

Dated: July 7, 2017.

Anna K. Abram,
Deputy Commissioner for Policy, Planning,
Legislation, and Analysis.

[FR Doc. 2017-14566 Filed 7-11-17; 8:45 am]

BILLING CODE 4164-01-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

National Cancer Institute; Amended Notice of Meeting

Notice is hereby given of a change in the meeting of the National Cancer Institute Special Emphasis Panel, July 20, 2017, 11:00 a.m. to July 20, 2017, 05:00 p.m., National Cancer Institute Shady Grove, Shady Grove, 9609 Medical Center Drive, 7W102, Rockville, MD 20850 which was published in the **Federal Register** on May 31, 2017, 82 FR 24983.

The meeting notice is amended to change the meeting title to "Core Infrastructure & Epidemiology Cohorts". The meeting date has been changed to August 8, 2017 and the contact person has been changed to Shakeel Ahmad, Ph.D.; phone 240-276-6349; ahmads@mail.nih.gov. The meeting is closed to the public.

Dated: July 6, 2017.

Melanie J. Pantoja,
Program Analyst, Office of Federal Advisory Committee Policy.

[FR Doc. 2017-14539 Filed 7-11-17; 8:45 am]

BILLING CODE 4140-01-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

National Institute on Aging; Notice of Closed Meeting

Pursuant to section 10(d) of the Federal Advisory Committee Act, as amended (5 U.S.C. App.), notice is hereby given of the following meeting.

The meeting will be closed to the public in accordance with the provisions set forth in sections 552b(c)(4) and 552b(c)(6), Title 5 U.S.C., as amended. The grant applications and the discussions could disclose confidential trade secrets or commercial property such as patentable material, and personal information concerning individuals associated with the grant applications, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Name of Committee: National Institute on Aging Special Emphasis Panel; The Dog Aging Project.

Date: August 4, 2017.

Time: 11:00 a.m. to 3:00 p.m.

Agenda: To review and evaluate grant applications.

Place: National Institute on Aging, Gateway Building, 2W200, 7201 Wisconsin Ave., Bethesda, MD 20892, (Telephone Conference Call).

Contact Person: Isis S. Mikhail, DRPH, MD, MPH, National Institute on Aging, Gateway Building, 7201 Wisconsin Avenue, Suite 2C212, Bethesda, MD 20892, 301-402-7704, MIKHAIL@MAIL.NIH.GOV.

(Catalogue of Federal Domestic Assistance Program Nos. 93.866, Aging Research, National Institutes of Health, HHS)

Dated: July 6, 2017.

Melanie J. Pantoja,
Program Analyst, Office of Federal Advisory Committee Policy.

[FR Doc. 2017-14540 Filed 7-11-17; 8:45 am]

BILLING CODE 4140-01-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

Center for Scientific Review; Notice of Closed Meeting

Pursuant to section 10(d) of the Federal Advisory Committee Act, as amended (5 U.S.C. App.), notice is hereby given of the following meeting.

The meeting will be closed to the public in accordance with the provisions set forth in sections 552b(c)(4) and 552b(c)(6), Title 5 U.S.C., as amended. The grant applications and the discussions could disclose confidential trade secrets or commercial property such as patentable material, and personal information concerning individuals associated with the grant applications, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Name of Committee: Center for Scientific Review Special Emphasis Panel; Myocardial Ischemia and Metabolism Members Conflict.

Date: August 1-2, 2017.

Time: 12:00 p.m. to 5:00 p.m.

Agenda: To review and evaluate grant applications.

Place: National Institutes of Health, 6701 Rockledge Drive, Bethesda, MD 20892, (Virtual Meeting).

Contact Person: Abdelouahab Aitouche, Ph.D., Scientific Review Officer, Center for Scientific Review, National Institutes of Health, 6701 Rockledge Drive, Room 4222, MSC 7814, Bethesda, MD 20892, 301-435-2365, aitouchea@csr.nih.gov.

