

GAO

Report to the Committee on Finance,
U.S. Senate

September 2010

TAX GAP

IRS Can Improve Efforts to Address Tax Evasion by Networks of Businesses and Related Entities



GAO

Accountability * Integrity * Reliability

Why GAO Did This Study

A taxpayer can control a group of related entities—such as trusts, corporations, or partnerships—in a network. These networks can serve a variety of legitimate business purposes, but they also can be used in complex tax evasion schemes that are difficult for the Internal Revenue Service (IRS) to identify.

GAO was asked to (1) describe what IRS knows about network tax evasion and how well IRS's traditional enforcement programs address it and (2) assess IRS's progress in addressing network tax evasion and opportunities, if any, for making further progress. To do this, GAO reviewed relevant documentation about IRS programs and interviewed appropriate officials about those programs and IRS's plans for addressing such tax evasion. GAO also interviewed relevant experts and agency officials in developing criteria needed to perform the assessment.

What GAO Recommends

Among other items, GAO recommends that IRS establish an IRS-wide strategy that coordinates its network tax evasion efforts. Also, IRS should assess its network programs and tools and should evaluate adding more data to its current tools. IRS generally agreed with these recommendations and noted additional organizational changes the agency is making that will address networks.

View [GAO-10-968](#) or [key components](#). For more information, contact James White at (202) 512-9110 or whitej@gao.gov.

TAX GAP

IRS Can Improve Efforts to Address Tax Evasion by Networks of Businesses and Related Entities

What GAO Found

IRS views network-based tax evasion as a problem but does not have estimates of the associated revenue loss in part because data do not exist on the population of networks. IRS does know that at least 1 million networks existed involving partnerships and similar entities in tax year 2008. IRS also knows that many questionable tax shelters and abusive transactions rely on the links among commonly owned entities in a network.

IRS generally addresses network-related tax evasion through its examination programs. These programs traditionally involve identifying a single return from a single tax year and routing the return to the IRS division that specializes in auditing that type of return. From a single return, examiners may branch out to review other entities if information on the original return appears suspicious. However, this traditional approach does not align well with how network tax evasion schemes work. Such schemes can cross multiple IRS divisions or require time and expertise that IRS may not have allocated at the start of an examination. A case of network tax evasion also may not be evident without looking at multiple tax years.

IRS is developing programs and tools that more directly address network tax evasion. One, called Global High Wealth Industry, selects certain high-income individuals and examines their network of entities as a whole to look for tax evasion. Another, yK-1, is a computerized visualization tool that shows the links between entities in a network. These efforts show promise when compared to GAO's criteria for assessing network analyses. They represent new analytical approaches, have upper-management support, and cut across divisions and database boundaries. However, there are opportunities for more progress. For example, IRS has no agencywide strategy or goals for coordinating its network efforts. It has not conducted assessments of its network tools, nor has it determined the value of incorporating more data into its network programs and tools or scheduled such additions. Without a strategy and assessments, IRS risks duplicating efforts and managers will not have information about the effectiveness of the new programs and tools that could inform resource allocation decisions.

Network Scheme Example: Installment Sale Bogus Optional Basis Transaction (iBOB)

An iBOB is an example of a network-related tax evasion scheme that shows how networks pose enforcement challenges for IRS. In an iBOB, a taxpayer uses multiple entities, all owned or controlled by the taxpayer, to artificially adjust the basis of an asset to evade capital gains taxes. The scheme can involve multiple transactions and take place over many tax years, making it difficult for IRS to detect. A short video illustrating an iBOB is available at <http://www.gao.gov/products/GAO-10-968>.

Contents

Letter		1
	Background	3
	IRS Suspects Networks Pose a Growing Tax Evasion Risk but Faces Barriers in Addressing the Risk through Its Traditional Enforcement Efforts	9
	IRS's Recent Efforts to Better Detect and Pursue Network Tax Evasion Show Promise, but Opportunities Exist for Additional Progress	13
	Conclusions	20
	Recommendations for Executive Action	21
	Agency Comments and our Evaluation	22
Appendix I	Objectives, Scope, and Methodology	24
Appendix II	Example Diagrams of Network Relationships by Entity Type	28
Appendix III	Overview of Studies Using Formal Network Analysis to Examine or Detect Criminal/Illicit Activity	32
Appendix IV	Comments from the Internal Revenue Service	40
Appendix V	GAO Contact and Staff Acknowledgments	44
Tables		
	Table 1: Descriptions of Entities That Can Be Linked in Networks	4
	Table 2: How Different Types of Entities Can Be Connected in a Network through Ownership or as a Beneficiary	5
	Table 3: IRS Progress in Meeting Network Analysis Criteria	17
	Table 4: Key Studies Using Visualization or Core Network Measures to Explain Criminal or Illicit Activity	34

Table 5: Key Studies Using Visualization or Core Network Measures for Intervention and Enforcement in Criminal Networks	35
Table 6: Key Studies Using Data-Mining and Related Approaches for Analyzing and Detecting Criminal/Illicit Activity	37
Table 7: Key Studies Using Multivariate and Statistical Analysis to Identify Associations and Causal Relationships among Network Variables and Key Behavioral Outcomes	39

Figures

Figure 1: Example of a Complex Business Network from IRS Research	6
Figure 2: Growth in Partnership Forms 1065 and 1065B and S Corporation Form 1120S Filings, Calendar Years 1998 through 2008	10
Figure 3: Example of yK-1 Output Graphic	15
Figure 4: Example of a Network with C Corporations	28
Figure 5: Example of a Network with S Corporations	29
Figure 6: Example of a Network with Partnerships	30
Figure 7: Example of a Network with Trusts	31

Abbreviations

CI	Criminal Investigation
EIN	Employer identification number
EOT	Enhancing Ownership Transparency
GHWI	Global High Wealth Industry
iBOB	Installment Sale Bogus Optional Basis Transaction
IRS	Internal Revenue Service
LDC	Lead Development Center
LMSB	Large and Mid-Size Business
NRP	National Research Program
OTSA	Office of Tax Shelter Analysis
SAT ESC	Servicewide Abusive Transaction Executive Steering Committee
SB/SE	Small Business / Self Employed
TE/GE	Tax Exempt and Government Entities
TIN	Taxpayer identification number
W&I	Wage and Investment

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

September 24, 2010

The Honorable Max Baucus
Chairman
The Honorable Charles Grassley
Ranking Member
Committee on Finance
United States Senate

Taxpayers can use networks to carry out a wide variety of legitimate business functions; however, networks also can be used to evade federal tax obligations. A network is a collection of entities linked through direct ownership or through common owners, associates, or shareholders. For example, a network may consist of a taxpayer who owns a corporation that does business with a partnership in which the same taxpayer is a majority shareholder.

Network-related federal tax evasion occurs when the network's taxpayers improperly structure complex transactions among commonly held entities. This allows the taxpayers to shift expenses or hide income, resulting in lost federal revenue. In one recent example, the U.S. Court of Appeals for the Ninth Circuit held that a family used transactions between commonly owned entities to improperly eliminate \$200 million in capital gains and avoid \$4 million in taxes.¹ The extent of network-related tax noncompliance has not been estimated, but in a 2007 tax compliance forum we sponsored with the Joint Committee on Taxation and the Congressional Budget Office, tax policy experts cited flows of income among related entities as a potentially large problem.² Some of the participants also said the Internal Revenue Service (IRS) needed to be more innovative in auditing such flows.

IRS recognizes the risk posed by network-related tax evasion and is developing new tools and programs to better identify and pursue such evasion. For example, one new tool helps examiners graph the relationship among entities in a taxpayer's network using information collected in an IRS database. IRS's new tools and programs are in various

¹*Stobie Creek Investments LLC v. U.S.*, 608 F.3d 1366 (9th Cir. 2010).

²GAO, *Highlights of the Joint Forum on Tax Compliance*, [GAO-08-703SP](#) (Washington, D.C.: June 2008).

stages of development—some have yet to be fully implemented—and their potential effectiveness is not known.

Given the above, you asked for more information about network-related tax evasion and IRS's efforts to combat it. Specifically, you asked us to (1) describe what IRS knows about network tax evasion and how well IRS's traditional enforcement programs address network tax evasion and (2) assess IRS's progress in addressing network tax evasion and opportunities, if any, for making further progress.

To describe what IRS knows and how well its traditional enforcement efforts address network-related tax evasion, we reviewed IRS planning documents and statistics, and interviewed relevant officials at IRS. We also developed a video with technical assistance from IRS's tax enforcement experts that illustrates a hypothetical example of a network tax evasion scheme. To assess IRS's progress and opportunities for further progress, we compiled an inventory of IRS's network compliance efforts by reviewing IRS documentation on auditing procedures for network-related cases and interviewing officials involved with identifying and addressing tax evasion related to networks. Because we could not find existing criteria that could be used for assessing IRS's network compliance efforts, we developed criteria. To do this, we conducted semistructured interviews with researchers who specialized in areas such as network analysis and computer science, interviewed relevant officials at select federal agencies that operate programs analyzing related entities or networks, and interviewed IRS examiners about their work. We selected the researchers based on our literature search of studies applying network analysis techniques to noncompliance behavior as well as from referrals from the researchers we had already interviewed. We distilled the common themes our interviews to establish criteria. Officials responsible for IRS's compliance programs concurred with the criteria. Using our work on the inventory of IRS's efforts, we then compared the status of each of the efforts against the criteria.

We determined for the purposes of this review that the data used were reliable. (See app. I for details on our scope and methodology.) We conducted this performance audit from June 2009 through September 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Networks of related entities are a feature of modern business organizations. Many legitimate reasons explain why a business owner (or owners) may choose to use a network of related entities to conduct operations. While this list is not exhaustive, a network may be used legitimately to:

- isolate one line of business from the potential liabilities or risk of business loss of another;
- isolate regulated industries into separate entities to manage ownership, reporting, or licensing requirements;
- manage a business's financing arrangements;
- separate ventures based in different states and countries; or
- separate activities for which ownership is restricted from those for which ownership is not restricted (such as when subchapter S corporation ownership restrictions apply).

A variety of entities can be linked in networks and report taxes in different ways. Table 1 briefly describes some of the entities that will be discussed in this report.³ Certain entities file tax returns with IRS to report their taxes owed, such as subchapter C corporations (C corporations), which file Form 1120, U.S. Corporation Income Tax Return. Other entities may operate as pass-throughs. A pass-through entity generally has the legal right to impute or pass net income or losses through to its partners, shareholders, and beneficiaries untaxed. Pass-through entities are required to provide each partner, shareholder, or beneficiary with a Schedule K-1⁴ stating the individual share of net income or loss to be reported. The entities also provide this information to IRS. The partners, shareholders, or beneficiaries are responsible for reporting this income or loss on their individual income tax returns and paying any tax. Entities that may serve as pass-throughs include subchapter S corporations (S corporations) and partnerships.

³Under the Department of the Treasury's check-the-box rules, eligible business entities may choose their entity type for federal income tax purposes. Business entities with two or more members can be a corporation or a partnership. Business entities with only one member can be a corporation or a single-owner organization. Certain corporations are not eligible to choose their entity type and are always taxed as corporations. 26 C.F.R. §§ 301.7701-1 to -4.

⁴Schedule K-1 is an information return that certain entities file to report income, credits, deductions, and other items that are distributed to other parties. Different Schedules K-1 exist for different entities, such as partnerships, S corporations, and trusts.

