U.S. DEPARTMENT OF ENERGY

PNNL-21908

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

A Nonproliferation Third Party for Dual-Use Industries – Legal Issues for Consideration

FA Morris
AM Seward
AJ Kurzrok

October 2012

Pacific Northwest NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm

This document was printed on recycled paper.
(9/2003)

A Nonproliferation Third Party for Dual-Use Industries- Legal Issues for Consideration

FA Morris AM Seward
AJ Kurzrok

October 2012

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

Contents

Important note: This paper discusses legal issues in connection with formation of a "third party" to facilitate information sharing and best practices by companies in nuclear-related dual-use industries. This paper has been prepared for discussion purposes only and does not constitute legal advice or legal opinions. Readers of this paper should consult an attorney for legal advice or legal opinions on this topic.

I. Introduction

The spread of nuclear weapons relies not just on the proliferation of nuclear material, but the transfer of industrial materials and technology as well. Developing a nuclear weapon requires a significant infrastructure of industrial tools and commodities, and these are manufactured across a range of industries in many countries. Some equipment, like a uranium centrifuge, is especially designed and prepared (EDP) for nuclear use. Other products, like particular machine tools, scientific instruments, and advanced steels, have both nuclear and non-nuclear uses. These items are known as "dual-use."

Since EDP items are, by definition, made specifically for nuclear uses, it is relatively easy for suppliers to ensure that these technologies do not end up in the wrong hands. A limited number of countries have the ability to manufacture these items, and nearly all are members of the Nuclear Suppliers Group (NSG) with strict nuclear export control regimes. The relatively small number of countries and companies with the capacity to use these technologies for peaceful ends is well-known to the set of nuclear suppliers and export control of these items thus relatively straightforward. Dual-use technologies, however, present different challenges. Legitimate non-nuclear end uses provide a potential cover for illicit purchase. While NSG guidelines apply to dual-use exports, not all exporting or transshipment states are members of the NSG. Moreover, the potentially legitimate non-nuclear uses of much dual-use equipment are numerous, diverse, and globally spread. As a result, exporters may have difficulty in determining whether a given transaction is for a legitimate non-nuclear use. Dual-use export control legislation, such as that of the United States, often relies on exporters to successfully make such determinations.

There is growing awareness among government, academia, NGOs and industry itself that active industry engagement could significantly complement existing governmental efforts to control the export of dual-use items. Since 2005, PNNL analysis has sought to identify how industry can best be leveraged to support nonproliferation.[1] The research has focused on the concept of industry self-regulation, defined as "a systematic, voluntary program of actions undertaken by an industry or by individual companies to anticipate, implement, or supplement regulatory requirements, generally through the adoption of best practices." A 2007 legal analysis of self-regulation for the nuclear and related industries (Morris and Hund 2007) found that "to a substantial degree, international instruments and national laws and regulations are in place to prevent access to the means of acquiring nuclear or radiological weapons." The analysis concluded, however, that increased industry engagement could increase the effectiveness of these regimes.

Subsequent PNNL research, which included interviews with 14 companies in various dual-use industries, identified steps that could be taken to actively promote nonproliferation (see Hund and Seward 2008).

[1] See Appendix A for an overview of PNNL research on the concept of industry self-regulation.

The research suggested a number of measures that companies could take individually, such as making the control and security of dual-use commodities and technology a tenet of their corporate governance structure, establishing strong export control management systems, and reporting suspicious export requests to government. The analysis concluded that while these actions would be beneficial, actions taken by an industry as a whole could ultimately have greater impact.

One such industry-wide action would be the creation of an independent, industry-led organization ("third party") to enable member companies to more effectively support nonproliferation. Such third parties have been established by other industries to facilitate the sharing of information concerning such matters as safety and security. A third party comprised of members of one or more dual-use industries could serve as a mechanism for information collection and dissemination among companies and with government authorities, as well as for the development and promotion of a set of nonproliferation best practices.

The competitive nature of industry often inhibits information exchange among companies because of such concerns as the potential loss of proprietary information and allegations of anti-competitive behavior (i.e. antitrust). There is also the concern that sharing certain information with government authorities (when that information is not required to be reported) could lead to investigations that otherwise could be avoided – entailing costs in time, money, and management attention. Thus, information gathered by a company during its export control compliance activities is not typically shared among competitors or, unless required, with government authorities. Yet companies receive and often deny suspicious requests. However, as the information is not shared to enable other companies to avoid filling the order, critical denial opportunities are missed.

Most firms that make dual-use technologies are highly aware of the potentially sensitive nature of their products, and have no interest in supporting nuclear proliferation. To combat illicit procurement, these firms set up internal compliance programs (ICP) to vet potential exports and ensure that the stated end use and end user are appropriate and peaceful. When a firm with a strong ICP receives a suspicious purchase request, it will refuse to fill the order, and in some cases, will choose to notify the appropriate authorities.

Refusing to fill the order stops that instance of proliferation, but does not put the bad actor out of business. If the firm chooses to report the case to authorities—and, as noted above, many firms do not due to fears of additional scrutiny—government may or may not pursue the lead. Even if the government does follow the case, the proliferator's identifying information will likely not be published on a denied parties list for months or years while the investigation is underway. Other firms in the industry could still run afoul of doing business with this bad actor, unaware that another firm has already identified illicit activity. In fact, some proliferators rely exactly on this weakness and barrage an entire industry with a purchase request on the same day. Tapping the "wisdom of crowds," or distributed knowledge, can help manufacturers protect against illicit procurement. Although each individual firm may only have vague suspicions about a given buyer, the dual-use commodity manufacturing community as a whole may have enough evidence to identify illicit behavior.

