for 6 years and 3 months from the date of closeout (where closeout is the date FEMA closes the grant in its financial system) and final audit and appeals are resolved and then deleted. Records of real properties (property acquisition agreement and lists of acquired properties) acquired with FEMA funds for maintenance in accordance with agreement terms of the grant cannot be destroyed until agreement with locality is no longer viable.

SYSTEM MANAGER AND ADDRESS:

Director, Risk Reduction Division, FEMA, 1800 South Bell Street, Arlington, VA 20598–3030.

NOTIFICATION PROCEDURE:

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the FEMA FOIA Officer, whose contact information can be found at *http://www.dhs.gov/foia* under ''contacts.'' If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, 245 Murray Drive SW., Building 410, STOP–0655, Washington, DC 20528.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, *http://www.dhs.gov* or 1–866–431–0486. In addition you must:

- Explain why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created;
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records; and
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without the above information the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

RECORD ACCESS PROCEDURES:

See ''Notification procedure'' above.

CONTESTING RECORD PROCEDURES:

See ''Notification procedure'' above.

RECORD SOURCE CATEGORIES:

Information in this system of records is obtained by FEMA from state, local, tribal, territorial governments, and private and non-profit organizations via hard copy and electronic applications for assistance. Individual property owners cannot apply directly to FEMA for assistance.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: July 12, 2012.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2012–17783 Filed 7–20–12; 8:45 am]

BILLING CODE 9110–17–P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[Docket No. USCG–2012–0546]

Policy on the 2009 Revision of the International Maritime Organization Code for the Construction and Equipment of Mobile Offshore Drilling Units

AGENCY: Coast Guard, DHS.

ACTION: Notice of availability.

SUMMARY: The Coast Guard announces the availability of CG–ENG Policy Letter 02–12, ''Acceptance of the 2009 MODU Code.'' On December 2, 2009, the International Maritime Organization (IMO) adopted IMO Assembly Resolution A.1023(26), Code for the Construction and Equipment of Mobile Offshore Drilling Units, 2009 (2009 MODU Code). CG–ENG Policy Letter 02–12 establishes that the Coast Guard considers the design and equipment standards of the 2009 MODU Code to be at least as effective as the design and equipment standards of the 1979 and 1989 versions of the MODU Code. Therefore, an Officer in Charge, Marine Inspection (OCMI) may consider a foreign documented MODU with a valid 2009 MODU Code Certificate issued by the flag state or its authorized agent to comply with 33 CFR 143.207(c) after confirming substantial compliance with the provisions of the 2009 MODU Code.

DATES: CG–ENG Policy Letter 02–12 is effective as of May 7, 2012.

ADDRESSES: This notice and the documents referenced within are available in the docket and can be viewed by going to *www.regulations.gov,* inserting USCG–2012–0546 in the ''Keyword'' box, and then clicking ''Search.'' CG–ENG Policy Letter 02–12 is also available at www.uscg.mil and can be viewed by clicking the link to the Office of Design and Engineering Standards (CG–ENG) under the ''Units,'' ''USCG Headquarters Organization,'' and ''CG–5P'' tabs, and scrolling down to ''Policy Documents.''

FOR FURTHER INFORMATION CONTACT: If you have questions on this notice or CG–ENG Policy Letter 02–12, call or email Lieutenant Commander Heather Mattern, Human Element and Ship Design Division (CG–ENG–1), telephone (202) 372–1361, or email *Heather.R.Mattern@uscg.mil*. If you have questions on viewing material in the docket, call Renee V. Wright, Program Manager, Docket Operations, telephone (202) 366–9826.

SUPPLEMENTARY INFORMATION:

Background and Purpose

Foreign documented MODUs engaged in any offshore activity associated with the exploration for, or development or production of, the minerals of the U.S. Outer Continental Shelf (OCS) must comply with one of three options outlined in 33 CFR 143.207, which deal with design and equipment standards. The majority of foreign MODU operators on the OCS choose to comply with 33 CFR 143.207(c), often referred to as ''Option C.'' When choosing this option, MODU operators present the OCMI with a valid MODU Code Certificate issued by the flag state or an agent authorized to act on its behalf. Existing regulation and policy permits MODUs to comply with the design and equipment standards in the 1979 MODU Code or 1989 MODU Code.

The Coast Guard has evaluated the 2009 MODU Code, which applies to MODUs, the keels of which are laid or at a similar stage of construction on or after January 1, 2012. The Coast Guard considers the design and equipment standards of the 2009 MODU Code to be at least as effective as the design and equipment standards of the 1979 and

1989 MODU Codes. Therefore, OCMIs may consider a foreign MODU with a valid 2009 MODU Code Certificate issued by the flag state or its authorized agent to be compliant with 33 CFR 143.207(c) after confirming that the MODU is in substantial compliance with the provisions of the 2009 MODU Code.

The guidance in this notice and CG–ENG Policy Letter 02–12 is not a substitute for applicable legal requirements, nor is it itself a rule. It is intended to provide operational guidance for Coast Guard personnel and is not intended to nor does it impose legally binding requirements on any party outside the Coast Guard. It represents the Coast Guard's current thinking on this topic and may assist industry, mariners, the general public, and the Coast Guard, as well as other Federal and State regulators, in applying statutory and regulatory requirements.

This notice is issued under authority of 43 U.S.C. 1331, et seq., 5 U.S.C. 552(a), and 33 CFR 1.05–1.

Dated: July 12, 2012.

J.G. Lantz,

Director of Commercial Regulations and Standards, U.S. Coast Guard.

