preventing the products and services of the Money Services Business from being used to facilitate money laundering or terrorist financing through these relationships and detecting the use of these products and services for money laundering or terrorist financing by the Money Services Business or agent. Relevant risk factors may include, but are not limited to:

- The foreign agent or counterparty's location and jurisdiction of organization, chartering, or licensing. This would include considering the extent to which the relevant jurisdiction is internationally recognized as presenting a greater risk for money laundering or is considered to have more robust anti-money laundering standards.
- The ownership of the foreign agent or counterparty. This includes whether the owners are known, upon reasonable inquiry, to be associated with criminal conduct or terrorism. For example, have the individuals been designated by Treasury's Office of Foreign Assets Control as Specially Designated Nationals or Blocked Persons (*i.e.*, involvement in terrorism, drug trafficking, or the proliferation of weapons of mass destruction)?
- The extent to which the foreign agent or counterparty is subject to anti-money laundering requirements in its jurisdiction and whether it has established such controls.
- Any information known or readily available to the Money Services Business about the foreign agent or counterparty's anti-money laundering record, including public information in industry guides, periodicals, and major publications.
- The nature of the foreign agent or counterparty's business, the markets it serves, and the extent to which its business and the markets it serves present an increased risk for money laundering or terrorist financing.
- The types and purpose of services to be provided to, and anticipated activity with, the foreign agent or counterparty.
- The nature and duration of the Money Services Business' relationship with the foreign agent or counterparty.

Specifically, a Money Services Business' anti-money laundering program should include procedures for the following:

1. Conduct of Due Diligence on Foreign Agents and Counterparties

Money Services Businesses should establish procedures for conducting reasonable, risk-based due diligence on potential and existing foreign agents and counterparties to help ensure that such foreign agents and counterparties are not themselves complicit in illegal activity involving the Money Services Business' products and services, and that they have in place appropriate anti-money laundering controls to guard against the abuse of the Money Services Business' products and services. Such due diligence must, at a minimum, include reasonable procedures to identify the owners of the Money Services Business' foreign agents and counterparties, as well as to evaluate, on an ongoing basis, the operations of those foreign agents and counterparties and their implementation of policies, procedures, and controls reasonably designed to help assure that the Money Services Business' products and services are not subject to abuse by the foreign agent's or counterparty's customers, employees, or contractors.[5] The extent of the due diligence required will depend on a variety of factors specific to each agent or counterparty. We expect Money Services Businesses to assess such risks and perform due diligence in a manner consistent with that risk, in light of the availability of information.

2. Risk-based Monitoring of Foreign Agents or Counterparties

In addition to the due diligence described above, in order to detect and report suspected money laundering or terrorist financing, Money Services Businesses should establish procedures for risk-based monitoring and review of transactions from, to, or through the United States that are conducted through foreign agents and counterparties.[6] Such procedures should also focus on identifying material changes in the agent's risk profile, such as a change in ownership, business, or the regulatory scrutiny to which it is subject.

The review of transactions should enable the Money Services Business to identify and, where appropriate, report as suspicious such occurrences as: instances of unusual wire activity, bulk sales or purchases of sequentially numbered instruments, multiple purchases or sales that appear to be structured, and illegible or missing customer information. Additionally, Money Services Businesses should establish procedures to assure that their foreign agents or counterparties are effectively implementing an anti-money laundering program and to discern obvious breakdowns in the implementation of the program by the foreign agent or counterparty.

Similarly, money transmitters should have procedures in place to enable them to review foreign agent or counterparty activity for signs of structuring or unnecessarily complex transmissions through multiple jurisdictions that may be indicative of layering. Such procedures should also enable them to discern attempts to evade identification or other requirements, whether imposed by applicable law or by the Money Services Business' own internal policies. Activity by agents or counterparties that appears aimed at evading the Money Services Business' own controls can be indicative of complicity in illicit conduct; this activity must be scrutinized, reported as appropriate, and corrective action taken as warranted.

