



11350 Random Hills Road, Suite 800, Fairfax, Virginia 22030 Phone (703) 934-6101 Fax (703) 352-3678

fff@fff.org www.fff.org

InfraGard: An Unhealthy Government Alliance **by Gary D. Barnett**

There is an organization that is quietly and secretly becoming very large and powerful. The FBI started this partnership or alliance between the federal government and the private sector in 1996 in Cleveland with a few select people. After September 11, 2001, when the general population replaced their rationality with fear, this organization, called InfraGard, continued growing, and with little notice. By 2005 more than 11,000 members were involved, but as of today, according to the InfraGard website, there are 23,682 members, including FBI personnel. At first glance, many would think this alliance healthy and useful in the fight against “terrorism,” but upon further examination, one has to wonder.

InfraGard began as an alliance between the FBI and local businesses with the objective of investigating cyber threats. Since that time, little resemblance to that design exists. According to InfraGard’s own website,

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the Federal Bureau of Investigation and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and participants dedicated to sharing information and *intelligence* [emphasis added] to prevent hostile acts against the United States.

Every InfraGard chapter has an FBI special agent coordinator attached to it, and this FBI coordinator works closely with FBI headquarters in Washington, D.C. Initially, while under the direction of the National Infrastructure Protection Center (NIPC), the focus of InfraGard was cyberinfrastructure protection, but things have gotten much more interesting since September 11, 2001. NIPC then expanded its efforts to include *physical* as well as cyberthreats to critical infrastructures.

A progression is occurring, but it gets even more interesting as time passes. In March 2003, NIPC was transferred to the Department of Homeland Security which now has total responsibility for critical infrastructure protection (CIP) matters. Part of the Department of Homeland Security's mission is to facilitate InfraGard's continuing role in CIP activities and to further develop InfraGard's ability to support the FBI's investigative mission, especially as it pertains to counterterrorism and cyber crimes.

InfraGard's stated goal "is to promote ongoing dialogue and timely communications between members and the FBI." Pay attention to this next part:

InfraGard members gain access to information that enables them to protect their assets and in turn give information to government that facilitates its responsibilities to prevent and address terrorism and other crimes.

I take from this statement that there is a distinct tradeoff, a tradeoff not available to the rest of us, whereby InfraGard members are privy to inside information from government to protect themselves and their assets; in return they give the government information it desires. This is done under the auspices of preventing terrorism and *other crimes*. Of course, as usual, "other crimes" is not defined, leaving us to guess just what information is being transferred. Since these members of InfraGard are people in positions of power in the "private" sector, people who have access to a massive amount of private information about the rest of us, just what information are they divulging to government? Remember, they are getting valuable consideration in the form of advance warnings and protection for their lives and assets from government. This does not an honest partnership make; quite the contrary.

In my article ["The New Crime of Thinking."](#) I criticized H.R.1955 and Senate 1959, which, if passed, will literally criminalize thought against government. As usual, the exact type of thought is left undefined. This vagueness in the thought-crime legislation together with the secrecy of InfraGard makes for a dangerous combination. S.1959, if passed, will be attached to the Homeland Security Act and InfraGard is already a part of the Department of Homeland Security. This is not a coincidence. Under section 899b of S.1959 it is stated:

Preventing the potential rise of self radicalized, unaffiliated terrorists domestically cannot be easily accomplished solely through traditional Federal intelligence or law enforcement efforts, and can benefit from the incorporation of State and local efforts.

This appears to be a direct reference to the InfraGard program. Moreover, in section 899c of S.1959 the new commission created after passage is to build upon and bring together the work of other entities, and will establish, as designated under 899d, a "Center of Excellence." This

center will be university-based, and is to study “violent radicalization and homegrown terrorism” in the United States. According to InfraGard’s mission statement, it is a group of businesses, academic institutions, state and local law enforcement, and other participants dedicated to sharing information and intelligence. Keep in mind that this new center will be, and InfraGard already is, a part of the Department of Homeland Security. I’m just speculating, of course, but is it possible that InfraGard will be a domestic police and spying arm for the government concerning “thought crime”?

There is a definite and natural link here, and it should give us pause. The definitions concerning thought crime are vague and unclear, left to the interpretation of government only. InfraGard, on the other hand, is an organization cloaked in secrecy. It holds secret meetings with the FBI. It also, according to FBI Director Robert Mueller, shares information (what information, we don’t know) with the Secret Service and *all* government agencies involved with security in the United States.

One question on InfraGard’s application for membership is, Which critical infrastructures does your organization belong to? Some choices listed are defense, government, banking and finance, information and telecommunications, postal and shipping, transportation, public health, and energy. At least 350 of the Fortune 500 companies have representation in InfraGard, this according to their website. These representatives have access to most of our private records, including phone and Internet use, health records, and banking and finance records. Considering the recent attempts by President Bush and his administration to protect many telecommunications companies and executives from prosecution for releasing private information, how many of the top telecom executives are members of InfraGard? I, for one, would be very interested in this information, but alas, it is not public information; it is secret.

According to InfraGard’s own policies and procedures,

The interests of InfraGard must be protected whenever presented to non-InfraGard members.

Independent of the type of presentation, (interview, brief, or published documentation) the InfraGard leadership and the local FBI representative should be made aware of the upcoming presentation. The InfraGard member and the FBI representative should agree on the theme of the presentation. The identity of InfraGard members should be protected at all times.

This means that no one outside InfraGard is to know who is a member unless previous approval has been given. In addition, when interviews with members of the press are forthcoming, all questions should be submitted in writing prior to the interview. The InfraGard leadership and the local FBI representative should review the submitted questions, agree on the character of the answers, and identify the appropriate person to be interviewed prior to the

interview. Even demeanor is addressed in this directive, and strict guidelines for behavior are listed. You see, when I said secret, I wasn't kidding.

The bottom line is this: This is an organization created by the FBI, sanctioning individuals from the private business sector to provide information, sensitive and private information, to government agencies for special concessions. These concessions, or favors, according to an article titled "The FBI Deputizes Business," in *The Progressive* magazine, include advance warning on a secure portal about any threatening information related to infrastructure disruption or terrorism. InfraGard notes as much on their website by advertising for members "access to an FBI secure communication network complete with VPN encrypted website, webmail, listservs, message boards and much more." Also advertised: "Learn time-sensitive, infrastructure related security information from government sources such as DHS [Department of Homeland Security] and the FBI." Is this elitist group of InfraGard members a group of Americans superior to the rest of us? Are they truly privileged or just selling their souls for protection and favors? And how involved will they be in watchdog activities, activities sanctioned by the U.S. government? Is this a new kind of conscription by government meant to increase its surveillance capabilities so that it can monitor our lives even more than it does now?

Legislation, bureaucracies, and government/business partnerships created since 9/11 have severely infringed our freedom. Almost all of the so-called terror-protection legislation has been linked — and in many cases it is linked — to increased government oversight of the rest of us. This is evident concerning InfraGard and the Department of Homeland Security. If this program is for the benefit of this country, why are the members' names and their activities kept so secret? Why do some gain protection and early warning while the rest of us do not? And what information and "intelligence" is being shared? Since these business members are fully protected by government, how far will they go, and when will it be too late to stop this secret assault by this behemoth we call government?

Gary D. Barnett is president of Barnett Financial Services, Inc., in Lewistown, Montana.

This article was originally published in February 2008.