Table 1: Descriptions of Entities That Can Be Linked in Networks

Entity type	Description
Individual	An individual meeting certain income and age requirements is required to file tax returns. Individuals generally report taxes on Form 1040 U.S. Individual Income Tax Return.
Corporation	<p>A corporation is a separate legal entity generally established under state law with limited liability for shareholders. Corporations are treated as either C corporations or S corporations (named after Subchapters C and S of the Internal Revenue Code) for federal income tax purposes.</p> <ul style="list-style-type: none"> • Any corporation not eligible or not electing to be treated as an S corporation is a C corporation. A C corporation's income is taxed at the corporate level; once distributed to a shareholder, it may be taxed again as income for the shareholder. C corporations generally report taxes on Form 1120 U.S. Corporation Income Tax Return. • An S corporation is a corporation that has elected to be treated as an S corporation. Only corporations meeting certain eligibility requirements, such as having 100 or fewer shareholders, may elect to be an S corporation. Only certain types of entities, including individuals, and certain trusts, estates, and tax exempt organizations may be shareholders of an S corporation. Generally, S corporations file Form 1120S U.S. Income Tax Return for an S Corporation, which provides information about the income and deductions of the corporation and the identity of the shareholders. In general, income and losses of an S corporation are not taxed at the corporate level, but are imputed to the shareholders.
Partnership	A partnership is a for-profit business, including any syndicate, group, pool, joint venture, or other unincorporated organization, with at least two owners and which is not a trust, estate, or corporation. A partnership generally must file a Form 1065 U.S. Return of Partnership Income, which provides information about the income and deductions of the partnership and the identity of the partners. Partnerships do not pay taxes; the income and losses of a partnership are imputed to the partners.
Trust	A trust is a fiduciary relationship governed by state law. A trust is created when the grantor, or creator of the trust, transfers property to a trustee to be held for the benefit of the beneficiaries. A trust is sometimes said to divide ownership of the trust property into two parts: legal ownership, which goes to the trustee, and beneficial ownership, which goes to the beneficiary. Trusts are often used for holding the assets of beneficiaries, estate planning, or charitable purposes. Taxes on income earned by the trust generally are owed by the trust or the beneficiaries, although certain trusts are ignored for tax purposes and treated as if the grantor owned the trust property.
Tax exempt entity	Tax exempt entities are those such as certain charities and private foundations that have applied for, and been granted, tax exempt status. Tax exempt entities can be various types of entities, such as corporations or trusts. Because a tax exempt organization may lose its exempt status if a substantial part of its activities involves a nonexempt purpose, tax exempt organizations have the ability to establish for-profit subsidiaries. Most tax exempt entities must file a Form 990 Return of Organization Exempt from Income Tax.
Single-owner organization	A single owner organization, also referred to as a disregarded entity, is an eligible entity with a single owner that has elected to be disregarded for federal income tax purposes. Many alternative corporate forms recognized by state law such as limited liability companies may be treated as single owner organizations. Sole proprietorships, which are unincorporated businesses run by individuals, are commonly classified as single owner organizations.

Source: GAO analysis of IRS guidance.

The various types of entities that make up networks can be linked in multiple ways. Table 2 summarizes how a select set of individuals, various forms of businesses, and trusts may own or control other entities. The ownership, beneficiary status, or family connections within a network may not be initially apparent. Individual entities connected to an owner may in

turn own other entities or be the beneficiaries of other trusts, thus creating the potential for a large, complex network. For illustrative purposes, appendix II includes diagrams showing how certain entities can be linked and how the income generated by these entities can pass around a network.

Table 2: How Different Types of Entities Can Be Connected in a Network through Ownership or as a Beneficiary

	Can own shares in a C corporation	Can be a partner in a partnership	Can own shares in an S corporation	Can be a beneficiary of a trust
Individuals	✓	✓	✓ ^a	✓
C corporations	✓	✓		✓
Partnerships	✓	✓		✓
S corporations	✓	✓	✓ ^b	✓
Trust	✓	✓	✓ ^c	✓

Source: GAO analysis.

^aIn general, individuals who are not U.S. citizens or resident aliens are not eligible S corporation shareholders. Nonresident aliens are usually not eligible to be S corporation shareholders. An exception does exist if a nonresident alien, who is married to a U.S. citizen or resident, elects to report all of his or her worldwide income on a joint return with the U.S. citizen or resident. 26 U.S.C. § 1361(b)(1)(C); 26 C.F.R. § 1.1361-1(g).

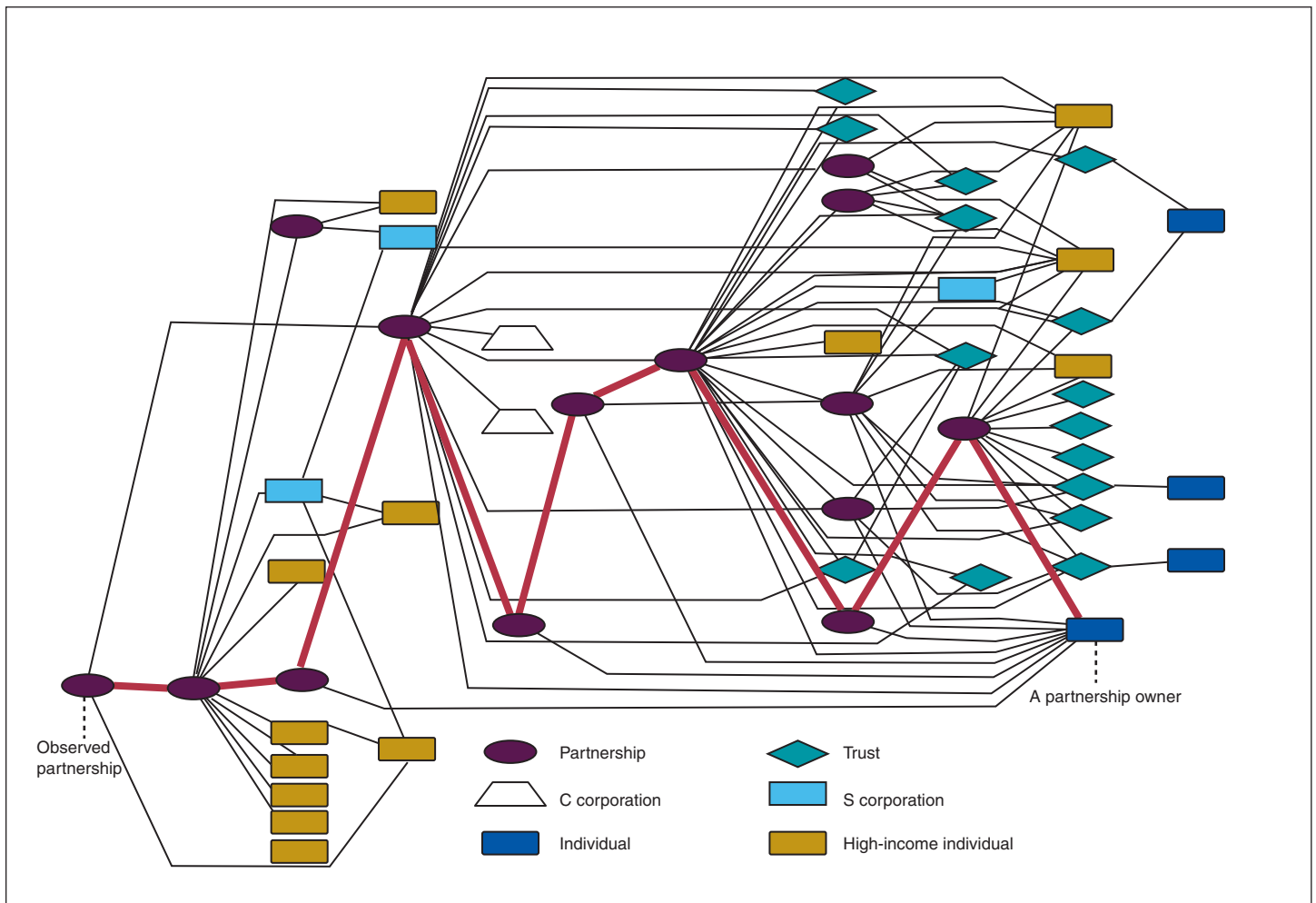
^bShares of an S corporation can only be owned by another S corporation if it is a qualified subchapter S subsidiary (QSub), and it must be wholly owned by the other S corporation. Only the parent S corporation owes a tax return to the federal government, as the income and deductions of the QSub are combined with those of the parent corporation. 26 U.S.C. § 1361(b)(3).

^cOnly certain trusts may be shareholders of an S corporation. 26 U.S.C. § 1361(c)(2). These trust types include certain grantor trusts, testamentary trusts, voting trusts, Qualified Subchapter S trusts, and electing small business trusts. 26 U.S.C. § 1361(c)(2).

When taxpayers use multiple pass-through entities, they create what IRS calls a “multitiered” network. In IRS’s definition, a multitiered network exists when a pass-through entity is itself a partner, shareholder, or beneficiary of another pass-through entity, leading to a situation where income is allocated from one pass-through entity to another.⁵ Figure 1, adapted from an IRS study, is an illustration of a hypothetical, complex network. In IRS’s example, the allocation from the observed partnership on the far left side of the diagram crosses nine pass-through entities along the red line before it reaches one of its ultimate owners on the right.

⁵IRS’s definition of tiering is more restrictive than our term, network. For purposes of this report, tiered networks should be considered a subset of networks.

Figure 1: Example of a Complex Business Network from IRS Research



Source: GAO adaptation from IRS study.

Owners of a network could use transactions among entities in the network to create tax evasion schemes in which taxpayers

- improperly conceal property ownership or income by diverting assets or income from one entity to another;

-
- improperly inflate an asset's basis⁶ to reduce capital gains taxes by selling the asset within the network;
 - improperly generate losses or tax deductions, which are passed through to other entities that use the losses or tax deductions to offset gains;
 - inappropriately shift losses, deductions, or credits from entities not subject to U.S. federal income tax, such as foreign entities, to those who are; or
 - inappropriately shift income from those entities subject to U.S. federal income tax to those entities that are not.

One example of a network tax evasion scheme is what IRS calls an installment sale bogus optional basis transaction (iBOB). In an iBOB scheme, taxpayers use commonly owned or controlled entities to artificially adjust the basis of an asset and evade capital gains taxes. The scheme can involve many layers of ownership, can take place over many tax years, and can be shrouded by legitimate transactions. IRS understands how the scheme works and has alerted examiners to its existence. IRS's Web site also describes a similar abusive transaction.⁷ In cooperation with IRS, we developed a video explaining how an iBOB works and the challenges IRS faces in ensuring those who are engaged in such schemes are caught. In our simplified example, a hypothetical taxpayer, Mr. Jones, sells a hotel that has appreciated in value resulting in capital gains that are taxable income. Mr. Jones uses an iBOB to evade paying capital gains taxes.⁸

Successful tax evasion schemes exacerbate the tax gap, which is the difference between the tax amount—including individual income, corporate income, employment, estate, and excise taxes—that should have been paid voluntarily and on time and the amount that was actually paid for a specific year. IRS most recently estimated that the tax gap was a net of \$290 billion in 2001.⁹ The tax-gap estimate relies on National

⁶Basis is generally the amount invested in a property for tax purposes. Basis is used to figure depreciation, amortization, depletion, casualty losses, and any gain or loss on the sale, exchange, or other disposition of the property.