[FR Doc. 2012–17572 Filed 7–20–12; 8:45 am]

BILLING CODE 9110–04–P

DEPARTMENT OF HOMELAND SECURITY

U.S. Customs and Border Protection

Notice of Issuance of Final Determination Concerning Certain Devices Known as ''Pwn Plugs''

AGENCY: U.S. Customs and Border Protection, Department of Homeland Security.

ACTION: Notice of final determination.

SUMMARY: This document provides notice that U.S. Customs and Border Protection (''CBP'') has issued a final determination concerning the country of origin of certain devices known as Pwn Plugs. Based upon the facts presented, CBP has concluded that the programming operations performed in the United States, using U.S.-origin software, substantially transform non-TAA country microcomputer devices. Therefore, the country of origin of Pwn Plugs is the United States for purposes of U.S. Government procurement.

DATES: The final determination was issued on July 13, 2012. A copy of the final determination is attached. Any party-at-interest, as defined in 19 CFR 177.22(d), may seek judicial review of this final determination on or before August 22, 2012.

FOR FURTHER INFORMATION CONTACT: Heather K. Pinnock, Valuation and Special Programs Branch: (202) 325–0034.

SUPPLEMENTARY INFORMATION: Notice is hereby given that on July 13, 2012, pursuant to subpart B of Part 177, U.S. Customs and Border Protection Regulations (19 CFR part 177, subpart B), CBP issued a final determination concerning the country of origin of certain devices known as Pwn Plugs which may be offered to the U.S. Government under an undesignated government procurement contract. This final determination, HQ H215555, was issued under procedures set forth at 19 CFR part 177, subpart B, which implements Title III of the Trade Agreements Act of 1979, as amended (19 U.S.C. § 2511–18). In the final determination, CBP concluded that, based upon the facts presented, the programming operations performed in the United States, using U.S.-origin software, substantially transform non-TAA country microcomputer devices. Therefore, the country of origin of the Pwn Plugs is the United States for purposes of U.S. Government procurement.

Section 177.29, CBP Regulations (19 CFR 177.29), provides that a notice of final determination shall be published in the **Federal Register** within 60 days of the date the final determination is issued. Section 177.30, CBP Regulations (19 CFR 177.30), provides that any party-at-interest, as defined in 19 CFR 177.22(d), may seek judicial review of a final determination within 30 days of publication of such determination in the **Federal Register**.

Dated: July 13, 2012.

Sandra L. Bell,

Executive Director, Regulations and Rulings, Office of International Trade.

Attachment

HQ H215555

July 13, 2012

MAR OT:RR:CTF:VS H215555 HkP

CATEGORY: Origin

Mr. Dave Porcello
CEO, Pwnie Express
Rapid Focus Security, LLC
27 French Street
Barre, VT 05641

RE: U.S. Government Procurement; Trade Agreements Act; Country of Origin of the ''Pwn Plug''; Substantial Transformation

Dear Mr. Porcello: This is in response to your undated letter, received on April 20, 2012, requesting a final determination on behalf of Rapid Focus Security, LLC, dba Pwnie Express (''Pwnie Express''), pursuant to subpart B of part 177 of the U.S. Customs and Border Protection (''CBP'') Regulations (19 C.F.R. Part 177). Under these regulations, which implement Title III of the Trade Agreements Act of 1979 (''TAA''), as amended (19 U.S.C. § 2511 et seq.), CBP issues country of origin advisory rulings and final determinations as to whether an article is or would be a product of a designated country or instrumentality for the purposes of granting waivers of certain ''Buy American'' restrictions in U.S. law or practice for products offered for sale to the U.S. Government.

This final determination concerns the country of origin of the ''Pwn Plug''. As a U.S. importer, Pwnie Express is a party-at-interest within the meaning of 19 C.F.R. § 177.22(d)(1) and is entitled to request this final determination.

FACTS:

The Pwn Plug is described as a full security testing suite packed into a micro-server the size of a power brick that provides covert, encrypted access over Ethernet, wireless and 3G/GSM connections. Its proprietary software is designed to conduct cyber security audits (''penetration tests'') of computer networks, including password auditing, vulnerability checking, network traffic inspecting, wireless network analysis, network port/service scanning, and firewall rule validating. The Pwn Plug runs on the publicly available off-the-shelf SheevaPlug computer platform (a microcomputer device that runs network-based software services that normally require a dedicated computer) made in China. Various types of wireless adapters and an external storage card can be attached to the Pwn Plug by the end-user. There are two versions of the Pwn Plug: the Pwn Plug Wireless, and the Pwn Plug Elite, both referred to herein as the Pwn Plug.

Pwnie Express imports SheevaPlug microcomputer devices from China that measure 4.3 x 2.7 x 1.9 inches and contain a central processing unit, memory chips (SDRAM and HDD), and a SDHC/SDIO card slot for disk and Input/Output expansion. Pwnie Express removes all software from the SheevaPlugs, including their operating systems, and programs them with the following software: Marvell/DENX U-boot environment (BIOS); Linux Kernel package; Ubuntu/Debian Linux open-source base operating system; Open-source security testing suite; Pwnie Express web User Interface; and, Pwnie Express remote access scripts. The Linux software and the other open-source tools were developed by the worldwide open-source community. The role of this software is to provide the basic operating system environment and the security tools needed to perform standard cyber security penetration tests. The role of Pwnie Express' proprietary software, developed entirely in the U.S., is to conduct the actual penetration tests of computer networks. It provides secure and reliable remote access over a variety of network protocols and customer environments and has its own interface for web-based configuration and set-up. Software installation takes approximately two hours. Product literature and packaging are printed