A database that manufacturers of dual-use technology could use to submit and search for denied purchase requests would allow each firm to benefit from the wisdom of the entire industry's internal compliance programs—essentially, crowdsourcing for national security. Export control violations, even accidental ones, can lead to fines, the loss of export privileges or criminal charges. By sharing denial data that would have otherwise ended up in the garbage bin, the dual-use industry would collectively raise its defenses to proliferation while mitigating the risk of regulatory penalty. Such a database would not

replace ICPs, but augment them. Each firm would still maintain the responsibility for policing its own exports.

The potential nonproliferation benefit of sharing such information is substantial. In particular, this information could help alert companies of the potential for illicit export requests involving prohibited end users, end uses, or destinations. Such information sharing could also facilitate compliance with export control regulations, thereby helping companies avoid the consequences of a regulatory violation, such as enforcement action and a damaged reputation. Making a prohibited export could be detrimental to the reputation of the company responsible, and could also negatively impact the industry as a whole. Thus, even companies not involved in an illicit transaction that is prevented through such information sharing could benefit.

The development and promotion of a set of nonproliferation best practices for industry members would reinforce and strengthen the nonproliferation benefit of information sharing. Taken together, these measures could raise the bar on industry compliance with export control requirements and cement industry as the true first line of defense in thwarting proliferation. By actively promoting nonproliferation and best practices designed to prevent the export of dual-use items to prohibited end users or destinations or for prohibited end uses, industry might also avoid the imposition of more onerous government regulation. The quality of the data companies receive would be a key driver to their participation in a third party, enabling them to make more informed export decisions.

When this proposal is broached informally, potential members of such a third party frequently indicate that legal issues are an important concern. Accordingly, this report identifies key legal issues that could potentially be raised by the specific structure, features and operational functions of a third party; assesses how each legal issue might affect the design and functions of the third party; considers how the third party might be structured to avoid legal issues; and seeks to identify any issues that might prove prohibitive to the creation of such third party.

A third party that links the many dual-use industries could be developed incrementally to explore and address legal and other concerns in the organization's structure and function. This analysis recognizes the challenges inherent in developing a third party for all dual-use industries, and recommends a phased approach in which incremental steps lead to an organization with the appropriate structure, membership, and functioning to address the full scope of the nonproliferation issue. For instance, membership could begin with companies in one dual use industry and be expanded to encompass all the dual use industries. Membership could at first be limited to companies (including multinationals) with a headquarters in the United States; it could later be expanded to be a global organization that addresses the true scope of the problem. The third party may initially serve to facilitate the development and exchange of a set of industry best practices before moving to the export information exchange function. Exchange of information could at first be restricted to only among companies, and if the members deem appropriate, at a later date be expanded to include government entities. Such a phased approach would enable the companies participating in the third party to tailor the organization to fit their own needs and be workable within the relevant legal framework. Thus, this report explores options for the third party with suggested starting points and potential sequential steps.

Two case studies help inform this analysis.[2] In each of these cases, individual companies within an industry perceived the benefit to themselves and the respective industry as a whole sufficient to justify

[2] These case studies have been excluded from this report for distribution due to confidentiality agreements with the representatives of each organization.

establishing a mechanism to facilitate information sharing among members with the intent of mitigating a specific safety or security concern. The authors conducted interviews with members of these industry third parties to determine the legal issues that they encountered in the development and functioning of each respective third party in order to inform the analysis of a third party entity for the dual-use industries.

II. Consideration of Legal Issues

The analysis in this paper addresses three main types of issues: (a) issues related to the formation of the third party entity in general, (b) issues related to the best practice function of the third party, and (c) issues related to the information sharing function of the third party.

A. General Issues Related to the Formation of the Third Party

At the outset, several issues arise related to the formation of the third party in general – that is, the issues associated with any industry organization formed to serve the interests of multiple individual companies. These issues include: the possible use of an existing organization as the third party, and if a new organization is established, the form of organization, the place of incorporation or other form of organization, membership in the organization, and whether the third party should perform some or all of its operations itself or contract with another organization to perform them.

Use of an Existing Organization

Some have suggested that the functions of the third party could be performed by an existing organization, such as an NGO devoted to nonproliferation or perhaps an educational institution. While this approach may have an apparent appeal of simplicity, it raises difficult issues of governance and control. In particular, the information sharing function is highly sensitive because of the nature of the information to be shared (potentially prohibited end users or end uses); the care with which such information must be compiled, stored, and disseminated; and the potential consequences of inadvertent or intentional disclosure to parties not entitled to receive it. As a result, participating companies would likely want to exert tight control over the information sharing function.

An existing organization, such as an NGO, would already have its own board, management, and members who are concerned with the organization's current mission and operations. It is unclear how the participating dual-use companies could exert sufficient control over such an organization with respect to their highly particular interests and the very specific operations being performed on their behalf to feel confident that those interests were satisfied. For example, dual-use companies could obtain representation on the board or membership in the organization, but their interests and priorities would inevitably be diluted by the interests and priorities of the existing directors and the existing members. Control would be partial at best.