(Catalogue of Federal Domestic Assistance Program Nos. 93.306, Comparative Medicine; 93.333, Clinical Research, 93.306, 93.333, 93.337, 93.393-93.396, 93.837-93.844,

93.846-93.878, 93.892, 93.893, National Institutes of Health, HHS)

Dated: July 6, 2017.

Melanie J. Pantoja,
Program Analyst, Office of Federal Advisory Committee Policy.

[FR Doc. 2017-14538 Filed 7-11-17; 8:45 am]

BILLING CODE 4140-01-P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[Docket No. USCG-2016-1084]

Navigation and Vessel Inspection Circular (NVIC) 05-17; Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities

AGENCY: Coast Guard, DHS.

ACTION: Notice of availability and request for comments.

SUMMARY: The Coast Guard announces the availability of draft Navigation and Inspection Circular (NVIC) 05-17; Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities, and requests public comment on the draft. This NVIC proposes to clarify the existing requirements under MTSA to incorporate analysis of computer and cyber risks and guidance for addressing those risks. This NVIC would provide guidance on incorporating cybersecurity risks into an effective Facility Security Assessment (FSA), as well as additional recommendations for policies and procedures that may reduce cyber risk to operators of maritime facilities. Operators may use this document as a benchmark to develop and implement measures and activities for effective self-governance of cyber risks.

DATES: Comments must be submitted to the online docket via <http://www.regulations.gov>, or reach the Docket Management Facility, on or before September 11, 2017.

FOR FURTHER INFORMATION CONTACT: If you have questions on this notice, call or email, Jason Warren, Coast Guard; telephone 202-372-1106, email Jason.S.Warren@uscg.mil or LCDR Josephine Long, Coast Guard; telephone 202-372-1109, email Josephine.A.Long@uscg.mil.

ADDRESSES: You may submit comments identified by docket number USCG-2016-1084 using the Federal eRulemaking Portal at <http://www.regulations.gov>. See the "Public Participation and Request for Comments" portion of the

SUPPLEMENTARY INFORMATION section for further instructions on submitting comments.

SUPPLEMENTARY INFORMATION:

Public Participation and Request for Comments

We encourage you to submit comments (or related material) on the draft NVIC. We will consider all submissions and may adjust our final action based on your comments. If you submit a comment, please include the docket number for this notice, indicate the specific section of this document to which each comment applies, and provide a reason for each suggestion or recommendation.

We encourage you to submit comments through the Federal eRulemaking Portal at <http://www.regulations.gov>. If your material cannot be submitted using <http://www.regulations.gov>, contact the person in the **FOR FURTHER INFORMATION CONTACT** section of this document for alternate instructions. Documents mentioned in this notice, and all public comments, are in our online docket at <http://www.regulations.gov> and can be viewed by following that Web site's instructions. Additionally, if you go to the online docket and sign up for email alerts, you will be notified when comments are posted or a final rule is published.

We accept anonymous comments. All comments received will be posted without change to <http://www.regulations.gov> and will include any personal information you have provided. For more about privacy and the docket, you may review a Privacy Act notice regarding the Federal Docket Management System in the March 24, 2005, issue of the **Federal Register** (70 FR 15086).

Discussion

As highlighted in the United States Coast Guard Cyber Strategy, cyber security is one of the most serious economic and national security challenges we face as a nation. Adversaries, including state-sponsored and independent hacker groups, terrorists, Transnational Organized Crime groups, and insider threats can pose significant threats to our nation's Marine Transportation System (MTS). Yet these same systems allow the MTS to operate with an impressive record of efficiency and reliability. With approximately 360 sea and river ports, which handle more than \$1.3 trillion in annual cargo, we are dependent on a safe, secure, and efficient MTS, which in turn is highly dependent on a

complex, globally-networked system of technology.