⁷See the redemption bogus optional basis transaction at <http://www.irs.gov/businesses/corporations/article/0,,id=154246,00.html>, accessed Sept. 23, 2010.

⁸To view the video, follow the link <http://www.gao.gov/products/GAO-10-968>.

⁹The net estimate takes into account taxes that IRS expects to recover. The gross estimated tax gap was \$345 billion for tax year 2001.

Research Program (NRP) data. NRP compiled data on taxpayers' noncompliance by randomly sampling from the population of individual filers, intensively reviewing tax returns in the sample to determine the extent of noncompliance, and using the sample results to produce noncompliance estimates for the entire population.

IRS has four operating divisions—Wage and Investment (W&I), Small Business/Self-Employed (SB/SE), Large and Mid-Size Business (LMSB),¹⁰ and Tax Exempt and Government Entities (TE/GE). Each division has its own compliance programs, such as conducting examinations. W&I generally addresses individual taxpayers filing Form 1040; SB/SE addresses small businesses with assets of less than \$10 million and self-employed taxpayers; LMSB addresses C corporations, S corporations, and partnerships with assets of \$10 million or more; and TE/GE addresses pension plans, exempt organizations, and government entities. IRS's Criminal Investigation (CI) unit also investigates cases of fraud that may involve networks. CI has investigative jurisdiction over tax, money laundering, and bank secrecy laws.

The Office of Tax Shelter Analysis (OTSA), the Lead Development Center (LDC), and the Servicewide Abusive Transaction Executive Steering Committee (SAT ESC) are three groups within IRS with responsibilities that may touch on network tax evasion. OTSA is an LMSB group that collects and analyzes information, some of which is reported by taxpayers¹¹ about certain tax shelters.¹² LDC in SB/SE acts as the clearinghouse to receive, identify, and develop leads on individuals and entities that promote and/or aid in the promotion of abusive tax avoidance transaction schemes. IRS has charged SAT ESC with coordinating information about tax shelter schemes—including those that might involve networks—that individual operating divisions identify.

¹⁰As part of an organizational shift, LMSB will be known as the Large Business and International division beginning October 1, 2010.

¹¹OTSA collects Form 8886, Reportable Transaction Disclosure Statements, which is filed by investors who participate in listed transactions or other reportable transactions.

¹²A tax shelter generally refers to a strategy or promotion that “shelters” income from taxation. Depending on the facts and legal analysis, a specific transaction/promotion may represent either lawful tax avoidance or unlawful tax evasion. Tax shelters resulting in evasion are said to be “abusive” tax shelters. The Internal Revenue Code defines tax shelter in specific circumstances such as when applying certain penalties or for certain tax accounting rules. 26 U.S.C. §§ 461(i)(3), 6662(d)(2)(C).

IRS Suspects Networks Pose a Growing Tax Evasion Risk but Faces Barriers in Addressing the Risk through Its Traditional Enforcement Efforts

IRS Does Not Know the Magnitude of Network Tax Evasion, but Has Observed an Increase in Risk Factors for Such Evasion

IRS does not have an estimate of the total amount of revenue lost through network tax evasion because of cost and complexity constraints. IRS faces challenges in developing an NRP-type study to estimate the amount of network tax evasion because it does not know the population of networks. Therefore, IRS does not know what portion of the \$290 billion net tax gap is network related. Nor does IRS routinely track the amount of network tax evasion it identifies through its enforcement programs. As will be discussed in more detail below, IRS's enforcement programs have traditionally focused on single entities as the unit of analysis, such as an individual or corporation, rather than networks.

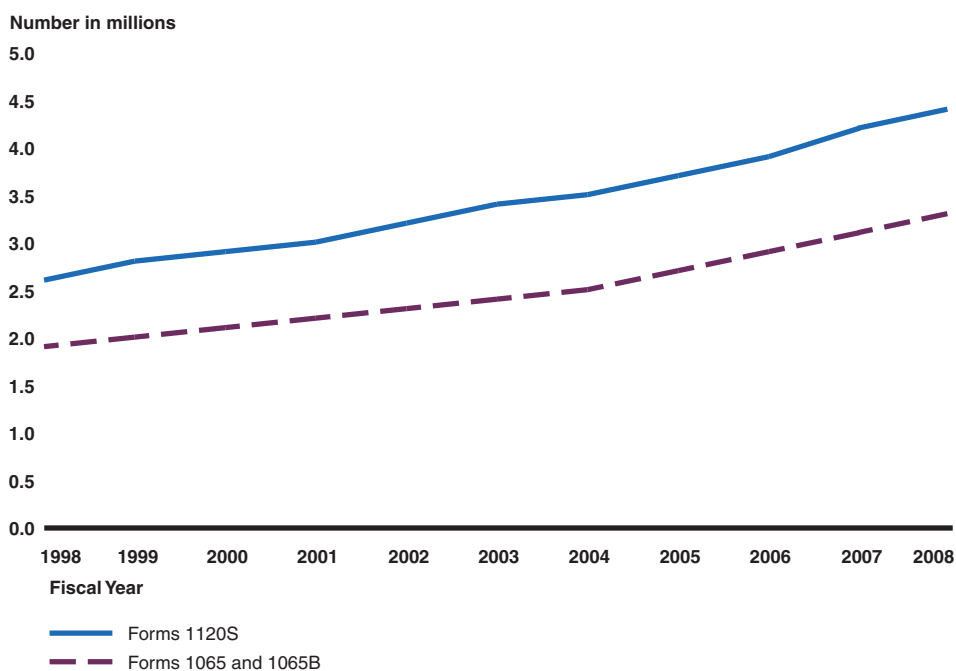
While IRS does not know the population of networks, it has estimated the size of a subset of that population. Based on a study of networks with two or more pass-through entities, IRS estimated that in tax year 2008, more than 1 million of these networks existed, of which about 2 percent had 11 or more different entities' returns.

Although IRS lacks an estimate of network tax evasion, IRS officials said they have evidence of a problem because of their experiences with abusive tax shelters. Some of the tax schemes that IRS considers impermissible necessarily involve, or could involve, networks. IRS maintains a list of tax avoidance transactions on its Web site; any taxpayer engaging in such a listed transaction, or a transaction substantially similar to a listed transaction, must disclose to IRS certain information about that

transaction.¹³ IRS's list of tax avoidance transactions includes examples of abusive tax shelters involving networks. The iBOB scheme previously described is an example of network tax evasion involving a tax shelter.

IRS officials have cited trends that they said indicate an increased risk of network tax evasion. These officials noted the increased use of pass-through entities. This suggested to them that the use of networks is growing, that networks are becoming increasingly complex, and that the risk of tax evasion is growing. Figure 2 illustrates the extent to which partnership and S corporation tax return filings have increased from calendar years 1998 to 2008.

Figure 2: Growth in Partnership Forms 1065 and 1065B and S Corporation Form 1120S Filings, Calendar Years 1998 through 2008



Source: GAO analysis of IRS data.

Schedule K-1 filings from pass-through entities also have increased. From 2008 to 2009, submission of Schedules K-1 increased from 19.8 million to

¹³26 C.F.R. § 1.6011-4(b)(2). For IRS's list of transactions, see <http://www.irs.gov/businesses/corporations/article/0,,id=120633,00.html>, accessed Sept. 23, 2010.

21.2 million for partnerships filing Form 1065, U.S. Return of Partnership Income. Meanwhile, submission of Schedule K-1 forms for S corporations filing Form 1120S, U.S. Income Tax Return for an S Corporation, stayed about the same at about 7 million from 2008 to 2009.

IRS examiners we spoke with who have experience in network-related examinations said that, anecdotally, they have noticed an increase in the use of disregarded entities in a network, which they said is another risk factor for network tax evasion. A disregarded entity can be part of a network, but its connection to a taxpayer may not be clear in the tax information IRS uses to detect network tax evasion. The total number of disregarded entities is unknown, but IRS estimated that there were at least 443,000 disregarded entities during a period between July 2007 and August 2008.

IRS's Traditional Enforcement Programs Are Not Designed to Detect Network Tax Evasion

IRS's programs for addressing network-related tax evasion include its examinations (or audits) in which IRS examiners analyze taxpayers' records to ensure that the proper tax was reported. IRS's examination practices have made contributions to tax enforcement. In fiscal year 2009, IRS examined 1.6 million tax returns, identifying over \$49 billion in additional recommended tax.

IRS traditionally has conducted examinations on a return-by-return basis, beginning with a single tax return in a particular tax year as the unit of analysis and examining other tax returns connected with the original return, if necessary, in what can be called a bottom-up approach.¹⁴ The examination selection process generally involves identifying a pool of high-risk returns and from that group, determining which returns to examine.

CI follows a similar approach. It starts with a taxpayer suspected of criminal violations of the Internal Revenue Code or related financial crimes and then branches out to related entities. When investigators want to find connections between the suspected taxpayer and other entities, they use Reveal, a network visualization tool. Reveal draws on data from multiple sources that CI uses to analyze intelligence and to detect patterns

¹⁴Additionally, under the Tax Equity and Fiscal Responsibility Act of 1982 (TEFRA), the tax treatment of a partnership, including any adjustment or penalty, is generally determined at the partnership level. Pub. L. No. 97-248, §§ 401-406, 96 Stat. 324, 648-671 (Sept. 3, 1982), *codified* at 26 U.S.C. § 6221.

of criminal and terrorist activities. Data that Reveal uses include certain cash transactions, tax information, and counterterrorism information. Its outputs include a visual representation containing names, Social Security numbers, addresses, and other personal information of individuals suspected of financial crime or terrorist activity. Because of CI's authority to access sensitive information, only in rare instances do non-CI staff use Reveal, according to CI data security staff.

IRS's traditional enforcement efforts are not designed to identify networks, select those networks that appear to be involved in tax evasion, or follow up with in-depth examination or investigation. Specifically, IRS's traditional efforts are challenged in dealing with network tax evasion by the combined effects of a number of factors such as the following.

- *A bottom up approach focusing on a single taxpayer.* As with the businesses in the iBOB scheme previously described, an entity involved in a network may not raise suspicions when examined in isolation. The tax evasion may only be apparent in how it relates to other entities in the network.
- *Internal divisional boundaries.* A single network may contain many types of entities that cross the responsibilities of IRS's operating divisions (i.e., W&I, SB/SE, LMSB, TE/GE). While IRS has the SAT ESC in place for overseeing abusive transaction issues, examiners on any particular audit may not have the expertise or authority to pursue the network connections of the taxpayer under review. For example, SB/SE examiners auditing a small partnership may not have the time, expertise, or authority to recognize or pursue a related large S corporation that is a member of the partnership.
- *Single tax year examinations.* IRS examiners typically begin examinations by looking at tax return data for a single tax year, limiting their opportunity to notice multiyear schemes. The iBOB is an example of a scheme in which the transactions creating the tax evasion can occur in multiple tax years.
- *Competing time and resource priorities.* IRS generally aims to conduct examinations in a manner that maximizes the amount of tax noncompliance found while minimizing an examiner's time commitment. Network examinations may be highly time-consuming for an examiner and the outcome is less predictable.