Entering into a rigorous contract with the existing organization would not provide a sufficient solution. While such a contract could impose stringent obligations on the existing organization, it would not provide a vehicle for collective governance by the participating companies since they would be acting in their individual capacities as contracting parties. In order to have a vehicle for collective decision making, the participating companies would have to form their own organization to be the other party to the contract. That course would transform this option from use of an existing organization to formation

of a new organization and contracting out operations, which is a different option entirely, as discussed at the end of Section II.A.

Form of Organization

In principle, there are numerous options for the organizational form of the third party. It could be organized as a for-profit entity in the form of a corporation, a general partnership, a limited partnership, a limited liability partnership (LLP), or a limited liability company (LLC). Or it could be organized as a nonprofit entity in the form of a nonprofit corporation, a charitable trust, an unincorporated association, or an LLC. Whether organized as a for-profit or nonprofit entity, it could seek to obtain tax-exempt status under one of the applicable provisions of the Internal Revenue Code.

In practice, most U.S. industry associations choose to organize as nonprofit corporations with tax-exempt status under Section 501(c)(6) of the Internal Revenue Code, and this seems the likely choice for the third party. The corporate form helps limit the liability of the member companies. The nonprofit, tax-exempt status helps limit their costs. Section 501(c)(6) is the Internal Revenue Code provision that applies to business leagues (and certain other types of organizations), defined by regulation as an association of persons (including corporations) having a common business interest, whose purpose is to promote the common business interest and not to engage in a regular business of a kind ordinarily carried on for profit.

In order to qualify as a tax-exempt organization under Section 501(c)(6), the third party would need to meet seven specified criteria, each of which appears to be feasible:

1. *Must be an association of persons having a common business interest and its purpose must be to promote this common business interest.* The third party would be an association of dual-use exporting companies having a common business interest in achieving a high level of export control compliance and the purpose of the third party would be to promote this interest.

2. *Must be a membership organization, in which member support of the organization in the form of dues and involvement are at a meaningful level.* Through its articles of incorporation and bylaws, the third party could and should be structured as a "membership corporation," in which the member companies are assessed dues to fund the third party's operations, have the right and duty to participate in its information sharing and best practice functions, and elect its board of directors.

3. *Must not be organized for profit.* The third party would not be organized for profit.

4. *No part of its net earnings may benefit any private shareholder or individual.* The third party would not generate net earnings.

5. *Activities must be directed at improving business conditions in one or more lines of business (versus performing particular services for individual persons)*. The third party's information sharing and best practice activities would be directed at improving the conditions of the member companies' dual-use export lines of business. The reputation and reality of the industry

and individual companies related to responsible export control would be considered business conditions.

6. *Primary activity does not consist of performing services for individual persons.* Neither the information sharing nor the best practice functions are services for individual persons.

7. *Purpose must not be to engage in a regular business of a kind ordinarily carried on for profit.* Neither the information sharing nor the best practice functions are regular for-profit businesses.

The organizers of the third party could perhaps choose other options, but this seems the most straightforward.

Place of Incorporation

As with corporations generally, nonprofit corporations are created by filing articles of incorporation with the designated official of the particular state (or the District of Columbia) in which it is incorporated. While the nonprofit corporation laws of the various states are broadly similar, there are some variations based on whether the state statute follows the Revised Model Nonprofit Corporation Act of 1987, the earlier Model Nonprofit Corporation Act of 1964, or neither. In addition, the specific criteria for exemption from state taxes vary among states, and some states afford no exemption from state taxation at all. For example, in the State of Washington, which does not have a state income tax, nonprofit corporations are with limited exceptions taxed like any other business. Choosing a place of incorporation for the third party will likely be based on which state corporation laws have the most desirable features from the standpoint of the organizers, tax consequences, and practical considerations. While important, this choice does not appear to present major issues.

Another option would be incorporation in a foreign country. Consideration of this option for the third party is beyond the scope of this paper and would need to be based on the application of conflict of laws principles to particular liability concerns. Questions of taxation and other practical matters would also need to be taken into account.

Membership of Third Party

In principle, a nonprofit corporation can choose whether or not to have members. A nonprofit corporation without members is generally governed by a board of directors that selects its successors. In a corporation with members, the members are essentially analogous to the shareholders of a for-profit corporation in that they elect board members and provide financial support through the payment of dues. As noted above, having members is one of the requirements for tax-exempt treatment under Section 501(c)(6) of the Internal Revenue Code. And in practice, virtually all industry associations are member driven, and it seems clear that the third party would be as well, given both the tax considerations and the strong interest of the constituent companies in having a voice in policy and governance, especially as related to the sensitive issue of information exchange.

The question then becomes what criteria should determine the companies that are eligible for membership. As discussed above, qualification for 501(c)(6) status also depends on the members having a common business interest which the organization promotes through activities directed at improving business conditions in one or more lines of business. These criteria appear to be flexible enough in application to permit a broad scope of membership (any exporter of dual-use commodities), a much

more limited scope (exporters of dual-use machine tools), or something in between (exporters of dual-use industrial equipment).Perhaps the most practical approach to this issue is to see what companies express an interest in forming the third party and then to define the scope of potential membership accordingly, at least in the beginning.

Within the defined universe of companies eligible for membership, the third party will need to be open to membership to any company within the defined class to avoid charges of discrimination on antitrust or other groups (see below). The third party could however, establish classes of membership – for example, in which various levels of dues paid determines the member's rights relative to the organization's governance and other matters.