[5] Our anti-money laundering program rule, 31 CFR 103.125(d)(iii), permits Money Service Businesses to satisfy this last requirement with regard to their domestic agents (which are also Money Service Businesses under the BSA regulations), by allocating responsibility for the program to their agents. Such an allocation, however, does not relieve a Money Service Business from ultimate responsibility for establishing and maintaining an effective anti-money laundering program. *Id.*

[6] Nothing in this Interpretive Guidance is intended to require Money Service Businesses to monitor or review, for purposes of the Bank Secrecy Act, transactions or activities of foreign agents or counterparties that occur entirely outside of the United States and do not flow from, to, or through the United States.

3. Corrective Action and Termination

Money Services Businesses should have procedures for responding to foreign agents or counterparties that present unreasonable risks of money laundering or the financing of terrorism. Such procedures should provide for the implementation of corrective action on the part of the foreign agent or counterparty or for the termination of the relationship with any foreign agent or counterparty that the Money Services Business determines poses an unacceptable risk of money laundering or terrorist financing, or that has demonstrated systemic, willful, or repeated lapses in compliance with the Money Services Business' own anti-money laundering procedures or requirements.

While Money Services Businesses may already have implemented some or all of the procedures described in this Interpretive Guidance as a part of their anti-money laundering programs, we wish to provide a reasonable period of time for all affected Money Services Businesses to assess their operations, review their existing policies and programs for compliance with this Advisory, and implement any additional necessary changes. We will expect full compliance with this Interpretive Release within 180 days.

Finally, we are mindful of the potential impact that this Interpretive Release may have on continuing efforts to bring informal value transfer systems into compliance with the existing regulatory framework of the Bank Secrecy Act. Experience has demonstrated the challenges in securing compliance by, for instance, hawalas and other informal value transfer systems. Further specification of Bank Secrecy Act compliance obligations carries with it the risk of driving these businesses underground, thereby undermining our ultimate regulatory goals. On balance, however, we believe that outlining the requirements for dealing with foreign agents and counterparties, including informal networks, is appropriate in light of the risks of money laundering and the financing of terrorism.

William J. Fox,

Director.

[FR Doc. 04–27287 Filed 12–13–04; 8:45 am]

BILLING CODE 4810–02–P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

33 CFR Part 117

[CGD01–04–146]

Drawbridge Operation Regulations: Merrimack River, MA

AGENCY: Coast Guard, DHS.

ACTION: Notice of temporary deviation from regulations.

SUMMARY: The Commander, First Coast Guard District, has issued a temporary deviation from the drawbridge operation

regulations for the Essex Merrimack Bridge, mile 5.8, across the Merrimack River, at Newburyport, Massachusetts. This deviation allows the bridge to remain in the closed position from 6 a.m. on December 13, 2004 through 6 p.m. on December 17, 2004. This temporary deviation is necessary to facilitate structural repairs at the bridge.

DATES: This deviation is effective from December 13, 2004 through December 17, 2004.

FOR FURTHER INFORMATION CONTACT: John McDonald, Project Officer, First Coast Guard District, at (617) 223–8364.

SUPPLEMENTARY INFORMATION: The Essex Merrimack Bridge, at mile 5.8, across the Merrimack River, has a vertical clearance of 15 feet at mean high water, and 22 feet at mean low water in the closed position. The existing regulations are listed at 33 CFR § 117.605(c).

The bridge owner, Massachusetts Highway Department, requested a temporary deviation from the drawbridge operating regulations to facilitate necessary structural repairs to the balance wheels at the bridge.

This deviation to the operating regulations allows the bridge to remain in the closed position from 6 a.m. on December 13, 2004 through 6 p.m. on December 17, 2004.

This deviation from the operating regulations is authorized under 33 CFR § 117.35 and will be performed with all due speed in order to return the bridge to normal operation as soon as possible.

Dated: December 3, 2004.

David P. Pekoske,

Rear Admiral, U.S. Coast Guard, Commander, First Coast Guard District.

[FR Doc. 04–27303 Filed 12–13–04; 8:45 am]

BILLING CODE 4910–15–P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

33 CFR Part 165

[CGD05–04–216]

RIN 1625–AA00

Security Zone; Cape Fear River, Eagle Island, North Carolina State Port Authority Terminal, Wilmington, NC

AGENCY: Coast Guard, DHS.

