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) Office of Private Sector (OPS). The purpose of the InfraGard program is to share intelligence and criminal information between the FBI and the private sector about 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.

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	Applicants	Frequency	Response Time	Annual hour burden
Electronically	7,200	1 time	30 min	3,600

(7,200 X 1 X 30)/60 = 3,600 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 SIU's purge of inactive members from the new InfraGard website. This resulted in a reduction in the membership from in a rise in applications from 30,000 to 50,000 or approximately 7,200 applicants per year.

16. Anticipated Publication Plan and Schedule

The questionnaire is currently being used on the InfraGard secure website. Once approved, it will continued to be utilized for information collection.

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.

19. 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 internal reports as needed.