Examiners' ability to follow network connections also is restricted in another way. The Taxpayer Browsing Protection Act¹⁵ prohibits federal employees from willfully inspecting taxpayer information without authorization. To comply with the law, IRS restricts the access examiners have to certain tax information. According to IRS, the law helps protect the confidentiality of taxpayer information, but examiners told us it also may restrict an examiner's flexibility to explore leads, without manager approval, across different tax forms that could reveal network abuse.

IRS's Recent Efforts to Better Detect and Pursue Network Tax Evasion Show Promise, but Opportunities Exist for Additional Progress

IRS Is Developing Programs and Tools Intended to Help Address Network Tax Evasion

Global High Wealth Industry (GHWI)

IRS has been creating specific programs and tools that address network tax evasion more directly than its traditional examination approach.

Under GHWI, IRS identifies certain high-wealth individuals and then examines each individual's network. According to the Commissioner of Internal Revenue, the intent is to take a unified look at the entire complex web of business entities controlled by a high-wealth individual to assess the tax compliance of the network, rather than of the separate entities individually. IRS initiated GHWI in 2009. Although it resides in LMSB, IRS plans for GHWI to include staff with expertise that crosses divisional boundaries. For example, GHWI examiners might address small partnerships included in a network, even though small partnerships otherwise would be under the purview of SB/SE. As a result, GHWI is

¹⁵26 U.S.C. § 7213A.

Enhancing Ownership
Transparency (EOT)

expected to directly examine tax issues that otherwise might have been missed.

SB/SE launched the EOT project in January 2010 to gather data on the owners and locations of new businesses through employer identification number (EIN)¹⁶ applications. Primarily, IRS officials said they are interested in identifying what they refer to as the responsible party, which is the true beneficial owner of the business in this context. As of January 2010, the EIN application form requests additional information from business owners, such as the Social Security number of the responsible party and location of incorporation, which IRS previously did not request. The goal of the project is to link the new data to existing information in IRS's databases for identifying related businesses or a network of businesses. As the operating division responsible for the EIN process, W&I will implement the program once design is complete, which is tentatively scheduled for January 2012.

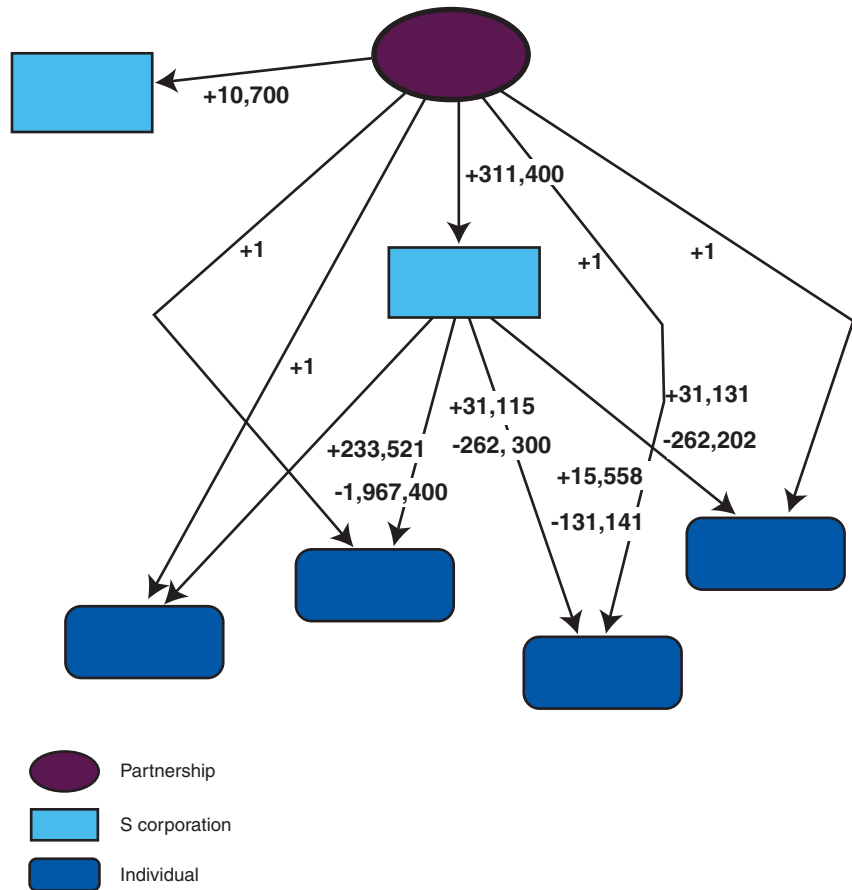
yK-1

The network tool that is furthest along in development and most widely used at IRS is yK-1. yK-1 is a network visualization tool that is now being used by some IRS staff in doing examinations and in reviewing networks. Users enter a taxpayer identification number (TIN)¹⁷ into the yK-1 software, which produces a picture showing how that TIN is connected to other entities through information filed on Schedule K-1. Figure 3 shows an example of yK-1 output. In this example, the numbers along the arrows represent the flow of money among the three different types of entities.

¹⁶An EIN is a taxpayer identification number that IRS uses to identify a business entity.

¹⁷A TIN is a number that IRS uses in the administration of tax laws. It is either a Social Security number issued by the Social Security Administration or a taxpayer identification number issued by IRS, such as an EIN.

Figure 3: Example of yK-1 Output Graphic



Source: GAO adaptation of IRS figure.

yK-1 diagrams can help examiners and other yK-1 users determine a specific entity's sources and amounts of income and whether other entities in the taxpayer's network need further examination. Examiners and users can then access other tax information about the entities in the network from IRS databases as well as non-IRS information from sources such as Accurant, a financial information database, and the Internet. Programmers are continuing to work on expanding yK-1's capabilities, such as adding estate and gift tax data and data on international taxpayers.

GraphQuery

IRS's Research, Analysis and Statistics group is developing another tool related to yK-1 called GraphQuery. GraphQuery is a pattern-matching tool being designed to facilitate top-down identification and selection of those networks that have the highest risk for noncompliance. In this top-down

approach, users would enter into GraphQuery a specified pattern, such as the structure of a known tax evasion scheme; the program would search for other networks showing the same pattern and list the TINs of the entities in those networks.

NetReveal

IRS's Office of Performance Evaluation and Risk Analysis has demonstrated a program called NetReveal, which can build a diagram of related entities or individuals using a wider variety of data, including nontax return data, than are used by yK-1. NetReveal, which is unrelated to CI's Reveal program, remains under consideration by IRS and has not yet been made available to the operating divisions for tax compliance purposes.

IRS's Ongoing Development of New Programs and Tools Is Generally Consistent with Network Analysis Criteria but Further Progress May Be Hindered by the Lack of a More Strategic Approach

Judged according to 14 network analysis criteria we developed, IRS's work on creating new network programs and tools already shows promise. We used interviews with academic experts and users of network analysis programs at other federal agencies to develop the 14 criteria, which are listed in table 3, for assessing network analysis programs and tools. Appendix I discusses what the criteria entail and how we developed them.

While the criteria describe good management practices that could apply to a wide variety of programs, the experts we spoke with cited these criteria as directly relevant to network analysis. In particular, the criteria highlight the crosscutting nature of network-related problems. The experts we spoke with also noted that network problems, such as network tax evasion, include by definition multiple entities that could cut across databases and an oversight agency's organizational units. As a logical consequence, they emphasized using criteria that call for an agencywide strategy, access to a wide range of data, and good collaboration across an agency's organizational structures.

For IRS, criteria focused on the crosscutting nature of network analysis are directly relevant to the problem of network tax evasion. A variety of entities could comprise a network, which could be under the purview of different IRS divisions. Similarly, data on the tax accounts for the different entities could be in different IRS databases.

Our assessment of IRS's new programs and tools against the criteria is shown in table 3. The assessment is of IRS's progress to date—the programs and tools are still under development. The assessment also indicates areas where IRS's efforts to date do not satisfy the criteria. These areas present opportunities to make further progress.

Table 3: IRS Progress in Meeting Network Analysis Criteria

Criteria	IRS progress
Strategy	
Agencies should have clear strategies with goals for network analysis programs	<ul style="list-style-type: none"> • IRS recognizes the need for new approaches to network analysis and has various efforts underway throughout the agency. • Pursuing tax shelters, which may involve networks, is part of IRS's strategic plans, but networks are not explicitly mentioned. • IRS has no agencywide strategy that coordinates or sets goals for the various network efforts.
Network analysis programs should have initial and ongoing support from upper management	<ul style="list-style-type: none"> • Management directives to assess network risk led to GHWI. • Management has publicly cited networks as a compliance problem and supports additional network efforts. • Management has not developed an IRS-wide resource investment plan for network efforts.
Agencies running network analysis programs should plan for ongoing program development	<ul style="list-style-type: none"> • Programmers update yK-1 based on user feedback. • GraphQL is being tested and developed on a time-available basis without a date for being operational. • GHWI is still developing, including acquiring additional staff, identifying ways to select workload, and developing measures for assessing their work.
Network analysis plans and related analytical tools should be flexible to adapt to emerging issues, including changes in network structures	<ul style="list-style-type: none"> • GraphQL's pattern recognition capability could be applied to new types of tax schemes in the future, if implemented. • yK-1 includes data on the various types of recipients and senders of Schedules K-1, giving it the flexibility to trace different kinds of network structures. • IRS officials told us that legacy computer systems can make data inflexible, requiring adjustments before it can be used in new tools and programs.
The network analysis program should serve across internal organizational structures and avoid creating barriers between those structures	<ul style="list-style-type: none"> • GHWI crosses examination groups in three divisions but resides in LMSB. • yK-1 draws on data that can be used across divisions. • Typically, new network programs and tools start in one of the operation divisions.
Agencies should develop goals, measures, and methods for assessing network analysis program effectiveness	<ul style="list-style-type: none"> • IRS has no plans to evaluate from a network perspective existing tools, such as yK-1, or programs, such as GHWI, in addressing network tax evasion. • Existing examination performance measures do not take into account the additional time needed to examine a network's multiple entities.
Programming and data	
Network analysis programs should use data from multiple sources	<ul style="list-style-type: none"> • yK-1 links entities just using Schedule K-1 data and IRS is considering other data to expand the linkages; however, combining external data with IRS's tax return data would involve significant administrative efforts, according to IRS officials. • IRS is piloting a program that allows state tax authorities to use yK-1, which may potentially reveal noncompliance at the federal level.