Use of Contractors

The third party would not necessarily need to perform all of the organization's operations itself and could contract out aspects of its operations that are not cost-effectively performed internally. Such contracting could be narrow (for example IT functions), broad (contracting with an existing nonproliferation NGO to perform many or most operations), or something in between (retaining overall management and the best practice function, contracting out the information sharing function). It should go without saying that any such contracts should impose rigorous obligations relating to standard of care and integrity of operations. But even more important, any such contractors should be very carefully chosen based on their reputation and track record for integrity and competence.

B. Issues Related to the Best Practice Function of the Third Party

The third party could function as a mechanism to establish and promote nonproliferation best practices among member companies. Best practices would focus on the companies' internal compliance systems for dual-use export control, including procedures and practices for reviewing export requests.

Scope of Best Practices

In constituting the third party, the founding member companies would need to address the fundamental question of the scope of the best practices to be established. These practices could be narrowly focused on internal compliance programs for compliance with the U.S. Export Administration Regulations (EAR) and other national export control legislation including company procedures and practices for reviewing export requests. Or they could be more broadly designed to go "beyond compliance," for example, to further reduce the risk of incorrectly identifying a prohibited transaction as legitimate by erring on the side of denying an export request in some circumstances even when it might be permissible within the letter of the EAR. This is essentially a policy question for the founding members: greater corporate nonproliferation responsibility, leadership, and penalty avoidance versus potentially losing business to companies who choose not to go so far. However, there are some potential legal concerns associated with resolution of this question.

Under the law of corporations and other business organizations, the required duty of care, known as the "business judgment rule," generally gives managers broad discretion to run the business as they see fit as long as there is some rational basis for their decisions. Nonetheless, if management of a public company chose to subscribe to export control policies that went so far beyond what the EAR strictly requires that the company suffered significant economic harm due to lost business, shareholders could

bring an action against management that at least theoretically could result in liability. While this scenario may be far-fetched, even the remote possibility of such litigation could nonetheless inhibit selection of best practices that go so far beyond what is legally required that they could be viewed as unreasonable.

Similarly, if the third party were to adopt best practices that went significantly beyond what is required by the EAR, and member companies subscribing to those best practices as a result denied exports in situations where the prospective importer met EAR criteria, both the third party and the member companies could potentially be vulnerable to legal action by those importers based on antitrust or tort claims. These issues are discussed in more detail in Section II.C below.

In summary, the third party has substantial freedom to adopt and implement highly rigorous best practices, but at some point there may be a limit on how far beyond compliance a consensus of member companies is prepared to go, at least initially.

Basis of Best Practices

Once the general scope of the best practice program is determined, the third party would need to draft the best practices themselves. This would likely be accomplished through some process in which representatives of member companies came together in a workshop format to draft these materials, perhaps with the involvement of third party staff, legal counsel to the third party, or other contractors. As part of this process, individual companies could share the details of their own internal compliance systems. However, they might be reluctant to do this for fear of disclosure to competitors, regulators, or the public. Depending on the depth of these concerns, they might be adequately addressed by strict non-disclosure agreements among the participants in the drafting process.

Implementation of Best Practices

Once firms form the third party and adopt best practices, several related implementation questions arise. Will adoption of the best practices be a mandatory condition of company membership in the third party? How will companies demonstrate that they have implemented the best practices? For example, will the third party review company programs and certify consistency with the agreed upon best practices? As with the scope of the best practices, these are primarily policy issues for the member companies to decide. Member companies would probably want some level of assurance that the other members are implementing the best practices in order to avoid the potential adverse competitive impact of going it alone. If adoption of the best practices is not strictly a mandatory precondition of joining the third party, there should probably be a strong expectation of adoption. For the reasons discussed in the previous section, in the beginning companies may be reluctant to open their compliance programs to the external scrutiny that certification would entail. Initially, self-certification may be the most appropriate approach. Over time, as companies build trust with each other and the third party, this could potentially expand to external verification, perhaps through adoption and implementation of an ISO-like standard.

C. Issues Related to the Information Sharing Function of the Third Party

As currently envisioned, the third party would collect information from member companies on the results of their "red flag" review of export requests, including information about end use, end user, ultimate destination, or other facts relating to the export request that raise nonproliferation concerns. This information would then be shared with other member companies to assist them in evaluating export requests made to them. Potentially, this information could also be shared with governmental authorities, such as the Department of Commerce Bureau of Industry and Security (DOC-BIS). However, many of the details of the information sharing function of the third party remain to be defined. The legal issues relevant to the information sharing function of the third party will depend partly on these details, such as the specific information to be collected and disseminated; the form of information collection and dissemination and the information security and protection applied; and to whom the information is distributed. Accordingly, this section begins with a discussion of these design matters, followed by a discussion of legal issues.

Information to be Collected and Shared

To assist dual-use exporters in complying with the dual-use export controls in the EAR, DOC-BIS provides "Know Your Customer Guidance" for application by exporters in evaluating export requests. This guidance includes six steps:

1. *Decide whether there are "red flags."* These are indicators that the export may be destined for an inappropriate end-use, end-user or destination. They consist of the following:

    - The customer or purchasing agent is reluctant to offer information about the end use of a product.
    - The product's capabilities do not fit the buyer's line of business; for example, a small bakery places an order for several sophisticated lasers.
    - The product ordered is incompatible with the technical level of the country to which the product is being shipped. For example, semiconductor manufacturing equipment would be of little use in a country without an electronics industry.
    - The customer has little or no business background.
    - The customer is willing to pay cash for a very expensive item when the terms of the sale call for financing.
    - The customer is unfamiliar with the product's performance characteristics but still wants the product.
    - Routine installation, training or maintenance services are declined by the customer.
    - Delivery dates are vague, or deliveries are planned for out-of-the-way destinations.
    - A freight forwarding firm is listed as the product's final destination.
    - The shipping route is abnormal for the product and destination.
    - Packaging is inconsistent with the stated method of shipment or destination. When questioned, the buyer is evasive or unclear about whether the product to be purchased is for domestic use, for export, or for re-export.

