Andrew Kurzrok and Gretchen Hund

A Hollywood, Florida, conference of specialists in preventing, detecting, and responding to money laundering might not seem to be the most likely spot for the next innovation in nuclear nonproliferation policymaking. Yet, a March speech by Jennifer Shasky Calvery, director of the Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN), suggested an approach that regulators charged with stopping the proliferation of nuclear weapons would do well to study.

Shasky Calvery stated that “FinCEN needs to find ways for more dynamic, real-time information sharing, both by and between financial institutions, and with FinCEN and law enforcement.” The information to which she was referring is transaction data related to money laundering that currently reside within banks, casinos, credit card processing companies, and many other types of financial businesses.

Export control regulators could apply Shasky Calvery’s approach to their own mission. In the nonproliferation context, FinCEN’s anti-money laundering data would be analogous to the inquiries that potential buyers of dual-use commodities place over the phone or on commercial websites. Dual-use commodities have legitimate civilian applications, but can also be used to support nuclear weapons development. If a request appears suspicious, most firms will decline the request. Unlike their counterparts in the financial sector, however, export control regulators and private business have few tools with which to gather and disseminate this critical information about the networks illicitly seeking strategic commodities. Taking a page from the anti-money laundering playbook may help stop proliferation procurement.

Information Sharing Today

To evade detection, proliferators rarely seek sensitive technologies with obvious nuclear weapons applications, such as centrifuges for enriching uranium. Instead, they hunt for readily available raw materials, industrial tools, and laboratory instruments that they can assemble into the elements of a potential nuclear weapons program. This places the commercial marketplace, from metal distributors to oil and gas supply companies, squarely in proliferators’ crosshairs. Although export control laws exist to prevent such transfers, bad actors will go to great lengths to dupe well-meaning firms by hiding their true identities and motives.

Like money launderers, proliferators must interact with legitimate finance and trade systems and divulge to their commercial partners some relevant information about themselves or who they claim to be. In an effort to capitalize on this exchange of information, the Department of Commerce encourages firms to remain vigilant against weak cover stories such as a bakery requesting high-performance computers or a buyer seeking semiconductor manufacturing equipment when the destination country does not have an electronics industry. The Commerce Department encourages suppliers to apply extra scrutiny if the buyer exhibits unusual behaviors, such as refusing a servicing plan (perhaps because the item will be resold) or paying cash for an item that typically requires financing.

These warnings matter because proliferators regularly target the private sector. One alleged
A major European parts manufacturer has reported instances of its many sales offices worldwide receiving identical quotation requests from a prospective buyer, presumably hoping that at least one office would fail to conduct the necessary due diligence.[5]

**Figure 1: The Trail of Proliferation Procurement**

Proliferators use a complex web of front companies, intermediaries, and delivery methods to hide the true nature of their transactions from unwitting suppliers.

Source: Financial Action Task Force; Pacific Northwest National Laboratory.

Although the private sector plays a central role in stopping proliferation, there is no requirement under U.S. law for firms that see suspicious behavior to report it to U.S. regulators or law enforcement. The Commerce Department invites but does not require information sharing, stating in its regulations that “[i]f a person learns that an export control violation of the [Export Administration Regulations] has occurred or may occur, that person may notify” the Office of Export Enforcement, which is in the department’s Bureau of Industry and Security.[6]

To assist industry in reporting potential violations, the Commerce Department maintains a telephone tip line and an online submission capability. In addition, field agents from the Commerce Department conduct outreach visits to companies to introduce themselves as points of contact for questions and tips.[7] The bureau states that the information it gleans from industry is often the most helpful in pursuing cases.[8]

Despite the government’s efforts to encourage information sharing, it does not always occur. In interviews, numerous industry officials said that they avoid cooperating proactively with the government. The officials take this position for business reasons. Today, there are no protections for a firm that files a tip, so alerting the government to suspicious activity may serve only to draw unwanted attention to the fact that the company has a potential proliferation supply risk. For many firms, simply ignoring an order rather than reporting it is an effective compromise that protects the company’s interests while providing some national security benefit.
Stopped Illicit Procurement: Lessons From Global Finance
Published on Arms Control Association (https://www.armscontrol.org)

Unfortunately, discarded data are lost intelligence for government and corporate export control officials from other firms. Proliferators are rarely choosy; to succeed, they need just one supplier to fill an order. Nonproliferators, on the other hand, must defend successfully each time. Sometimes, it is only when the orders come together that a motive becomes clear. Although the purchase of any one item alone is likely ambiguous, a series of orders taken as a whole can suggest the motivation for procurement activities. Today, the lack of information sharing can make it difficult for industry or government to see the wider story.