Criteria	IRS progress
Network analysis programs should have access to the most current and complete data available	<ul style="list-style-type: none"> • Tax year 2008 Schedule K-1 data were updated to yK-1 in May 2010, several months earlier than the updates for previous tax years. • IRS plans to move responsibility for database administration, including Schedule K-1 databases, to the Modernization and Information Technology Services group, which may allow for earlier and more frequent updates. • According to EOT program officials, EOT intends to enhance the business ownership data that IRS has, which yK-1 users will be able to use to connect related entities in a network. • IRS management has decided that network analysis is not browsing. Therefore, GHWI and yK-1 users are not restricted from pursuing leads on related entities. • All data from paper-filed Schedules K-1 are not scanned electronically due to costs, which limits examiners' access to complete Schedule K-1 data that they told us would be helpful.
Network analysis programs should use historical data to test program's ability to identify known problems	<ul style="list-style-type: none"> • yK-1 users can use historical data to identify gaps in return filings once an examination is initiated, but such data are not used regularly to test yK-1's ability to identify known problems.
Network analysis programs should use a variety of research disciplines and analytical techniques	<ul style="list-style-type: none"> • yK-1 largely uses network visualization, and IRS is considering using other techniques, such as pattern matching in GraphQL. • IRS is hiring specialists with expertise in pass-through entities to work on network cases in GHWI. • None of IRS's network analysis tools that are operational start with a network as a unit of analysis.
Network analysis programs should use data and analytical tools that match the problem to be addressed	<ul style="list-style-type: none"> • The new programs and tools are intended to move beyond IRS's traditional focus on single entities. • yK-1 helps auditors identify related entities through Schedules K-1, but other types of connections exist that Schedule K-1 data alone cannot be used to identify. • Although burdens and costs limit collecting all potentially useful data, examiners said they do not have access to data, such as some trust data, that they need to address the problem of identifying the many ways networks can be connected.
Collaboration	
Network analysis programmers, analysts, and subject matter experts should have frequent and ongoing communication about user needs and program capabilities throughout development and continued operation of the program	<ul style="list-style-type: none"> • yK-1 developers consulted with auditors when creating yK-1. • yK-1 users can submit feedback to programmers directly or in an annual user survey. • IRS does not have a formal mechanism to solicit views from nonusers about their needs. • GraphQL is primarily being developed by one staffer with limited input from potential users. • IRS has no written expectations on users and programmers sharing views about the development of new network programs or tools.
Analysts and subject matter experts should have access to the program tools or reports generated by program analysts without extensive delays or burdensome training	<ul style="list-style-type: none"> • IRS offers training for new yK-1 users. • Some yK-1 users we spoke with were not aware of the program's full range of functions. • IRS staff told us that some examiners are unaware that yK-1 is available to them.
Network analysis programs should have a dedicated program team	<ul style="list-style-type: none"> • GHWI seeks to bring together experts from across IRS because, unlike a dedicated program team, each IRS division alone lacks complete technical or analytical expertise on network tax evasion. • IRS does not have a dedicated team responsible for coordinating across IRS's multiple network analysis efforts.

Source: GAO analysis of IRS documentation and interviews.

As table 3 indicates, IRS's efforts to focus more directly on network tax evasion, while still under development, are consistent with our criteria for judging network analyses but do not fully satisfy them. The efforts are supported by upper management, offer new analytical approaches that more directly address network tax evasion, and attempt to cut across IRS's divisional boundaries and databases. As a result, these efforts show promise at being able to detect and pursue network tax evasion more effectively than IRS's traditional enforcement programs.

However, table 3 also shows where opportunities exist to provide more overall direction to IRS's efforts and perhaps hasten the development of specific programs and tools. For example, the table notes the lack of agencywide strategy and goals for IRS's various network efforts that are spread throughout the agency. Without agencywide strategy or goals to coordinate and prioritize these efforts, two risks exist. First, IRS could make redundant investments; second, IRS could fail to concentrate investments on the programs and tools with the greatest potential.

IRS may need to take an incremental approach to managing these risks because of the uncertainties. As already discussed, the population of networks is not known, networks can be complex, and IRS does not know which programs and tools will be most effective. Further, the costs could be significant. IRS's current organizational structure, work processes, and data systems do not support using a network as a unit of analysis and adjusting them to do so could disrupt other important priorities and programs. In light of this uncertainty about potential benefits and the cost, IRS will need to be careful in reallocating resources from other compliance programs to its new network efforts. As IRS gathers more information, management will be better positioned to more fully develop its strategy.

IRS also faces challenges in responding to the criteria for programming and data. As noted in table 3, adding new data, updating existing data, and making existing data more readily available in electronic form all could enhance IRS's capabilities to identify and pursue network tax evasion. Similarly, IRS could potentially benefit from more complete consideration of the potential relevance of the array of analytical techniques developed

in the research literature and available in existing software applications.¹⁸ However, as also noted above, such efforts would have costs. This reinforces the need for a strategy that would prioritize investments in better data and analytical capabilities.

IRS has not assessed the impact and effectiveness of its new network analysis tools, as described in table 3. For example, the benefits of using yK-1 relative to the additional time it takes examiners to use it have not been studied, but anecdotal evidence from users and management indicate yK-1 is a useful tool. Effectiveness assessments have costs which can be managed by judgments about the depth of the assessment needed. However, without effectiveness assessments, IRS managers are left without information that could help with the development of a strategy and with decisions about prioritizing investments in better data.

Table 3 stresses the importance of regular communications and training among all types of staff involved in identifying, analyzing, and pursuing network evasion schemes. Without these, auditors could be missing information they need and network schemes could go undetected. IRS officials said that the direct costs for these actions tend to be minor, but that they must be mindful of how these actions might affect other priorities. For example, they said the initial 2-hour training for yK-1 imposes minor costs. However, the officials also said that learning yK-1 requires accessing it enough to appreciate all of its capabilities.

Conclusions

IRS's network compliance efforts have the potential to address a significant part of the tax gap. However, IRS does not know the extent of this compliance problem or how effective its new programs and tools will be. Nor does IRS have a strategic approach to coordinate these network efforts across the agency.

IRS needs to walk a middle course between doing too much too soon versus doing too little too slowly. If it does too much, IRS risks taking resources from other priorities without assurance that the investment in the network efforts will reduce network tax evasion. If it does too little,

¹⁸While we determined that it would not be appropriate to set criteria for the exact methodology the agency should use in their network analysis program, we performed a review of studies using approaches that may be of use to those attempting to develop such programs; see appendix III.

IRS runs the risk of not learning more about networks and how to detect their tax evasion schemes.

To successfully balance these trade-offs, IRS would benefit from having a more strategic approach to coordinate and focus its various network efforts across the agency. As IRS learns more, that strategic approach would work toward developing a set of goals and measures to guide future efforts and consider ways to assess the impacts of the various programs and tools that are to be developed. Effectiveness assessments have costs, but without any assessments, managers lack valuable information. With such information, IRS would have a better sense of the pace at which it should invest its resources into expanding the network analysis program, including adding the analytical tools, data, and staff expertise that would be needed to address the specific compliance issues that IRS would be discovering. IRS's efforts to develop network programs and tools would also be enhanced by ensuring that staff understand the benefits of using the tools and are provided with a mechanism to provide feedback on the tools' and programs' effectiveness.

Recommendations for Executive Action

We recommend that the Commissioner of Internal Revenue take the following three actions.

- Establish an IRS-wide strategy with goals, which may need to be developed incrementally, to coordinate and plan ongoing and future efforts to identify and pursue network tax evasion. The strategy should include:
 - assessing the effectiveness of network analysis tools, such as yK-1;
 - determining the feasibility and benefits of increasing access to existing IRS data, such as scanning additional data from Schedule K-1, or collecting additional data for use in its network analysis efforts;
 - putting the development of analytical techniques and tools that focus on networks as the unit of analysis, such as GraphQuery, on a specific time schedule; and
 - deciding how network efforts will be managed across IRS, such as whether a core program team or management group is needed.
- Ensure that staff members who will be using current and additional network tools fully understand the tools' capabilities.
- Establish formal mechanisms for front-line users to interact directly with tool programmers and program analysts to ensure future network analysis tools, such as GraphQuery, are easy to use and help achieve goals.

Agency Comments and our Evaluation

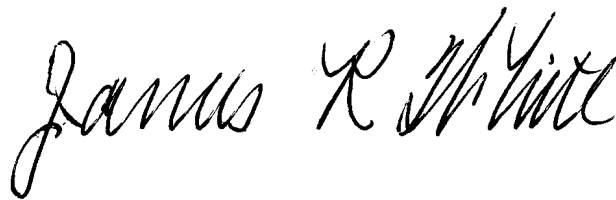
In a September 8, 2010, letter responding to a draft of this report (app. IV), IRS's Deputy Commissioner for Services and Enforcement provided comments on our findings and recommendations as well as information on additional agency efforts, changes, and studies to address network tax noncompliance. The letter also provided technical comments that we incorporated into our report as appropriate.

The Deputy Commissioner said that IRS agreed with our draft on the challenges involving network tax compliance and the status of IRS's network-related efforts. IRS also generally agreed with our recommendations to establish an IRS-wide strategy with goals, ensure that staff understand the capabilities of IRS's network tools, and establish a more formal way for IRS staff to collaborate as new network tools are developed and implemented.

In agreeing with our strategy recommendation, IRS's response noted that it may be more effective for IRS to consciously and appropriately include network issues in broader strategic plans, rather than develop a separate strategy for networks. We agree. Our recommendation is that IRS develops a strategy. We leave IRS with the discretion on how to articulate the strategy and point out that it may need to be developed incrementally.

As agreed with your offices, unless you publicly release the contents earlier, we plan no further distribution of this report until 30 days from its date. At that time, we will send copies to interested congressional committees, the Secretary of the Treasury, the Commissioner of Internal Revenue, and other interested parties. The report will also be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-9110 or whitej@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix V.

A handwritten signature in black ink that reads "James R. White". The signature is written in a cursive style with a large, prominent initial "J".

James R. White
Director, Tax Issues
Strategic Issues

Appendix I: Objectives, Scope, and Methodology

The objectives of this report were to (1) describe what the Internal Revenue Service (IRS) knows about network tax evasion and how well IRS's traditional enforcement efforts address network tax evasion and (2) assess IRS's progress in addressing network tax evasion and opportunities, if any, in making further progress.

To describe what IRS knows about network tax evasion and how well the traditional enforcement efforts the agency has in place address network tax evasion, we reviewed IRS statistics, policy manuals, and planning documents, including strategic plans. We also interviewed relevant IRS officials and staff.

We developed a video to highlight one type of network tax evasion. To develop this video describing the installment sale bogus optional basis adjustment (iBOB), we reviewed IRS technical information on iBOB schemes, out of which we developed a simplified, hypothetical example. IRS suggested the iBOB as a scheme that would make an appropriate example. IRS management and technical staff reviewed the video throughout its development, and we incorporated their technical comments where appropriate.

Because no existing criteria that we could find directly applied to reviewing the progress of IRS's network analysis programs, we developed our own. We conducted two groups of interviews with network analysis users and experts to develop our criteria for network analysis program development and implementation. The first group of interviews was with academic researchers considered to be experts whom we identified through detailed literature reviews and recommendations from other experts. The second group of interviews was with federal agencies that use network analysis tools. We also interviewed IRS auditors about their work.

To identify relevant academic experts, we reviewed the research literature using network analysis and related methods. We then created a literature search matrix and entered all studies obtained through the search that involved some quantitative/automated form of network analysis and an empirical application to a substantive area that had potentially direct applications to our review. We selected a subset of these studies for a more detailed review and used professional judgment to focus on studies of most immediate relevance. The literature review was the primary tool used for selecting researchers and experts for further follow up, which was ultimately based on ensuring a balance of experts with expertise across the entire array of substantive research topics and methodological

approaches that we identified in our search and on determining that individual experts' research agendas were both broad and deep. We conducted semistructured interviews with these experts, during which time we asked for recommendations of other network analysis and data mining experts. Often these recommendations were for researchers or experts we had already identified. Not every expert we identified was available to speak with us. The experts we spoke with included Wayne E. Baker, University of Michigan; Stephen P. Borgatti, University of Kentucky; Kathleen M. Carley, Carnegie Mellon University; Sean Everton, Naval Postgraduate School; Mark Granovetter, Stanford University; David Jensen, University of Massachusetts Amherst; Mark Mizruchi, University of Michigan; Carlo Morselli, University of Montreal; Daniel M. Schwartz, Criminal Intelligence Service Ontario; Duncan Watts, Yahoo! Research; and Jennifer Xu, Bentley University. We used our interviews with these experts to aid only in developing our criteria; they did not otherwise contribute to the content of the report.