The maritime industry continues to increase use of cyber technology. Facility operators use computers and cyber dependent technologies for communications, engineering, cargo control, environmental control, access control, passenger and cargo screening, and many other purposes. Facility safety and security systems, such as security monitoring, fire detection, and general alarm installations increasingly rely on computers and networks. While these computer and network systems create benefits, they are inherently vulnerable and could introduce new vulnerabilities. Exploitation, misuse, or simple failure of cyber systems can cause injury or death, harm the marine environment, disrupt vital trade activity, and degrade the ability to respond to other emergencies.

There are many resources, technical standards, and recommended practices available to the marine industry that can help their governance of cyber risks. Facility operators should use those resources to promote a culture of effective and proactive cyber risk management. The purpose of this draft NVIC is to begin to lay out a series of policies and procedures to mitigate these risks while ensuring the continued operational capability of the nation's MTS.

The provisions of the Maritime Transportation Security Act (MTSA) (Pub. L. 105-297, November 25, 2002) address the security of the MTS and authorize regulations. Under the authority of MTSA, the Coast Guard has promulgated regulations, located in subchapter H of Title 33 of the Code of Federal Regulations (CFR), which provide general parameters for port and facility security while allowing facility owners and operators the discretion to determine the details of how they will comply. Owners and operators are responsible for assessing vulnerabilities and ensuring the security of their facilities with Coast Guard oversight and guidance. The Coast Guard currently has the regulatory authority to instruct facilities and Outer Continental Shelf (OCS) facilities regulated under MTSA to address computer system and network vulnerabilities within their required Facility Security Assessment (FSA) and to address these vulnerabilities, if necessary, within the Facility Security Plan (FSP).

This draft NVIC would provide guidance and recommended practices for MTSA regulated facilities to address cyber-related vulnerabilities. It consists of two major parts. The first part, titled "Cyber Security and MTSA: 33 CFR

parts 105 and 106," and labeled enclosure 1, discusses the existing MTSA regulatory requirements that are applicable to cyber security related threats. These provisions, located in parts 105 and 106 of 33 CFR, currently require that owners and operators of MTSA-regulated facilities and OCS facilities conduct FSAs, and if applicable, include in their FSPs measures addressing any vulnerabilities identified in the FSA. The NVIC would lay out the Coast Guard's interpretation of these existing requirements as they would apply to cybersecurity threats and recommended additions to the FSP. As these regulations are currently in force, the recommendations of the NVIC, if finalized, would serve as the Coast Guard's interpretation of those regulations. The NVIC would assist the owner/operator in identifying cyber systems that are related to MTSA regulatory functions, or whose failure or exploitation could cause or contribute to a Transportation Security Incident.

This NVIC also contains a more detailed set of cybersecurity parameters, labeled as enclosure 2 and titled "Cyber Governance and Cyber Risk Management Program Implementation Guidance," which provides best recommended practices. This proposed guidance, derived from a variety of standardized industry practices including the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), lays out the basics for establishing a set of security policies designed to counter cybersecurity threats. These policies involve the establishment of roles and responsibilities for a Cyber Risk Management team, policies, and program, as well as guidance on how to implement such a program over a variety of business models. It also provides recommendations for developing security measures including inventory, access control, acceptable use policies, and network design. The recommendations in enclosure 2 of this proposed NVIC would provide the foundation for an effective strategy to help prevent and mitigate the damage from cybersecurity threats to the MTS.

With the publication of this draft NVIC, the Coast Guard is seeking industry and public comments on the necessity, robustness, implementation, and costs of the proposed cybersecurity guidance. Specifically, we are seeking comments on the feasibility of its implementation, how flexible and useful it is in addressing the broad scope of vulnerabilities and risk facing regulated facilities, and its ability to remain valid when technology and industry's use of technology changes. In

addition, we seek comments on whether this guidance aligns with activities that may already be taking place by industry. The Coast Guard will carefully consider all comments submitted during the comment period before promulgating any final guidance. This notice is issued under authority of 5 U.S.C. 522(a).