The Anti-Fraud Approach

Efforts to stop financial fraud may offer a model for nonproliferation. Criminals such as narcotics traffickers and terrorism financiers need to move their funds without arousing suspicion.

Money laundering refers to financial transactions that criminals conduct in an “attempt to disguise the proceeds, sources or nature of their illicit activities.” According to FinCEN, money laundering “involves three steps: placement, layering and integration. First, the illegitimate funds are furtively introduced into the legitimate financial system. Then, the money is moved around to create confusion, sometimes by wiring or transferring through numerous accounts. Finally, it is integrated into the financial system through additional transactions until the ‘dirty money’ appears ‘clean.’”

Because money laundering requires at least the unwitting participation of financial institutions, the private sector often has the best perspective to identify illicit activity as it occurs. For example, internal transaction data enable banks to recognize indicators of potential money laundering, such as repeated transfers of large, round-number currency amounts or trade financing transactions that appear to have unnecessarily complex structures.

In the United States, the Bank Secrecy Act of 1970 (BSA) is the primary piece of legislation to control money laundering. Despite its name, the BSA is relevant to a range of institutions that could be misused for illicit finance, including casinos, money-changing businesses, insurers, and dealers of precious metals and jewelry. A primary requirement of the BSA is that depository institutions must inform FinCEN about unusual transactions through suspicious activity reports (SARs). A report contains information about the institution filing the claim, biographical information about the suspect entity, and a narrative about why the transaction was suspicious. Submitters can include attachments with additional information about the transaction.

FinCEN uses SARs and other reports required under the BSA to cue enforcement actions and analyze broad trends. Approximately every six months, FinCEN publishes a SAR Activity Review based on the aggregation of individual SAR submissions to highlight recent issues.

One essential feature of the BSA is that financial institutions submitting SARs are immune from liability arising from the shared information. Because the reports, by definition, need only report on “suspicious” activity, it is nearly certain that some filings will discuss behavior that, although appearing to be illegal, is entirely benign. If the customer were to learn of the SAR, it could sue the filer for defamation or other injuries. The “safe harbor” provision, as the liability clause is commonly known, protects industry and ensures that firms are not punished for fulfilling their legal requirements.

Although the combination of mandatory reporting with a safe harbor is powerful, it represents only one type of information sharing between industry and government. The 2001 PATRIOT Act added two new dimensions to the financial sector’s information-sharing tool kit. One provision of the act, section 314(a), enables law enforcement officers, through a secure online bulletin board maintained by FinCEN, to ask 22,000 financial institutions whether they have accounts or transactions related to suspects of terrorism and money laundering. This powerful querying capability simplifies what would otherwise be a nearly impossible task of engaging each institution individually. Also, a unified process simplifies responses for respondents. Rather than managing requests from many organizations, financial institutions receive a batch of requests from a single contact every two weeks.

This cooperation appears to pay dividends. Forty percent of requests from law enforcement
organizations receive at least one response from financial institutions. Of those requests with at least one response, law enforcement learns about an average of 8.4 bank accounts and 16.2 financial transactions related to the suspect.[12]

The second information-sharing aspect authorized by the PATRIOT Act, Section 314(b), is perhaps more radical. The provision permits financial entities assisting in the preparation of SARs to share information related to suspicious activities. Any financial transaction has at least two parties, so sharing information helps the financial entities involved untangle the sometimes complex structures that money launderers use to hide their activities.

For example, a money launderer might gamble at one casino with the winnings from another casino. “Cleaning” illicit funds through multiple locations makes following the money extremely difficult. If the two casinos work together to match the transactions, however, they may be able to unravel the laundering scheme. As with information shared with the government, a safe harbor provision protects firms that share information.[13]

The combination of obligations and protections under the BSA and the PATRIOT Act gives financial regulators and institutions powerful tools to combat money laundering. Information can move legally and securely among all interested parties to ensure that all parties with a need to know are aware of suspicious activities and trends.

Lessons for Nonproliferation

The anti-money laundering model is a useful precedent for export control regulators and enforcement agents. Through a combination of law, regulation, and policy, financial companies can work together and with the government to identify suspicious activity.[14]

A safe harbor from prosecution or civil liability may encourage commodity suppliers to be more forthcoming with tips. Although a safe harbor may reduce the number of opportunities for export enforcement agencies to pursue prosecutions, the value of the additional information for U.S. nonproliferation policy will likely outweigh that drawback.

A rapid-response mechanism for law enforcement could also help the U.S. government quickly assess the scale of a proliferator’s procurement efforts. An efficient request-for-information process, particularly under circumstances in which a safe harbor encourages enhanced reporting of tips, could help law enforcement organizations. Because nonproliferation cases can take years to build, there is a risk that proliferators will continue their activities in ways that authorities cannot track.[15] By polling suppliers, the government would reduce the chances that additional exports would take place without being noticed.

