may have common names with shared date of birth. In order to ensure the background investigation accurately reflects the specific individual, SSAN is utilized as part of the background search and confirmation of the applicants. The inclusion of the SSAN will also minimize the delay or denial of membership due to mis-identity issues. 2. SSAN of InfraGard members are utilized to obtain security clearance when needed to allow InfraGard members to access information that may be classified or to access facilities that may require clearance under certain programs and circumstances.

* + - PAGE #3

Middle Name Added- to more specifically identify applicant.

Surname Request Added - to more specifically identify applicant.

Home Email / Confirm Email Request Added **-** We made entering an email mandatory on this application to better maintain contact with the applicant.

Request for Citizenship Added**-** We asked if an applicant was a US citizen on the old application, however we did not ask for any further information or documentation of the answer, i.e., passport, or other citizenship-related information was not requested on the old application. We are asking for it in this application so that we verify US citizenship as part of the security risk assessment. InfraGard members are required to be US citizens. Changes are as follows:

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. Provide the following (if you have one):

* U.S. Passport Number (Current): (optional short field)
  + Expired (y/n)
  + Date issued (mm/dd/yyyy)

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)
  + Expired (y/n)
  + Date issued (mm/dd/yyyy)
* Document Number from State Department Form FS-240, DS-1350 or FS-545: (optional short fields for form type and number)
  + Date form was completed (optional mm/dd/yyyy)
  + 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)
  + Expired (y/n)
  + Date issued (mm/dd/yyyy)
* Citizenship Certificate Number (if applicable): (optional short field)
  + Where was the citizenship certificate issued (City/Court/State)? (optional short field)
  + Date issued (optional mm/dd/yyyy)
* Naturalization Certificate Number (if applicable): (optional short field)
  + Where was the citizenship certificate issued (City/Court/State)? (optional short field)
  + Date issued (optional mm/dd/yyyy)
    - * PAGE #4

Employer Website Request Added **-** Since we are asking that each InfraGard member be affiliated with a critical infrastructure, the answer to this question will help us to verify if that is true. It will also help verify if the applicant works for a legitimate company.

* + - PAGE #5

Business Email / Confirm Email Request Made Mandatory **-** We made entering an email mandatory on this application to better maintain contact with the applicant.

Are You Self-Employed Question Added **-** We are asking that each InfraGard member be affiliated with a critical infrastructure, the answer to this question will help us to verify if that is true.

Are You Retired Question Added**-** We are asking that each InfraGard member be affiliated with a critical infrastructure, the answer to this question will help us to verify if that is true.

Are You Unemployed Question Added - This question will help us to verify if that is true.

Are You A Student Question Added **-**  The answer to this question will help us to verify if that is true.

Have you EVER served in the US Military or US Merchant Marine Question Added -

* 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)
  + 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)

All the questions about military service are new. Since the military is part of the defense industrial base critical infrastructure, we felt it necessary to know if our members are, or ever were, in the military. Knowing this, if they had disciplinary issues in the military, and how they were discharged, will also assist us with the security risk assessment.

* + - PAGE #6

Have You Ever Had a Security Clearance Question Added This is an important part of the security risk assessment to know if the applicant has, or ever had, a security clearance.

With What Other Professional, Community or Social Organizations Are You Affiliated Question Added This will help us understand how involved the applicant already is in critical infrastructure security, or if he/she has interests which are in conflict with the InfraGard mission.

Have You Previously Been a Member of InfraGard Question Added

* If “yes,” which Chapter(s) and time frame? (optional short field)
* If “yes,” then skip next question.

This will help us cut down on administrative work with regard to processing the application.

Have You Applied to InfraGard Before Question Added

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

This will help us cut down on administrative work with regard to processing the application, and will assist us with the security risk assessment.

How Did You Hear About InfraGard Question Added

Check all that apply. (drop down: Colleague, Meeting Announcement, Presentation, Flyer, Other (include short field to describe what “other” is)

This will help us understand how well we are marketing the program and if we are marketing it to the appropriate organizations, or through appropriate channels.

Why Do You Want to Join InfraGard Question Added

Check all that apply. (drop down: Assist with the Protection of U.S. Critical Infrastructure, Networking, Liaison with FBI, Liaison with Other LE, Attend Meetings, Access IG Network, Access iGuardian, Participate on National or Local Board, Other (include short field to describe what “other” is)

This will help us to determine if the applicant intends to be an active or passive member of InfraGard, and/or if he/she is joining for reasons that are in line with the InfraGard mission.

2. Needs and Uses

The purpose of collecting the information listed in the questionnaire is to categorize approved applicants (members) according to their expertise. In times of need, individuals with specific expertise can be located and contacted for their assistance.

3. Use of Information Technology

The questionnaire will be filled out on-line on a FBI owned secure website by the member and processed electronically by the Criminal Justice Information System (CJIS). This system is being used to provide greater access to the public by using the Internet as well as reducing the paperwork involved in the process.