To identify federal agencies to interview, we first reviewed academic literature and reports on government agencies that conduct network analyses, including our own reports. Through this review, we identified Customs and Border Patrol (CBP); Federal Bureau of Investigation; Financial Crimes Enforcement Network; Immigration and Customs Enforcement; Risk Management Agency at the United States Department of Agriculture; and the Securities and Exchange Commission. We also identified the Financial Industry Regulatory Authority (FINRA), which is not a federal agency but has an oversight and enforcement component similar to that of federal financial regulators. We conducted semistructured interviews with relevant program staff that use network analysis tools at these agencies and FINRA. During each interview, we asked about what works well in their network analysis program; what about their network analysis program needs improvement; what tools they feel could improve their program; what are best practices for developing a network analysis program; and what other agencies use network analysis programs. Of those other agencies that were mentioned that had network analysis programs, we chose not to meet with the Central Intelligence Agency and National Security Agency due to time constraints and data sensitivity issues. The Drug Enforcement Agency (DEA) was also recommended to us to speak with; while we did not directly speak with DEA due to time constraints, we were able to speak with a DEA liaison at CBP who briefly described DEA's network analysis program.

From these two rounds of interviews, we distilled the common themes in those responses to establish the criteria. We first read through all the

interviews, recording potential criteria. We then systematically reviewed the entire set of interviews to identify all that contained our initial criteria; this resulted in the rephrasing or elimination of some of these criteria, as well as the addition of a number of new ones. The themes that emerged from the interviews fell into the following categories: strategy, management support, program evaluation, data management, staffing, collaboration, methodology, and other. We determined that for our review of IRS, it would not be appropriate to set criteria for the exact methodology the agency should use in its network analysis program, or particular software packages. Therefore, we eliminated any particular research or methodological approaches and techniques from our final criteria list.¹ We also eliminated ideas where there was a clear division of opinion among the experts we interviewed. For example, experts and users did not agree on the benefits of including narrative data in network analysis programs. We presented the criteria to IRS for its feedback.

The final 14 criteria were categorized by theme: overall strategy; programming and data; and collaboration. The criteria were neither prioritized nor made to be specific to IRS. Each criterion was supported, at minimum, by five interviews; many were supported by eight or more interviews. The criteria with the fewest interviews for support generally pertain to organizational structure issues. The academic experts generally did not address these issues because they tend to use network analysis programs for research purposes compared to a federal agency's use for enforcement purposes. In these instances, we also had support from prior GAO work.

To assess IRS's progress in identifying and addressing network tax noncompliance, we reviewed IRS documentation on its auditing procedures and interviewed officials involved with identifying and addressing noncompliance related to networks. We then compared the evidence we collected in these reviews and interviews with the criteria we had developed and identified specific instances where IRS has demonstrated progress towards meeting each of the criteria. We also identified opportunities for further progress in meeting the criteria. We determined for the purposes of this review that the data used were reliable. Because some of the efforts to address noncompliance were under development during the time of our review, we presented the

¹An overview of the information we gathered on methodological approaches to network analysis can be found in appendix III.

assessment to IRS officials for their feedback and for related updates that might affect the assessment.

Our review of key studies applying quantitative network analysis methods to areas of noncompliance or illicit activity (see app. III) focused on identifying analytical approaches that individuals developing network analysis systems may find useful. The criteria for selection of these studies were similar to those used in selecting experts. In particular we ensured that the studies taken as a whole group covered a broad set of topics and methodologies and also that the individual studies were supported by broad and deep individual research agendas. We included two additional criteria to ensure more direct applicability of the studies to the report topic.

- The selected studies applied network analysis directly to a specific set of activities most directly related to the report topic, particularly criminal intelligence, organized crime, fraud detection, public safety or security, and international trafficking.
- Studies focused on counterterrorism applications of network analysis and studies in the link analysis research area, which is focused on algorithms for identifying relationships among items in large databases of textual/narrative information, were largely excluded.

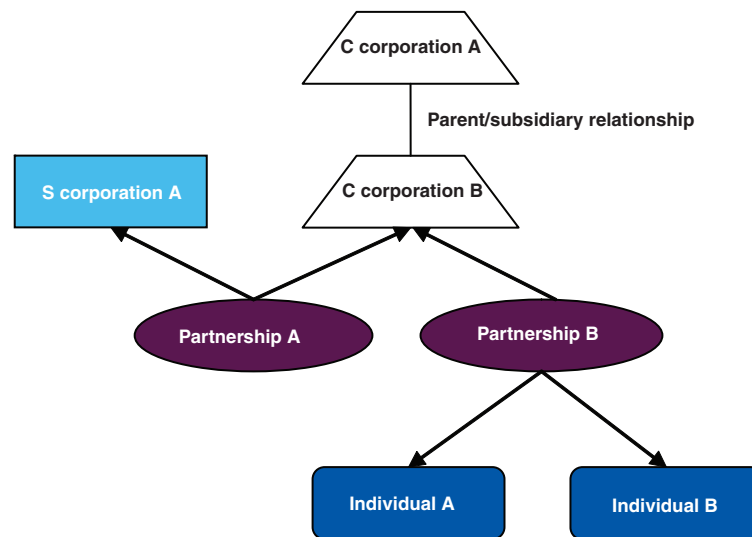
We conducted this performance audit from June 2009 through September 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Example Diagrams of Network Relationships by Entity Type

A network may comprise a variety of entities. Four types of entities that IRS recognizes that also can form networks are corporations, partnerships, trusts, and individuals. While these are not the only types of entities or connections that may exist in networks, they are entities that the Internal Revenue Service (IRS) has emphasized. The following examples show how networks can be connected and how income can flow among different entities. These examples are hypothetical and any resemblance with a known network is purely coincidental.

Figure 4 shows a network that includes two C corporations and two partnerships. Here, income and tax attributes (such as expenses, deductions, and losses) earned by the partnerships would flow back to C corporation B. However, the extent that C corporation A might also have received income from C corporation B depends on their business arrangements. S corporation A and Individuals A and B represent other partners that overlap with C corporation A's network.

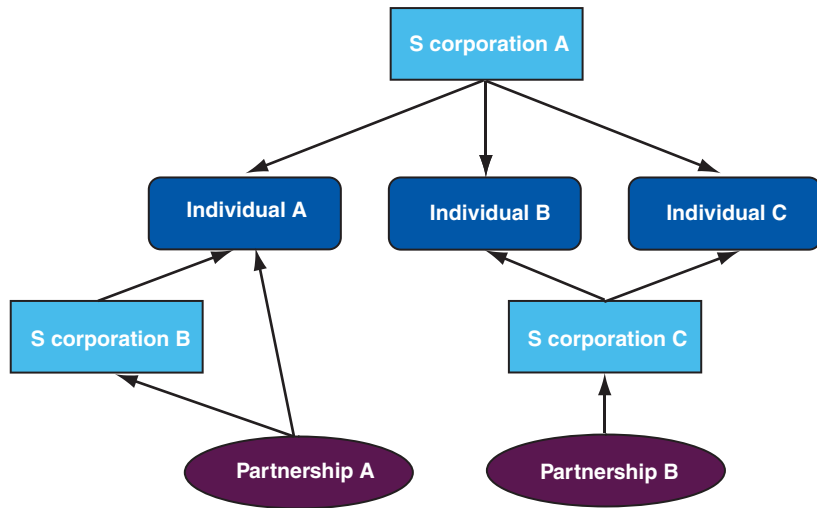
Figure 4: Example of a Network with C Corporations



Source: GAO analysis of IRS documents.

S corporations are pass-through entities that pass income on to shareholders. In figure 5, Individual A receives income and other tax attributes earned by S corporations A and B and Partnership A. Likewise, Individuals B and C receive income and tax attributes earned by S corporation C, which in turn receives income from Partnership B. S corporation A passes income on to all three individuals in this example.

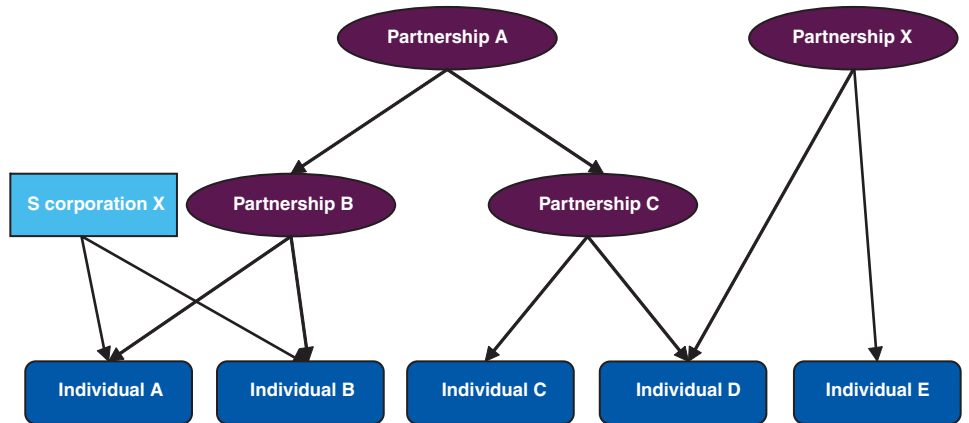
Figure 5: Example of a Network with S Corporations



Source: GAO analysis of IRS documents.

Figure 6 shows how partnerships can be layered and seemingly unconnected individuals can be connected. Individuals A and D have no direct connection but both ultimately receive income and other tax attributes from Partnership A. Individuals A through D are also connected to Individual E because of the financial ties between Individuals D and E through Partnership X.

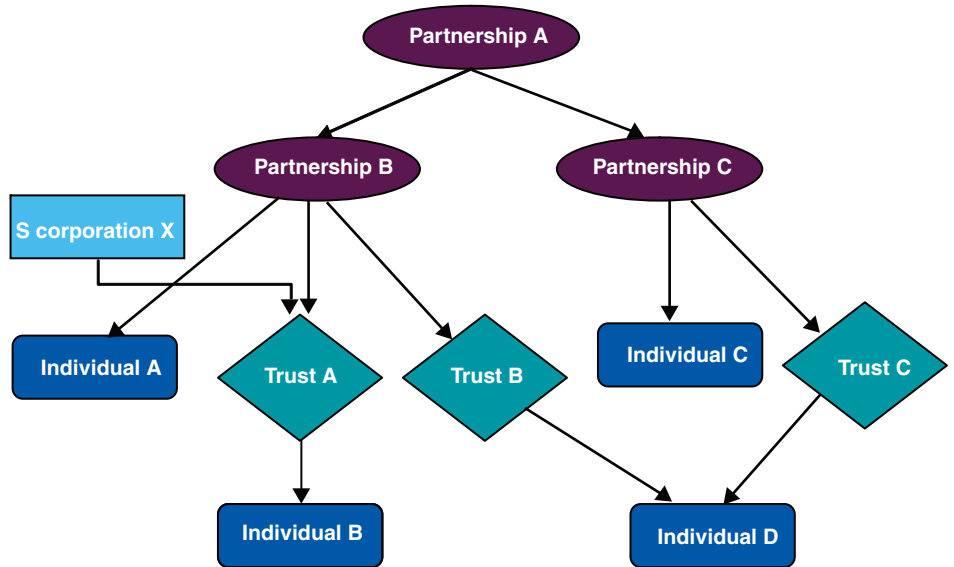
Figure 6: Example of a Network with Partnerships



Source: GAO analysis of IRS documents.