According to BIS, these red flags "are not all-inclusive but are intended to illustrate the types of circumstances that should cause reasonable suspicion that a transaction will violate the EAR."[3]

2. *If there are red flags, inquire.* In the absence of red flags (or an express requirement in the EAR), there is no affirmative duty for exporters to inquire, verify, or otherwise "go behind" the customer's representations. However, when there are red flags, BIS indicates that exporters "have a duty to check out the suspicious circumstances and inquire about the end-use, end-user, or ultimate country of destination."

3. *Do not self-blind.* Exporters should not deliberately insulate themselves from unfavorable information about potential customers, for example by instructing the exporter's sales force to tell potential customers not to discuss the actual end use, end user, or ultimate country of destination.

4. *Ensure that employees know how to handle red flags.* Exporters should establish policies and procedures that ensure employees transmit relevant information about potential transactions to senior management for evaluation.

5. *Reevaluate all of the information after the inquiry*. Following the inquiry, exporters should evaluate all the information obtained to determine whether the red flags can be explained or justified. If they can, the exporter may proceed with the transaction.

6. *Refrain from the transaction or advise BIS and wait.* If the red flags cannot be satisfactorily explained or justified, exporters should either refrain from the transaction or submit all of the information to BIS in the form of a license application or other form specified by BIS.

This guidance provides a helpful framework for determining which types of information is provided to the third party. Options include the following:

a. Results of all red flag reviews (Step 1 above), regardless of whether potential red flags are identified for the proposed export
b. Results of red flag reviews (Step 1 above), only if one or more potential red flags is identified
c. Results of red flag inquiry (Step 2 above)
d. Results of evaluation following red flag inquiry (Step 5 above)
e. Determination by exporter as to whether to refrain from the transaction or refer the propose transaction to BIS (Step 6 above)

Assuming that the overall goal is a high level of compliance with the EAR – avoiding exports to prohibited end users, end uses, and destinations – a company using such information would always benefit from receiving as much information as possible. A company providing the information, however, would have understandable concerns about providing unlimited information. For example, Option a (sharing results of all red flag reviews, regardless of outcome) would entail providing information about

[3] U.S. Department of Commerce Bureau of Industry and Security. "Know Your Customer Guidance." http://www.bis.doc.gov/enforcement/knowcust.htm.

essentially all dual-use exports under consideration by the company. This would mean releasing commercially valuable customer information to competitors and could also raise antitrust concerns (see below), so Option b would appear far more realistic and appropriate. Similarly, users of red flag information would want to see the complete sequence of information collection and analysis with respect to a particular proposed export (Options b through e). From the provider's viewpoint, however, the information provided under Options c through e becomes more subjective, judgmental, and subject to error, including both false positives (refraining from permissible exports) and false negatives (mistakenly proceeding with a prohibited export). Since all member companies would be both providers and users of information, they will presumably want to strike a balance regarding the amount of information shared.

Form and Process for Information Collection and Dissemination

Member companies could provide their information via forms created on a secure, password-protected website or via encrypted email. The level of detail could vary from completion of simple forms, to free text, to scanned copies of material created or obtained by the member company. (An example of a simple form is provided in Appendix B.) The third party would then need to compile and organize the information received, likely in some type of relational database. This process could be essentially automated or it could be mediated by third party staff to help ensure the completeness, consistency, and readability of data. The information could then be made available in a variety of formats, including the case file on a particular proposed export, aggregated data on a particular customer, end user, end use, or destination; analytical products on trends or the type prepared by third party staff; and alerts on particular customers, end users, end uses, or destinations of concern. The information could be disseminated via a secure, password-protected website or via encrypted email. The database could also be searchable so that, for example, if a member company has concerns about a particular customer, the company could perform a search to obtain information on that customer from other companies' red flag reviews. Provision could also be made for individual companies to discuss specific matters of concern with each other by telephone.

A key question is whether the name of the exporter providing information would be anonymous to users accessing that information. While such anonymity might create some comfort for those providing the information, anonymous information would seem to be inherently less credible and less useful than information associated with a named exporter. Also, within the dual-use community, actual anonymity might be difficult to achieve, since for many dual-use products there may be a limited number of suppliers, so guessing the exporter based on the product and other details of the transaction such as destination country might often be relatively easy for users. If fields in addition to the exporter's name were redacted in order to enhance anonymity, the resulting information would become less useful still.

In the end, it may be most practical to limit access to the shared information to designated, limited authorized users but not attempt to enter, maintain, or provide it anonymously.

Access to Information

Clearly the core purpose of the third party is to provide information to member companies to help them meet their obligation under the EAR to refrain from making dual-use exports to prohibited end users or destinations, or for prohibited end uses. Accordingly, authorized users from member companies should have access to information from other member companies that is compiled by the third party. There might be some temptation to limit the access of a given member company to information originating

from other member companies in the same industry, whether defined narrowly ("maraging steel") or broadly ("materials"). Such a limitation seems short-sighted because a prohibited end user might very well attempt to obtain a wide range of dual-use items, not limited to a particular industry. Prosecution documents in several cases have alleged that defendants had shopping lists, or sought many different commodities that could all support nuclear facilities.[4] Knowing that a particular customer tried and failed to illicitly obtain maraging steel from Company A could be quite useful to Company B when evaluating a request from the same customer that tries to purchase vacuum pumps.