4. Efforts to Identify Duplication

The InfraGard program is the only FBI public outreach program that vets and categorizes its members. The information contained in the questionnaire is needed to be able to properly categorize the members. InfraGard is not aware of any other program collecting this information.

5. Minimizing Burden on Small Businesses

This information will have no significant impact on small entities. No small business will be affected by this collection.

6. Consequences of Not Conducting or Less Frequent Collection

If the questionnaire were not used, then the program would be unable to identify a member’s expertise. InfraGard’s purpose to the FBI is to leverage a member’s expertise for national critical infrastructure protection. These individuals are experts in their fields. There may be instances when the FBI needs to contact these experts during times of crisis. Without the ability to identify these experts through the questionnaire process, the FBI will not be able to locate members when needed, or ensure that members are not given more information than what is relevant to their areas of expertise.

7. Special Circumstances

The member will complete the questionnaire once, which will create a profile that the member can update as needed.

8. Public Comments and Consultations

The 30 and 60 day notices was published with no comments received.

.

9. Provision of Payments or Gifts to Respondents

The InfraGard Program has not provided any gifts or payments to participants.

10. Assurance of Confidentiality

For site security and confidentiality purposes, and to ensure that this service remains available to all users, all network traffic is monitored in order to identify unauthorized attempts to upload or change information, or otherwise cause damage or conduct criminal activity. To protect the system from unauthorized use and to ensure that the system is functioning properly, individuals using this computer system are subject to having all of their activities monitored and recorded by personnel authorized to do so by the FBI (and such monitoring and recording will be conducted). Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals evidence of possible abuse or criminal activity, system personnel may provide the results of such monitoring to appropriate officials. Unauthorized attempts to upload or change information, or otherwise cause damage to this service, are strictly prohibited and may be punishable under applicable federal law.

Privacy risks identified pertain to the on‑line application via the Internet; in particular, unauthorized access to data and the unnecessary full display of user information were noted as concerns. The process of Certification and Accreditation (C&A) in accordance with the FBI Security Division (SecD), Information Assurance Section, verifies adequate security features are in place to protect the system and the data maintained in it. To mitigate the risks of unauthorized access, role based access controls have been implemented, based on membership classification. Access to information is based on a need-to-know basis. Privileged users are granted specific role based permissions to access and view information in accordance with their "need to know". When privileged users require information, only minimum relevant and required information is displayed. Although Social Security numbers are collected for purposes of vetting, they are not displayed except to FBI personnel who need access in order to do the background checks. Consent is obtained from those who provide information and is shared only consistent with that consent. Members have access to their individual profiles that they can update as needed.

11. Justification for Sensitive Questions

Sensitive questions are used to identify and qualify a person's expertise.

12. Estimate of Applicant's Burden

We estimated the applicant's burden for this data collection as follows:

Number of questionnaires annually 7,200

Frequency of responses 1 per application

Total annual questionnaires 7,200

Minutes per response 30 minutes electronic

Annual hour burden 3600 hours

Current InfraGard members will be required to complete the questionnaire for continued InfraGard membership. This will be a one-time task taking approximately 30 minutes to complete.

Means of Submitting Members Frequency Response Time Annual hour burden

Electronically 30,000 1 time 30 min 27,500

(30,000 X 1 X 30)/60 = 15,500 hours

13. Estimate of Cost Burden

Members will not incur any costs other than their time to respond. Members are not expected to incur any capital, start-up, or system maintenance costs associated with this information collection.

14. Cost to Federal Government

The estimated cost to the federal government for this data collection is $250,000 based on operational cost of managing the InfraGard Network. In addition, there is a cost associated with help desk operations. The estimated cost of initial capture of information online and storing in an FBI owned and controlled electronic database. This additional cost for Help Desk personnel is $63,192.66.

InfraGard Website Operations and Maintenance: $250,000.00

10% of Help Desk Salary to include application collection and Filing: $63,192.66

Total $313,192.66

15. Reason for Change in Burden

The existing collection has changed since the last submission due to NIPU’s purge of inactive members from the new InfraGard website. This resulted in a reduction in the membership from 55,000 to 30,000. At that time, the NIPU in partnership with InfraGard developed a marketing strategy to recruit a more robust membership with technical and industry professionals, also resulting in an increase in applications from 5,500 to 7,200.

16. Anticipated Publication Plan and Schedule

The questionnaire will be used in a systems upgrade of the InfraGard secure website. Once approved, it will be utilized immediately and the information will be collected and placed in a database.

17. Display of Expiration Date

All information collected under this questionnaire will display the OMB Clearance Number.

18. Exception to the Certification Statement

The InfraGard Program does not request an exception to the certification of this information collection.

B.. Collection of Information Employing Statistical Methods.

The information will not be used for statistics on a regular basis. The information collected will be contained in a database which may be used in an ad-hoc report as needed.