Trusts can be connected to other entities in a network in several ways. In figure 7, Trusts A and B are partners in Partnership B and, along with Individual A, receive income and tax attributes from Partnership B. Trust A is a type of trust that is allowed to own shares in S corporation X, which passes income and tax attributes to its beneficiary, Individual B. Trust C is a partner in Partnership C and, along with Trust B, sends its income and tax attributes to Individual D.

Figure 7: Example of a Network with Trusts



Source: GAO analysis of IRS documents.

Appendix III: Overview of Studies Using Formal Network Analysis to Examine or Detect Criminal/Illicit Activity

This appendix presents examples of research that have used formal quantitative network analysis techniques and methods to analyze network noncompliance, criminal, or illicit activity. Individuals developing network analysis programs may find relevant analytical approaches and techniques from this research. The research is summarized under four approaches to network analysis of illicit or criminal behavior. Key technical terms used in this summary include the following.

- Network: A set of actors and the set of ties representing some relationship or lack of relationship between the actors.
- Centrality: The number of direct contacts between a given network member and all other network members.¹
- Brokerage/network efficiency: Extent to which network members' connections are not to each other or are not within the same group (nonredundancy).²
- Cut-point: A network member that serves as the only connection among people or groups of people within a network.
- Key players: The set of network members whose removal will most disrupt or who can most efficiently diffuse information through a network.
- Density: The proportion of existing links out of all possible links in a network.
- Centralization: Extent to which a network is organized around a few central members.
- Clustering: Extent to which a network is subdivided into distinct, heavily interconnected subgroups.
- Connectedness: Extent to which all network members can reach each other along unbroken paths.
- Hierarchy: Extent to which the links in a network flow in one direction.³
- Chain: A network structure where a high proportion of network members can only reach each other via some other network member.

¹This definition applies to the “degree” centrality measure, which is the most basic measure of centrality. There are a number of other measures, such as closeness and betweenness centrality, which take into account indirect as well as direct contacts of network members.

²Network constraint is a closely related measure that can be thought of as the opposite of brokerage as it gauges the extent to which a network member's connections are to others who are also connected to one another.

³Hierarchy can also be understood as reflecting the degree of reciprocity in the network, or the extent to which there is mutual exchange between actors.

I. Interpretive Approaches Using Visualization or Core Network Measures to Explain Criminal or Illicit Activity

These studies use network visualization and measurement techniques to develop qualitative explanations of illicit/criminal behavior. This research has two major implications for network tax noncompliance.

First, these studies suggest that both individual- and network-level measures of position and structure may be useful diagnostics for identifying criminal/illicit behavior. For example, higher centrality of individuals in a network may be associated with higher levels of criminal activity. Further, high levels of brokerage/network efficiency may be associated with a leadership role in a criminal network and with success in criminal activity. At the network level, chain structures often characterize criminal networks, though more interconnected structures (measured as density) in criminal networks may correspond with higher-risk activities.

Second, tracking how network measures change may provide insight into how criminal behavior evolves. One study suggests that network leaders more effectively disguise involvement in criminal networks over time by using indirect relationships. Changes in the structure of noncompliance networks may correspond to changes in strategy and management. For example, management crisis in a noncompliance network may produce new relationships between previously disconnected individuals or change the extent of hierarchy in the network.

Table 4: Key Studies Using Visualization or Core Network Measures to Explain Criminal or Illicit Activity

Terrill L. Frantz and Kathleen M. Carley, “Organizational Response to the Turmoil of Personnel Turnover,” Center for Computational Analysis of Social and Organizational Systems, Dynamic Networks Project (n.d.).

Jana Diesner, Terrill L. Frantz, and Kathleen M. Carley, “Communication Networks from the Enron Email Corpus: It’s Always about the People, Enron is no Different,” *Computational and Mathematical Organization Theory*, vol. 11: 201–228 (2005).

The studies use Enron Corpus data^a from 1999-2002 to analyze the network response to crisis and management changes. They analyze changes in connectedness, hierarchy, efficiency of the networks, and patterns of downward, lateral, and upward communications between groups of individuals at different levels and functions of the organization.

Jennifer Xu, Byron Marshall, Siddharth Kaza, and Hsinchun Chen, “Analyzing and Visualizing Criminal Network Dynamics: A Case Study” (paper presented at the 2nd NSF/NIJ Symposium on Intelligence and Security Informatics, Tucson, AZ, 2004).

Study uses Tucson Police Department data on a large narcotics network over nine years to analyze the relationship between criminal behavior and network centrality of two key network leaders. It tracks the relationship of the leaders’ activity levels and network position over time.

Gerben Bruinsma and Wim Bernasco, “Criminal Groups and Transnational Illegal Markets,” *Crime, Law and Social Change*, vol. 41: 79–94 (2004).

Study compares the characteristics of criminal networks in three illegal transnational markets in Europe: heroin smuggling, trading stolen cars, and trafficking in women. Network characteristics include: cohesion, clustering (cliques), bridging, and overall chain structure. The relationship between network structure and the risk levels of the criminal activities is assessed.

Carlo Morselli, “Structuring Mr. Nice: Entrepreneurial Opportunities and Brokerage Positioning in the Cannabis Trade.” *Crime, Law and Social Change*, vol. 35: 203-244 (2001).

Study examines how Howard Marks, an international drug trafficker, used network brokerage strategies to build his criminal career, using data in his autobiography. Study focuses on associations between brokerage (i.e. network efficiency) and key outcomes (income, shipment size, and arrests/judicial sentences) over his three career phases (Building-Attainment-Fall).

Source: GAO research database search.

^aThe Enron Corpus is a dataset created by the Federal Energy Regulatory Commission in 2002 composed of 619,449 emails from 158 Enron employees

II. Approaches Using Visualization or Core Network Analysis Measures for Intervention and Enforcement in Criminal Networks

Numerous studies have used core network visualization and measurement techniques to develop interventions into criminal networks for enforcement purposes. A key implication is that intervention decisions should arise from analyzing network structures and processes. These studies suggest that effectively identifying intervention strategies may require varied network analysis approaches, ranging from basic to complex.

Basic network measures and constructs such as centrality or cut-points may effectively identify interventions in some contexts but not others. For example, in some contexts, using algorithms to find sets of key players may enable more efficient disruption or surveillance of criminal networks than approaches using centrality measures and cut-points. Extending the key player approach by incorporating data on individuals’ or entities’ attributes also may help. Approaches identifying cohesive subgroups and clusters, including the presence or absence of links between them, may

suggest effective interventions. For example, if a network has disconnected or weakly connected subgroups that are themselves heavily connected, it may be appropriate to focus on the more cohesive subgroups, rather than on central individuals across the network. Relatedly, it may be more productive to disrupt decentralized criminal networks than more centralized ones.

Table 5: Key Studies Using Visualization or Core Network Measures for Intervention and Enforcement in Criminal Networks

Carlo Morselli and Katia Petit, “Law-Enforcement Disruption of a Drug Importation Network,” *Global Crime*, vol. 8: 110-130 (2006).

Study examines how a drug importation network is decentralized and re-ordered by intense law-enforcement. Study uses electronic surveillance data from a 2-year investigation of hashish and cocaine distribution chains. It focuses on how the network responds to the removal of a central leader and to the enforcement opportunities that arise as criminal networks decentralize.

Jean Marie McGloin, “Policy And Intervention Considerations of a Network Analysis of Street Gangs,” *Criminology and Public Policy*, vol. 4: 607-636 (2005).

Study examines how using cohesion analysis (cliques) and “cut-points” can help develop anti-gang intervention programs. Data are from 32 group interviews at criminal justice agencies in Northern New Jersey. The study points to possible effective interventions given particular levels of cohesion in separate network sub-groups and when prominent cut-point nodes connect the sub-groups.

Stephen P. Borgatti, “Identifying Sets of Key Players in a Social Network,” *Computational and Mathematical Organization Theory*, vol. 12: 21–34 (2006).

Study develops an optimal way to find key players in a social network for enforcement and surveillance purposes. Two datasets are used: (1) data on a terrorist network; and (2) data on advice-seeking ties in a global consulting company. The study develops a graph fragmentation measure (for identifying individuals whose removal would most disrupt the network) and an inter-set cohesion measure (for identifying players who most efficiently diffuse information through a network).

Daniel M. Schwartz and Tony (D.A.) Rouselle, “Using Social Network Analysis to Target Criminal Networks,” *Trends in Organized Crime*, vol. 12:188–207 (2009).

Study extends the key player approach to make it more relevant to criminal enforcement and intelligence activity by incorporating data on player attributes^a as well as on the level of uncertainty about their network roles. The study develops measures for maximum disruption and maximum reach into a network, using hypothetical data to illustrate them.

Jennifer Xu and Hsinchun Chen, “Untangling Criminal Networks-A Case Study,” *Lecture Notes in Computer Science*, vol. 2665: 232-248 (2003).

Jennifer J. Xu and Hsinchun Chen, “CrimeNet Explorer: A Framework for Criminal Network Knowledge Discovery,” *ACM Transactions on Information Systems*, vol. 23: 201-226 (2005).

This research develops and assesses a criminal network analysis system, using multiple network analyses. They include centrality measures, shortest-path algorithms, subgroup analysis, hierarchical clustering, multidimensional scaling, and network visualization. The data come from the Tucson Police Department’s narcotics and gang-related crime incident summaries. Both studies use exercises with experts and students to validate the system’s capabilities.

Source: GAO research database search.

^aThese attribute measures include the ability to corrupt public officials, propensity to use violence, and capacity to discipline members of the network.

III. Data-Mining and Related Approaches for Analyzing and Detecting Criminal/Illicit Activity

This research covers various approaches from the computational sciences, relying on data-mining, machine learning, and simulation techniques. The approaches develop methods that may help detect unknown aspects of noncompliance networks. Possibilities include the following:

- relational machine learning approaches that identify systems of statistical relationships among attributes of network entities, such as individual roles, status and experience, and firms' locations, using complex relational data;
- risk-assessment methods that use probabilistic models to identify firms and employees with a high risk for misconduct. For example, algorithms have been developed to identify individuals that are atypically moving together among locations or organizations, which may help assess non-compliance risk;
- methods for identifying links, identities, or groups in a network. Link prediction, for example, uses machine-learning to identify unknown links in a network. An alternative method is anomalous link detection, which identifies links that are more likely to involve illicit/criminal/fraud activity. A third method is anonymous identity matching, which uses known relationships of unknown entities to predict their identities. Pattern matching or clustering algorithms can identify groups of entities occupying similar positions in the overall network; and
- dynamic simulation approaches that model networks' likely responses to varied interventions and assess the effectiveness of the interventions.

Table 6: Key Studies Using Data-Mining and Related Approaches for Analyzing and Detecting Criminal/Illicit Activity

Andrew Fast, Lisa Friedland, Marc Maier, Brian Taylor, David Jensen, Henry G. Goldberg, and John Komoroske, “Relational Data Pre-Processing Techniques for Improved Securities Fraud Detection” (paper presented at the 13th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Jose, California, 2007).

