OFFICE OF
CHIEF COUNSEL

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

November 19, 1999

Number: **200002046**
Release Date: 1/14/2000
UILC: 6103.00-00
GLS-506805-99

MEMORANDUM FOR REGIONAL COUNSEL
NORTHEAST REGION CC:NER
ATTN: [redacted]

FROM: DAVID L. FISH
Chief, Branch 4
Disclosure Litigation CC:EL:D:Br4

SUBJECT:

This is in response to your fax dated August 20, 1999. This document is not to be cited as precedent.

ISSUE(S): Whether the IRS Criminal Investigation Division can participate in an organization identifying, investigating and preventing computer crimes, known as InfraGard.

CONCLUSION(S): To the extent the IRS elects to join InfraGard, consideration must be given to Internal Revenue Code section 6103 and the limitations it places on the IRS' ability to share information with other group members, as well as the protection it may impose on information the IRS receives from other InfraGard members. Privacy Act limitations must also be assessed.

FACTS: Your office received a memorandum from the Chief, Criminal Investigation Division of the Ohio District, providing that his office would like to participate in InfraGard as a formal member, and looked to your office to address any legal issues raised by CID's participation in the group. The Chief (CID) forwarded a memorandum from one of his employees describing InfraGard and forwarding a copy of the Secure Access Member Agreement that IRS CID would have to execute in order to become a member of the group.

The CID employee's memorandum states that InfraGard is an association of computer professionals in both the private and public sectors working together to protect the nation's information infrastructure. It is a vehicle for communicating information relative to ongoing computer security breaches whose members share information on how to prevent computer system intrusions and properly address

intrusions that do occur. There will also be a multi-agency computer crime task force organized by the U.S. Attorney's office in Cleveland that will be working with the Cleveland InfraGard chapter, charged with criminally investigating those who have committed computer crimes with the goal of prosecution.

The CID memorandum provides that most crimes, including computer crimes, use financial gain as a primary motive, so that the possibility of IRS violations exists. The memorandum also notes that through involvement in InfraGard, the IRS would maintain a high degree of visibility with regard to criminal activity involving the banking and financial infrastructure of this country.

Three requirements must be met to be a member of InfraGard. IRS CID must sign a Secured Access Member Agreement (SAM), a confidentiality pledge and make an active participation commitment. We have been provided a copy of the SAM, but not the confidentiality pledge or the active participation commitment.

LAW AND ANALYSIS: The goal of Infragard, as stated in the information provided to us, is the flow of information. Information in the IRS' custody may be confidential returns or return information protected from disclosure by Internal Revenue Code § 6103. Returns as defined by I.R.C. § 6103(b)(1) include tax or information returns, estimated tax declarations, or refund claims, and any amendments, including supporting schedules, attachments, or lists which are supplemental to or part of the return, which are required by, provided for, or permitted by Title 26 and which are filed with the Secretary by, or on behalf of, or with respect to any person. Return information is defined by I.R.C. § 6103(b)(2) as

> a taxpayer's identity, the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, overassessments, or tax payments, whether the taxpayer's return was, is being, or will be examined or subject to other investigation or processing, or any other data, received by, recorded by, prepared by, furnished to, or collected by the Secretary with respect to a return or with respect to the determination of the existence, or possible existence, of liability (or the amount thereof) of any person under this title for any tax penalty, interest, fine, forfeiture, or other imposition or offense...

The IRS can not share protected returns or return information with Infragard unless there is a provision in the Internal Revenue Code authorizing such disclosure. The Secure Access Member Agreement (SAM) the IRS would execute to join Infragard provides in paragraph 1 that a Secure Access Member is not obligated to disclose information to the FBI or Infragard, so the confidentiality provisions of section 6103 should not be a problem. If the IRS finds it has return information it would like to disclose to Infragard, determinations regarding whether authority exists to make such disclosure can be made on a case by case basis. All IRS

employees working with Infragard should be reminded, however, of the confidential nature of returns and return information and of the inability to share such information with Infragard without Title 26 authority.

There is no specific provision in the Internal Revenue Code authorizing disclosures to Infragard. There are three potential sources of authority by which some Infragard members could have access to returns and return information, and each method has procedural prerequisites that must be met prior to disclosure. First, federal agencies may obtain returns or return information for use in nontax criminal investigations pursuant to an ex parte order of a federal district court judge or magistrate. I.R.C. § 6103(i)(1). The application for such order must be authorized by the Attorney General, Deputy Attorney General, Assistant Attorney Generals, United States Attorneys, Independent Counsel or an attorney in charge of a criminal division organized strike force established under 28 U.S.C. § 510. The application must establish: (1) reasonable cause to believe that a federal nontax criminal violation has occurred; (2) reasonable cause to believe that tax information is or may be relevant to a matter relating to the commission of the crime; and (3) that the information sought will be used exclusively for the federal criminal investigation or proceeding concerning such crime and cannot reasonably be obtained from any other source. This does not specifically authorize disclosure to Infragard, but to Federal agencies for a nontax Federal criminal investigation.