Information compiled by the third party might also be made accessible to export licensing and enforcement authorities. Currently, exporters generally only share such information with authorities when they find red flags that cannot be satisfactorily explained and they choose to ask authorities for a review of the proposed export. While government entities might find it useful to obtain routine access to all of the information collected by the third party, granting such access could have a chilling effect on the willingness of member companies to submit completed and candid information to the third party, or even to participate at all. Accordingly, this option should be considered only if supported by a strong consensus among member companies and governments.

Confidentiality

For liability and other reasons discussed below, the third party and its member companies will want to keep confidential the information provided to the third party, compiled by the third party, and used by the member companies and any other parties. In practice, this means taking steps to limit access to the information provided to the third party (as well as the compilation or analysis of the information by the third party and data on use of the information by member companies), to authorized users with a need to know. This could be accomplished through non-disclosure agreements imposing contractual obligations on member companies and their employees, the third party and its employees, and any contractors of the third party and their employees. The detailed obligations should be carefully crafted to limit access to a small number of persons with a demonstrated need to know (that is, in order to perform their jobs, such as overseeing compliance with export control requirements). The information protection obligations should run to both the third party entity and to each of the member companies.

If it is decided to share information with governmental authorities such as BIS or others, the information should be provided in a manner that helps prevent disclosure in conformance with the Agency's own regulations regarding confidentiality (such as the BIS regulation at 10 CFR Part 718) as well as under the Freedom of Information Act (FOIA). It appears likely that FOIA Exemption 3 (Information Specifically Exempted by Other Statutes), 4 (Trade Secrets, Commercial or Financial Information), or 7 (Investigatory Records Compiled for Law Enforcement Purposes) would provide an adequate basis for such protection.

A related issue arises from the possibility that information held by the third party could be sought through the discovery process in litigation against the third party or one or more of its member companies. It might conceivably be possible to structure the sharing of information via the third party in a manner that invokes the attorney-client privilege and thus protects it from disclosure in litigation. However, such course seems likely to be very difficult if not impossible, and could introduce practical complications that would undermine the utility of the third party as an information sharing vehicle. Accordingly, member companies would likely need to assume the risk that information provided to the

[4] See, for example, the cases of Parviz Khaki or Jirair Avanessian, as discussed in "Summary of Major U.S. Export Enforcement, Economic Espionage, Trade Secret, and Embargo-Related Criminal Cases," http://www.justice.gov/nsd/docs/export-case-fact-sheet.pdf.

third party could be disclosed in litigation. If such litigation were to arise, the parties could attempt to at least limit the scope of disclosure through a protective order.

Standard of Care

Member companies and any other users of the information compiled by the third party would share a strong interest in the accuracy of the information provided, in order to avoid both false positives (incorrectly identifying a legitimate transaction as prohibited) and false negatives (incorrectly identifying a prohibited transaction as legitimate). As information users, they would want the information providers to exercise the highest possible standard of care in the provision of information to the third party. Of course, the very same companies that are information users would also themselves be information providers. In that role, their interests are different. They would naturally want to provide accurate information. But they would also be reasonably concerned that the information they provide might occasionally be incorrect, and that another member company that acted on the misinformation and was harmed as a result could attempt to hold the provider of the information liable, for example on a negligence theory.

Because of their dual roles of information providers and information users, the interest of the member companies in the accuracy of information provided to the third party would thus be mixed. They would likely want to strike some balance between obtaining the most accurate possible information as users and avoiding liability for inaccurate information as providers. To this end, they might include in their contractual arrangements with each other a provision along the lines that while as information providers they will make reasonable best efforts to provide accurate information, they disclaim all warranties as to the accuracy of the information provided, while as information users they hold each other (and the third party itself) harmless for any damage that results from information obtained through the third party that turns out to be inaccurate.

Antitrust

Federal antitrust laws, such as the Sherman Act, the Clayton Act, and the Federal Trade Commission Act, seek to prevent anti-competitive behavior by business enterprises. Because such behavior can occur through sharing of information and other joint actions among firms, the activities of industry associations nearly always have the potential to create antitrust issues. Through its information sharing function, the third party has the potential to raise two main antitrust issues: price fixing and group boycott, both of which are prohibited under Section 1 of the Sherman Act.

Price fixing involves an agreement among competitors that raises, lowers, or stabilizes prices or competitive terms. Price fixing includes not just an explicit agreement to set prices, but also exchange of information among competitors that can facilitate the setting of common prices. In the case of the third party, it should be possible to avoid liability for price fixing by scrupulously avoiding the provision of any information that could be helpful in fixing prices, such as prices, payment terms, costs, wages, salaries, and the like. In some instances, this might require excluding information that might raise a dual-use red flag, such as the customer's willingness to pay an above-market price or to pay cash when the exporter ordinarily offers financing. The third party could adopt common criteria, and each member company could establish specific procedures, to ensure that the information provided to the third party does not include anything that could facilitate price fixing. These criteria could also be reviewed by the Justice Department's Business Review Letter process and/or Federal Trade Commission.