R.D. Manning,

Captain, U.S. Coast Guard, Chief, Office of Port and Facility Compliance.

[FR Doc. 2017-14616 Filed 7-11-17; 8:45 am]

BILLING CODE 9110-04-P

DEPARTMENT OF HOMELAND SECURITY

U.S. Customs and Border Protection

Quarterly IRS Interest Rates Used in Calculating Interest on Overdue Accounts and Refunds on Customs Duties

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

ACTION: General notice.

SUMMARY: This notice advises the public that the quarterly Internal Revenue Service interest rates used to calculate interest on overdue accounts (underpayments) and refunds (overpayments) of customs duties will remain the same from the previous

quarter. For the calendar quarter beginning July 1, 2017, the interest rates for overpayments will be 3 percent for corporations and 4 percent for non-corporations, and the interest rate for underpayments will be 4 percent for both corporations and non-corporations. This notice is published for the convenience of the importing public and U.S. Customs and Border Protection personnel.

DATES: *Effective Date:* July 1, 2017.

FOR FURTHER INFORMATION CONTACT:

Shandy Plicka, Revenue Division, Collection and Refunds Branch, 6650 Telecom Drive, Suite #100, Indianapolis, Indiana 46278; telephone (317) 298-1717.

SUPPLEMENTARY INFORMATION:

Background

Pursuant to 19 U.S.C. 1505 and Treasury Decision 85-93, published in the **Federal Register** on May 29, 1985 (50 FR 21832), the interest rate paid on applicable overpayments or underpayments of customs duties must be in accordance with the Internal Revenue Code rate established under 26 U.S.C. 6621 and 6622. Section 6621 provides different interest rates applicable to overpayments: One for corporations and one for non-corporations.

The interest rates are based on the Federal short-term rate and determined

by the Internal Revenue Service (IRS) on behalf of the Secretary of the Treasury on a quarterly basis. The rates effective for a quarter are determined during the first-month period of the previous quarter.

In Revenue Ruling 2017-13, the IRS determined the rates of interest for the calendar quarter beginning July 1, 2017, and ending on September 30, 2017. The interest rate paid to the Treasury for underpayments will be the Federal short-term rate (1%) plus three percentage points (3%) for a total of four percent (4%) for both corporations and non-corporations. For corporate overpayments, the rate is the Federal short-term rate (1%) plus two percentage points (2%) for a total of three percent (3%). For overpayments made by non-corporations, the rate is the Federal short-term rate (1%) plus three percentage points (3%) for a total of four percent (4%). These interest rates are subject to change for the calendar quarter beginning October 1, 2017, and ending December 31, 2017.

For the convenience of the importing public and U.S. Customs and Border Protection personnel the following list of IRS interest rates used, covering the period from July of 1974 to date, to calculate interest on overdue accounts and refunds of customs duties, is published in summary format.

Beginning date	Ending date	Under-payments (percent)	Over-payments (percent)	Corporate over-payments (Eff. 1-1-99) (percent)
070174	063075	6	6	
070175	013176	9	9	
020176	013178	7	7	
020178	013180	6	6	
020180	013182	12	12	
020182	123182	20	20	
010183	063083	16	16	
070183	123184	11	11	
010185	063085	13	13	
070185	123185	11	11	
010186	063086	10	10	
070186	123186	9	9	
010187	093087	9	8	
100187	123187	10	9	
010188	033188	11	10	
040188	093088	10	9	
100188	033189	11	10	
040189	093089	12	11	
100189	033191	11	10	
040191	123191	10	9	
010192	033192	9	8	
040192	093092	8	7	
100192	063094	7	6	
070194	093094	8	7	
100194	033195	9	8	
040195	063095	10	9	
070195	033196	9	8	
040196	063096	8	7	
070196	033198	9	8	
040198	123198	8	7	