Second, IRS employees are specifically authorized by I.R.C. § 6103(k)(6) and Treas. Reg. § 301.6103(k)(6)-1 to disclose return information, but not returns, to the extent that disclosure is necessary in obtaining information which is not otherwise reasonably available with respect to the correct determination of tax, liability for tax, or the amount to be collected, or with respect to the enforcement of any other provision of the Code. The relevant inquiry is not whether the information sought is necessary for the investigation or examination but whether the disclosure of each item of return information is necessary to obtain the particular information sought. Barrett v. United States, 795 F.2d 446 (5th Cir. 1986). The only purpose of the disclosure is for the IRS to obtain information; the IRS may not disclose return information for the recipient's benefit. Disclosure of return information under this provision is very limited, depending on the specific facts and circumstances of each case. Courts reviewing disclosure made pursuant to I.R.C. § 6103(k)(6) have always looked into the circumstances surrounding each disclosure and taken a narrow view of the elements of return information that were necessary to be disclosed in order to obtain the information sought. In no event is a wholesale sharing of information, for example pursuant to a contract such as the SAM, authorized by this section.

Finally, Treas. Reg. § 301.6103(h)(2)-1 provides for the disclosure of return information to the Department of Justice in a joint Federal criminal tax/nontax investigation. The regulation contains a number of specific requirements. First, the nontax criminal aspects must arise out of the particular facts and circumstances

giving rise to the tax administration portion of the case. Second the tax portion of the investigation must have been duly authorized by the Tax Division of the Department of Justice at the request of the IRS. Finally, the regulation requires that if the tax administration portion of the proceeding is terminated, the Justice Department cannot use returns or taxpayer return information in the nontax portion of the matter without first obtaining a court order in accordance with I.R.C. § 6103(i)(1). Again, this provision does not specifically authorize disclosures to Infragard, but to Federal agencies involved in a criminal tax/nontax investigation.

If the disclosure of returns or return information to Infragard is determined in a specific situation to be authorized by any of these provisions of the Internal Revenue Code, limitations may be placed upon the recipients' use and redisclosure of that information. Infragard members must be made aware of this, particularly in light of paragraph 14 of the SAM which provides that the FBI may use for official purposes any information it receives from a Secure Access Member. There may also be safeguarding procedures the recipient of the return information may have to agree to and institute.

The memorandum also mentions a computer crimes task force being formed by the U.S. Attorney's office in Cleveland as a part of this effort. No provision of the Internal Revenue Code authorizes disclosure of returns or return information to such a Computer Crimes Task Force outside of those provisions discussed above, including the statutory and procedural requirements that must be met in order to fall within one of these exceptions to the confidentiality rule.

Additional I.R.C. § 6103 issues may arise regarding information the IRS receives from other Infragard members. If the information received by the IRS is gathered in connection with a taxpayer's liability or potential liability under the Internal Revenue Code, it becomes I.R.C. § 6103 protected return information in IRS files. Thus, even if the information was originally received from Infragard, the IRS may not be able to redisclose it after receiving it if it has been received in connection with a taxpayer's liability or potential liability under Title 26. Thus, if, as the CID employee mentions in his memo, paragraph 15 of the SAM means that the FBI retains full authority to control all information provided through Infragard, and this is intended to mean even after it has been sent to other Members such as the IRS, I.R.C. § 6103 may not allow the IRS to give the information back to, or discuss its use with, the FBI.

Paragraph 4 of the SAM provides that the Member agrees not to disclose any information it receives through Infragard other than to another Infragard Member, unless the information has been expressly designated for public disclosure. There are occasions where the IRS is required to disclose information in its control, even if the information is protected by section 6103. This could arise, for example, in the

context of a Congressional or GAO investigation.[1] Further, by way of example, IRS is required by statute to make disclosures to state tax authorities for state tax administration purposes unless disclosure would identify a confidential informant or seriously impair a civil or criminal tax investigation. I.R.C. § 6103(d). Thus, the IRS may not be in a position to contract that it will not disclose information when it may, in fact, have to.

Finally, information contained in a system of records that is retrievable by individual identifier is protected from disclosure by the Privacy Act of 1974, 5 U.S.C. 552a. Such information can be disclosed without the consent of the individual to whom it pertains only if such disclosure falls within one of the exceptions to the Privacy Act confidentiality rule, or if such disclosure would constitute a routine use of the information as provided for in the published Notice of System of Records for such information. Privacy Act limitations could come into play for systems of records containing Bank Secrecy Act/money laundering information not covered by I.R.C. § 6103. Such systems should also be checked prior to making any disclosure to Infragard.

If you have any further questions, please call 202-622-4570.

[1]There are exceptions in 6103 authorizing both Congress and the GAO to have access to returns and return information provided prerequisites to such access are met. See I.R.C. sections 6103(f) and (i)(7).