Study develops relational statistical models that identify firms and their employees at high-risk for misconduct. Data source is the Central Registration Depository (CRD), which has location, employment, and other data on federally registered firms and individuals. The study focuses on (1) finding “tribes” of employees who are at-risk for fraud due to atypical joint movements between branch offices, and (2) developing risk scores and models based on the finding tribes analysis and data on disciplinary actions against individuals.

Matthew J. Rattigan and David Jensen, “The Case for Anomalous Link Discovery,” *SIGKDD Explorations: The Newsletter of the ACM Special Interest Group on Knowledge Discovery and Data Mining*, vol. 7: 41-47 (2005)

Jennifer Neville and David Jensen, “Relational Dependency Networks,” *Journal of Machine Learning Research* 8: 653-692 (2007).

Both studies use probabilistic modeling and relational machine learning methods to identify data anomalies and statistical dependencies in complex relational data.^a The first study explores how algorithms commonly used in computationally problematic link prediction tasks may be more effectively used in detecting anomalous links in relational data. The second study uses an iterative estimation method to identify statistical dependencies between variables in several relational databases.

Shawndra Hill, “Social Network Relational Vectors for Anonymous Identity Matching” (paper presented at Workshop on Learning Statistical Models from Relational Data, International Joint Conference on Artificial Intelligence, Acapulco, Mexico, 2003).

The study indicates that anonymous identity matching methods using relational data may help identify unknown actors in networks. Testing relies on the CiteSeer database, a scientific literature library.

Brett W. Bader, Richard A. Harshman, and Tamara G. Kolda, “Temporal Analysis of Social Networks using Three-way DEDICOM.” Sandia National Laboratories, SAND2006-2161 (2006).

Using the Enron corpus data, the study develops a factor analysis-based pattern-matching approach to analyze how employees’ organizational roles and attributes are related. Models are produced that identify distinct clusters of employees and their relations to each other.

Jeffrey Baumes, Mark Goldberg, and Malik Magdon-Ismael, “Efficient Identification of Overlapping Communities,” *Lecture Notes in Computer Science*, vol. 3495: 27-36 (2005).

The study develops an algorithm for identifying communities or clusters based on density within a network to discover groups of actors that hide their communications, possibly for malicious reasons. Unlike other network clustering approaches, these algorithms allow for overlap so that one node can belong in multiple clusters. The algorithms iteratively scan network members and their neighborhoods until an optimal collection of clusters is reached. The algorithm’s efficiency is tested on random graphs as well as several datasets.

Kathleen M. Carley and Daniel T. Maxwell, “Understanding Taxpayer Behavior and Assessing Potential IRS Interventions Using Multiagent Dynamic-Network Simulation,” In J. Dalton and B. Kilss (Eds.), *Recent Research on Tax Administration and Compliance: Selected Papers Given at the 2006 IRS Research Conference* (2006).

Kathleen M. Carley, “Destabilization of Covert Networks.” *Computational and Mathematical Organization Theory*, vol. 12: 51-66 (2006).

These studies use dynamic-network analysis and multi-agent simulations to assess the effectiveness of interventions into illicit activity. The first study examines how variation in network structures conditions the effects of IRS ad campaigns on diffusion of information, change in beliefs, and participation in tax schemes. The second study examines how changes in network personnel affect information diffusion, depending on the structure of the network, the logic of interaction, and the presence of technology.

Source: GAO research database search.

^aIn a relational database, instances record the characteristics of heterogeneous objects and the relations among those objects. Examples of relational data include citation graphs, fraud detection data, and data on interrelated people, places, and events extracted from text documents.

IV. Multivariate and Statistical Analyses of Associations and Causal Relationships among Network Variables and Key Behavioral Outcomes

These studies use regression analysis or other multivariate statistical methods to examine collusion, unethical behavior, and adoption of illegal innovations. They emphasize statistically significant associations and causal relationships between measures of network position, overall structure, behaviors, and outcomes, while controlling for an array of individual and organizational attributes. Key implications include:

- Comparing different types of networks by their structural characteristics can help identify illicit activity. For example, illegitimate networks may be more hierarchical than legitimate networks. A network's need for secrecy, typically associated with illicit activity, as well as its information-processing demands, may determine the degree of centralization exhibited by the network.
- Important relationships between network and non-network variables can influence illicit behavior. For example, common codes of conduct may mitigate the likelihood that hierarchical or asymmetric relationships produce unethical behavior. While lower-status middle managers usually are the most vulnerable network participants, higher-status upper-level managers may be more vulnerable in centralized networks than in decentralized networks.

**Appendix III: Overview of Studies Using
Formal Network Analysis to Examine or
Detect Criminal/Illicit Activity**

Table 7: Key Studies Using Multivariate and Statistical Analysis to Identify Associations and Causal Relationships among Network Variables and Key Behavioral Outcomes

D.J. Brass, K.D. Butterfield, and B.C. Skaggs, “Relationships and Unethical Behavior: A Social Network Perspective,” *Academy of Management Review*, vol. 23: 14-31 (1998).

This study examines the associations between key network measures, individual and organization attributes, and their combined effects on unethical behavior. The study generates propositions about the likelihood of unethical behavior given particular types of individual relationships as well as overall network structure^a and actor/organizational attributes. It emphasizes the interaction effects between relationships and attributes (e.g., empathy, values, or the cost of losing a strong relationship) in influencing unethical behavior.

Brandy Aven, “The Network Structure of Corrupt Innovation: The Case of Enron,” Unpublished (2009).

Study examines differences in structures (using measures such as connectedness and hierarchy) in legitimate and corrupt networks, using descriptive statistics and correlation analysis. It also uses regression analysis to compare how actor centrality and constraint affect employees’ adoption of innovations in legitimate and corrupt networks. The data come from the Enron Email corpus from 1998 to 2002.

Wayne E. Baker and Robert R. Faulkner, “The Social Organization of Conspiracy: Illegal Networks in the Heavy Electrical Equipment Industry,” *American Sociological Review*, vol. 58: 837-860 (1993).

This study examines how core network measures^b affect enforcement and judicial outcomes (i.e. verdict, sentence, and fine) in three conspiracies in the heavy electrical equipment industry. It also examines how information-processing and secrecy needs determine the structure of corrupt networks. The data source is sworn testimony before the U.S. Senate Committee on the Judiciary.

Source: GAO research database search.

^aMeasures examined include tie strength, multiplexity, asymmetry, structural holes, closeness centrality, density, and cohesion. An example of one proposition at the level of the entire network is: “The effects of the constraints on unethical behavior of the density of relationships within a group will increase as the constraints of group norms, social consensus, and codes of conduct increase.”

^bThese include degree, betweenness, and closeness centrality, density, and centralization.

Appendix IV: Comments from the Internal Revenue Service



DEPUTY COMMISSIONER

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

September 8, 2010

Mr. James R. White
Director, Tax Issues
Strategic Issues Team
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. White:

Thank you for providing your draft report, *Tax Gap: IRS Can Further Develop Its Efforts to Address Tax Evasion by Networks of Businesses and Other Related Entities* (GAO-10-968), for our review and comments. We appreciate the time you and your team spent reviewing IRS programs and tools we use to identify business network tax evasion and the criteria that GAO developed for assessing network analysis processes.

The draft report does a good job presenting the challenges for tax administration created by business networks and, in general, accurately represents the current state of some of the steps taken by the Internal Revenue Service to address these challenges. As you state in your report, we need to walk a "middle course between doing too much too soon versus doing too little too slowly." We agree with the direction the report recommends: more focused strategic attention to network compliance, continued improvement and integration of tools used to analyze networks, and additional collaboration between IRS personnel with differing roles in the compliance process. We offer the following additional comments:

- Because of the broad impact of networks and the complex organizational responses required, developing a separate strategy to address network compliance will be useful, but ultimately may not be as effective as ensuring that network issues are consciously and appropriately included in broader strategic plans.
- The organizational changes we are undertaking (e.g., establishing the Global High Wealth Industry, piloting the Compliance Management Operations (CMO) approach, centralizing international compliance resources, and developing a Servicewide High Income Strategy) will help in this area, and have a significant impact on our capabilities to address network compliance.

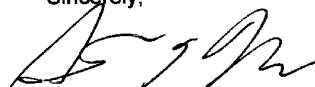
2

- In the end, the IRS will always be challenged to find technological, administrative, or auditing approaches to address the tax problems associated with the ever-increasing complexity and variability of both legitimate and abusive entity structures that use tiered flow through tax reporting. We are in the process of studying potential legislative and guidance changes to reduce the tax risks inherent in network structures.

The IRS response addressing your recommendations is enclosed. In addition, we are providing technical comments (Enclosure 2) on several specific statements in the draft report that we think may need clarification. However, these statements do not affect the overall conclusions of the report.

If you have any questions, please contact me, or a member of your staff may contact Don McPartland, Director, Research and Workload Identification, at (510) 637-2191.

Sincerely,



Steven T. Miller

Enclosure 1

GAO recommends that the Commissioner of the Internal Revenue Service take the following actions:

RECOMMENDATION 1:

Establish an IRS-wide strategy with goals, which may need to be developed incrementally, to coordinate and plan ongoing and future efforts to identify and pursue network tax evasion. The strategy should include:

1. Assessing the effectiveness of network analysis tools, such as yK-1
2. Determining the feasibility and benefits of increasing access to existing IRS data, such as scanning additional data from Schedule K-1, or collecting additional data for use in its network analysis efforts
3. Putting the development of analytical techniques and tools that focus on networks as the unit of analysis, such as GraphQL, on a specific time schedule
4. Deciding how network efforts will be managed across IRS, such as whether a core program team or management group is needed

RESPONSE:

Because of the broad impact of networks and the complex organizational responses required, developing a separate strategy to address network compliance will be useful, but may not be as effective as ensuring that network issues are consciously and appropriately included in broader strategic plans. In any event, a better articulated strategy for deploying, maintaining, and improving tools for network analysis is needed.

Item 1:

The IRS agrees that it is useful to assess the effectiveness of analysis tools, but it would be necessary to balance the costs of such an assessment.

Item 2:

The IRS agrees with this recommendation.

Item 3:

The IRS agrees that it would be useful to better structure and support the development of analytical tools.

2

Item 4:

The IRS will look at this issue. It may not be possible nor appropriate to manage network compliance activity centrally. However, at a minimum, we will consider how to manage better the analytic tools and whether a core program team would be useful in this regard.

RECOMMENDATION 2:

Ensure that staff members who will be using current and additional network tools fully understand the tools' capabilities.

RESPONSE:

The IRS agrees that training of compliance employees in the use of analytic tools can be improved.

RECOMMENDATION 3:

Establish formal mechanisms for front-line users to interact directly with tool programmers and program analysts to ensure future network analysis tools, such as GraphQL, are easy to use and help achieve goals.

RESPONSE:

Currently, the system developers have access to appropriate field employees, but we will consider improving the ability of field employees to have direct input and feedback to systems and risk assessment activities.

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

James R. White, 202-512-9110 or whitej@gao.gov

Acknowledgments

In addition to the contact named above, Tom Short, Assistant Director; Lydia Araya; Katie Arredondo; Russ Burnett; David Dornisch; Robert Gebhart; Eric Gorman; Sherrice L. Kerns; Melissa L. King; Adam Miles; Danielle Novak; Melanie Papasian; Ernest L. Powell Jr.; and A.J. Stephens made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