A group boycott is an agreement among competitors not to do business with targeted individuals or businesses. Because a primary objective of the third party would be to enable member companies to avoid exporting their products to suspicious or prohibited end users, the application of the information shared through the third party to achieve this result could be viewed as a prohibited group boycott. In practice, this outcome could almost certainly be avoided by a demonstration that in this case the boycott advances public policy and is not in fact anti-competitive because it helps achieve compliance with U.S. export control law. However, nothing in this field can be taken for granted, and so this matter too should be reviewed carefully with antitrust counsel and possibly with the Justice Department and/or the Federal Trade Commission to be sure the third party's design and processes are structured to avoid interpretation as facilitating an illegal group boycott.

Tort Claims by End Users

If an end user became aware that an exporter declined to sell a product to the end user based on information obtained from the third party, the end user might bring a claim against the third party as well as the member company that provided the adverse information. The most likely bases for such a claim would be tort claims for defamation or interference with a business relationship. While torts are based on state law, which can vary somewhat from state to state, the general principles are similar.

Defamation involves publishing a false statement that damages the plaintiff's reputation. Written defamation is generally referred to as libel and oral defamation as slander. The elements of a claim for defamation are (1) a false statement by the defendant about the plaintiff that is (2) made available to a third party and which (3) damages the plaintiff, and, in many jurisdictions, (4) which defendant knew or should have known in the exercise of reasonable care was false. Accordingly, the plaintiff end-user would need to prove that the defendant originating member company and/or the third party entity provided information, which they knew or should have known was false, which was then used by another member company as a basis for denying an export to the end user. There is also a privilege (similar to a defense) known as the common interest privilege in which defendants can avoid liability if they can demonstrate that the information was collected with care and provided in good faith in order to advance the common interests. The end-user plaintiff would also have to overcome this privilege.

The possibility of bringing a defamation claim that proves all of the elements and overcomes the common interest privilege seems relatively remote, but member companies and third parties could reduce their exposure to such liability by adopting and implementing policies and procedures to help ensure that their employees exercise due care in providing and compiling end-user information. In addition, this scenario reinforces the need for stringent information protection: if false information about an end user were made public the damages could be more significant and easier to prove.

The tort of interference with a business relationship occurs where the defendant acts to prevent the plaintiff from successfully establishing or maintaining a business relationship with a third person. The elements of a claim for interference with a business relationship are (1) the existence or prospect of business relations between the plaintiff and a third party, (2) intentional interference with those relationships by the defendant, (3) acting for a wrongful purpose or using dishonest, unfair, or improper means. The most likely scenario would be a situation in which a member company was providing or about to provide the end user with a product and then terminated the relationship based on information provided by another member company via the third party. It seems unlikely that the end user could show that the provision of this information was dishonest, unfair, or improper, and so the prospect of liability on this basis seems remote. But as with defamation, this possibility emphasizes the need for care and objectivity in providing information about end users.

Intellectual Property

It seems relatively unlikely that the information provided by member companies to the third party would contain or reveal intellectual property. An exception might be revelation of member companies' existing and prospective customer lists if it were decided that member companies would provide to the third party the results of all red flag reviews, regardless of whether potential red flags are identified for the proposed export. Indeed, this might be a good reason to limit the information provided to the much smaller set of transactions where potential red flags are identified.

III. Conclusions

The legal issues arising from formation and operations of a third party as envisioned in this paper appear to be manageable. The specifics interact strongly with choices the member companies make about how the third party is designed; the design affects the legal issues and the legal issues have implications for design. Accordingly, member companies should work closely with their legal advisers in establishing a third party. The approach recommended here is a phased one, in which the third party initially takes on a conservative scope, and takes incremental steps towards more challenging areas.

The authors have discussed the concept of a third party for the dual-use industries with industry representatives, government officials, NGOs and academia. In each of these audiences, the idea has been received positively by most, and such a collaboration is seen as bringing value to preventing proliferation. The breadth, depth and function of such a third party would be determined by the dual-use industries themselves to best suit their needs and interests.

Appendix A: PNNL Research on the Role of Industry in Preventing Proliferation

Since 2005, PNNL has been assessing the role of industry in strengthening governmental efforts to prevent proliferation, primarily focused on the concept of industry self regulation. Self regulation is defined as a systematic, voluntary program of actions undertaken by an industry as a whole of by individual companies to anticipate, implement or supplement regulatory requirements, generally through the adoption of best practices. This assessment has entailed analysis of self regulation approaches for the nuclear, radiological sources and dual-use industries to consider as a means of thwarting proliferation of weapons of mass destruction.

An initial 2005 report[5] presented four case studies of other industries that have taken such a self regulation approach, such as the Kimberly process adopted by the diamond industry to address the issues of 'blood diamonds.' The 2005 report offered a range of options for industry to consider, ranging from a Code of Conduct/Ethics to a third-party verified standard (i.e. ISO). A subsequent (2006) legal analysis[6] was conducted to determine where the greatest benefits could be gained, and suggested that the greatest gaps are in (1) dual-use export controls (an adequate model compliance program is needed); (2) security of radiological sources (better guidance is needed); and (3) physical protection guidance for dual-use items.