ACTION: Temporary final rule.

SUMMARY: The Coast Guard is establishing a temporary security zone at the North Carolina State Port Authority (NCSPA), Wilmington to include the Cape Fear River and Eagle Island. Entry into or movement within the security zone will be prohibited without authorization from the COTP. This action is necessary to safeguard the vessels and the facility from sabotage, subversive acts, or other threats.

DATES: This rule is effective from December 3, 2004, until April 1, 2005.

ADDRESSES: Documents indicated in this preamble as being available in the docket are part of docket CGD05–04–216 and are available for inspection or copying at the Marine Safety Office 721 Medical Center Drive, Suite 100, Wilmington, North Carolina 28401 between 7:30 a.m. and 3 p.m., Monday through Friday, except Federal holidays.

FOR FURTHER INFORMATION CONTACT: LCDR Charles A. Roskam II, Chief Port Operations (910) 772–2200 or toll free (877) 229–0770.

SUPPLEMENTARY INFORMATION:

Regulatory Information

We did not publish a notice of proposed rulemaking (NPRM) for this rule. The Coast Guard is promulgating this security zone regulation to protect NCSPA Wilmington and the surrounding vicinity from threats to national security. Accordingly, based on the military function exception set forth in the Administrative Procedure Act, 5 U.S.C. 553(a)(1), notice and comment rule-making and advance publication are not required for this regulation.

Background and Purpose

Vessels frequenting the North Carolina State Port Authority (NCSPA) Wilmington facility serve as a vital link in the transportation of military munitions, explosives, equipment, and personnel in support of Department of Defense missions at home and abroad. This vital transportation link is potentially at risk to acts of terrorism, sabotage and other criminal acts. Munitions and explosives laden vessels also pose a unique threat to the safety and security of the NCSPA Wilmington, vessel crews, and others in the maritime and surrounding community should the vessels be subject to acts of terrorism or sabotage, or other criminal acts. The ability to control waterside access to vessels laden with munitions and explosives, as well as those used to transport military equipment and personnel, moored at the NCSPA Wilmington is critical to national defense and security, as well as to the safety and security of the NCSPA Wilmington, vessel crews, and others in the maritime and surrounding community. Therefore, the Coast Guard is establishing this security zone to safeguard human life, vessels and facilities from sabotage, terrorist acts or other criminal acts.

Discussion of Rule

The security zone is necessary to provide security for, and prevent acts of terrorism against vessels loading or offloading at the NCSPA Wilmington facility during a military operation. It will include an area from 800 yards south of the Cape Fear River Bridge encompassing the southern end of Eagle Island, the Cape Fear River, and the grounds of the State Port Authority Terminal south to South Wilmington Terminal. The security zone will prevent access to unauthorized persons who may attempt to enter the secure area via the Cape Fear River, the North Carolina State Port Authority terminal, or use Eagle Island as vantage point for surveillance of the secure area. The security zone will protect vessels moored at the facility, their crews, others in the maritime community and the surrounding communities from subversive or terrorist attack that could cause serious negative impact to vessels, the port, or the environment, and result in numerous casualties.

No person or vessel may enter or remain in the security zone at any time without the permission of the Captain of the Port, Wilmington. Each person or vessel operating within the security zone will obey any direction or order of the Captain of the Port. The Captain of the Port may take possession and control of any vessel in a security zone and/or remove any person, vessel, article or thing from this security zone.

Regulatory Evaluation

This rule is not a ''significant regulatory action'' under section 3(f) of Executive Order 12866, Regulatory Planning and Review, and does not require an assessment of potential costs and benefits under section 6(a)(3) of that Order. The Office of Management and Budget has not reviewed it under that Order. It is not ''significant'' under the regulatory policies and procedures of the Department of Homeland Security (DHS).

Although this regulation restricts access to the security zone, the effect of this regulation will not be significant because: (i) The COTP or his or her representative may authorize access to the security zone; (ii) the security zone will be enforced for limited duration; and (iii) the Coast Guard will make notifications via maritime advisories so mariners can adjust their plans accordingly.