Better information analysis products could help this process. Some of the officials interviewed said they provide information to law enforcement, but expressed frustration that they did not know whether their tips were useful. Others struggled to understand the top proliferation challenges and how they could help.

Although limited by the restrictions imposed by classification requirements and the confidentiality of ongoing investigations, government-published trend analysis would provide industry with valuable feedback about its support and ensure that it remains vigilant against the latest threats. FinCEN’s SAR Activity Reviews are a useful precedent of a regular, unclassified analytic product to help inform industry. Appropriate authors of this analysis might include the Commerce Department, the Department of Homeland Security’s Homeland Security Investigations unit, or the interagency Export Enforcement Coordination Center.

It is unclear whether the equivalent of a mandatory SAR is appropriate for suppliers of dual-use commodities. Generally, U.S. law does not obligate citizens to report crimes; alerting the police is considered a civic duty, not a legal one. In this light, the financial industry’s requirement to report suspicious activity is unusual. Although money laundering and proliferation both are crimes with significant impacts, some differences between them raise questions as to whether suspicious dual-use commodity requests should require similar reporting requirements.
For example, financial institutions generally report on money laundering crimes potentially in progress, rather than the future crimes that could take place if a suspicious order were to be filled. Furthermore, unlike money laundering, proliferation procurement is a relatively specialized criminal enterprise that is prosecuted relatively infrequently. Congress, executive agencies, and industry would need to determine whether the nonproliferation benefits of increased information, particularly when coupled with limited liability, would outweigh the financial and civil liberty implications associated with mandatory reporting.

Rules to govern how and under what circumstances businesses could share nonproliferation information among themselves might be valuable, although the principles from section 314(b) would likely need to be modified for the nonproliferation context. Because banking transactions are usually between two institutions on behalf of their clients, it is natural for the institutions to cooperate. In this way, both financial entities benefit from the pooled client information and thus better protect their own businesses from money laundering. Because vendors of dual-use commodities exist in a more complex supply chain, information sharing between two firms may not materially improve either firm’s understanding of the proliferation network. Proliferation requires many items; therefore, integrating information from many firms is most likely to help identify suspicious behaviors. A single point of contact, known as a third party, may enable firms to coordinate this information while managing antitrust risks.[16]

Improving information sharing among U.S. law enforcement organizations and industry is an important first step. Because proliferators target suppliers from many countries, it will be important to consider whether companies and governments can securely share information internationally. Without the legislative safe-harbor protections that could be afforded as part of domestic sharing, companies may fear the liability implications of participating. Further, although law enforcement could handle any domestic misuse of shared information through prosecutions, the international recourse for data misuse are limited. If these challenges prove manageable, however, the resulting globally sourced information would have significant nonproliferation benefits.

Conclusion

Stopping the illicit spread of nuclear weapons technologies requires global cooperation among governments and industry, particularly on information sharing. Currently, U.S. export regulations do not give suppliers an incentive to cooperate. Instead, doing the right thing and sharing suspicions can create perceived if not actual legal exposure for a company.

With these dynamics, identifying models that can illuminate new approaches is beneficial. Because money laundering supports narcotics trafficking and terrorism, financial regulators and enforcement agents have developed strong tools to work with industry productively.

More-effective information sharing will not cure all ills; procurement agents will continue to develop new approaches to circumvent or undermine nonproliferation efforts. Similarly, any proposal should not copy anti-money laundering rules directly into export control regulations. The dual-use commodity supply chain has unique considerations that must be taken into account.

Implementing a new information-sharing approach will require champions within government and industry. Regulators could execute some elements of improved information sharing administratively, but a safe harbor would likely require congressional action. For any new activity, industry will need to provide input to ensure that any information-sharing proposal is feasible and provides benefits to the private sector.

Results from the financial sector show that secure information sharing is possible and can help stop crimes. With the lessons from the banking sector in mind, it is worth thinking anew about how government and industry could better share information to stop nuclear crimes. A failure to do so would have consequences that go far beyond the financial ones.

Andrew Kurzrok is a research scientist and Gretchen Hund is a senior scientist at Pacific Northwest National Laboratory in Washington state. The views expressed are their own and do not
necessarily represent the views of the laboratory or the U.S. Department of Energy.

ENDNOTES


14. FinCEN provisions may encourage financial institutions to share more information than required
based on the logic that it is preferable to let the government sift through too much data rather than face a penalty for failing to disclose suspicious activity.

15. During *Khaki*, for example, communications with an undercover agent spanned two years.


**Source URL:** https://www.armscontrol.org/act/2014-06/stopping-illicit-procurement-lessons-global-finance