Based on this work, PNNL conducted fourteen interviews with dual-use industry representatives, trade associations, and relevant non-governmental organizations (NGOs) to determine their interest in possible self regulation or industry governance approaches. The interviews clarified the challenges industry sees in both meeting existing regulations to ensure that nuclear and dual-use commodities and technologies are controlled and secured, and in adopting some kind of self regulation approach. Some of the challenges identified included proprietary concerns of information sharing on suspicious requests, and a less than collaborative government-industry relationship

A 2008 report[7] described the findings of these interviews, and laid out steps that can be taken by individual companies and industries as a whole to augment the control and security of sensitive goods in the supply chain. The report concluded that ultimately, engagement of entire industries will have the greatest nonproliferation benefit. The report contained a continuum of potential self regulation approaches, ranging from a Code of Conduct or Ethics at one end to a more rigorous, certified standard that would be potentially required, issued and monitored by a third party, such as those granted authority through the ISO at the other end to ensure compliance.

[5] Hund, Gretchen and Oksana Elkhamri. 2005. "Industry Self Regulation as a Means to Promote Nonproliferation. A Pacific Northwest Center for Global Security Publication. PNNL-15355.
[6] Morris, Fred and Gretchen Hund. February 2007. "Legal Analysis: Scope for Industry Self Regulation under Existing Nuclear Export Control and Physical Protection Laws." A Pacific Northwest Center for Global Security Publication. PNNL-16349.
[7] Hund, Gretchen and Amy Seward. November 2008. "Broadening Industry Governance to Include Nonproliferation." A Pacific Northwest Center for Global Security Publication. PNNL-17521.

In October 2011, PNNL convened a workshop with approximately 15 leaders in nonproliferation from government, academia, non-governmental organizations, and industry. For many of the attendees, the meeting was the first opportunity they had had to meet as a group and discuss industry engagement issues. As a result of the meeting, PNNL has pursued research on the role of the financial sector, the legal feasibility of a third party entity for information sharing, and indelible markings to improve dual-use commodity identification.

PNNL has published and presented on the role of industry in promoting nonproliferation in numerous fora. In November 2009, *Nuclear News* published an article by the PNNL team on the role for industry to play in promoting nonproliferation.[8] PNNL also described industry self-regulation and the increasing interest in industry's role in a spring 2011 article for the Federation of American Scientists' *Public Interest Report.*[9]

PNNL has presented research on this topic in several international meetings including at the Nuclear Suppliers Group (NSG) annual plenaries in Budapest, Hungary in 2009, in Noordwijk, Netherlands in June 2011 and in Seattle, WA in June 2012. PNNL also presented the work to the Missile Control Technology Regime (MCTR) in Rio de Janeiro, Brazil in 2009 and at Wilton Park in England in 2012. The work has also been presented at several Institute for Nuclear Materials Management (INMM) meetings and at the International Atomic Energy Agency (IAEA).

PNNL has collaborated or discussed potential collaboration with a number of other organizations, institutions and individuals that are analyzing and promoting an industry role in nonproliferation. These include the American Association for the Advancement of Science (AAAS), American Physical Society, Brookings, Carnegie Endowment for International Peace (CEIP), Institute of Science and International Security (ISIS), the Stimson Center, World Institute for Nuclear Security (WINS) and Nuclear Energy Institute (NEI).

[8] Hund, Gretchen, Amy Seward and Oksana Elkhamri. "A Role for Industry in Promoting Nuclear Security and Nonproliferation." Nuclear News. Nov 2009 edition, p. 58-59.
[9] Hund, Gretchen and Amy Seward. "Self-Regulation to Promote Nonproliferation. Federation of American Scientists Public Interest Report. June 25, 2012. http://www.fas.org/blog/pir/2012/06/25/self-regulation-to-promote-nonproliferation/

Appendix B: Notional Template for Information Sharing[10]

Exporting company		
Date of report	April 2, 2012	
Item	High-power direct current power supply	
Model	DL Series V, Model 500-A	
ECCN	3A226	
Reason for control	NP	
Destination	Cote D'Ivoire	
Check against destination controls		
• **Embargoed country?**	No	
• **License required based on country chart?**	Yes (Column 1)	
• **End-user**	Abidjan Heavy Industries, S.A.	
Other parties to the transaction	Henri Mabri, Managing Director	
Check against end-user prohibitions		
• **Denied persons list?**	Negative	
• **Unverified list?**	Negative	
• **Entity list?**	Negative	
• **Specially designated nationals list?**	Negative	
Stated End Use	"Manufacturing"	
Red flag review (15 CFR Part 732, Supp. 3)	**"x" if concern**	**Comments**
1. Customer reluctant to offer end use information	x	In email exchange, Mr. Mabri declined to elaborate how product would be used beyond "manufacturing"
2. Product does not fit buyer's business	x	Despite name, buyer appears to be a trading company
3. Product incompatible with importing country's technical level	x	Cote d'Ivoire lacks known applications for this product (e.g., automotive, aviation, solar power, R&D)
4. Customer has little business background		
5. Customer willing to pay cash		

[10] Notional template developed by Fred Morris.

6. Customer unfamiliar with product's performance characteristics		
7. Customer declines routine services	x	Mr. Mabri declined offer of installation, maintenance, and training services
8. Delivery dates vague or delivery planned for remote destination	x	Delivery requested to Bondoukou (pop. 60,000) near border with Ghana; city has no known industrial or R&D base
9. Final destination is freight forwarder		
10. Abnormal shipping route		
11. Inconsistent packaging		
12. Buyer evasive about whether item is for domestic use, export, or re-export		
Overall conclusion following red flag review	Red flags cannot be explained or justified; serious concern that buyer intends to re-export though Ghana	
Disposition of export request	Refrain from transaction at this time	

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*

U.S. DEPARTMENT OF
ENERGY

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)
www.pnnl.gov