onto the NIH campus. All visitor vehicles, including taxis, hotel, and airport shuttles, will be inspected before being allowed on campus. Visitors will be asked to show one form of identification (for example, a government-issued photo ID, driver's license, or passport) and to state the purpose of their visit.

In order to facilitate public attendance at the open session of Council in the main meeting room, Conference Room 6, please contact Ms. Lisa Kaeser, Program and Public Liaison Office, NICHD, at 301–496–0536 to make your reservation, additional seating will be available in the meeting overflow rooms, Conference Rooms 7 and 8. Individuals will also be able to view the meeting via NIH Videocast. Please go to the following link for Videocast access instructions at: *http://www.nichd.nih.gov/about/advisory/nachhd/Pages/virtual-meeting.aspx.*

(Catalogue of Federal Domestic Assistance Program Nos. 93.864, Population Research; 93.865, Research for Mothers and Children; 93.929, Center for Medical Rehabilitation Research; 93.209, Contraception and Infertility Loan Repayment program, National Institutes of Health, HHS)

Dated: December 12, 2014.

Michelle Trout,

Program Analyst, Office of Federal Advisory Committee Policy.

[FR Doc. 2014–29570 Filed 12–17–14; 8:45 am]

BILLING CODE 4140–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

Office of the Director, National Institutes of Health; Notice of Meeting

Pursuant to section 10(a) of the Federal Advisory Committee Act, as amended (5 U.S.C. App.), notice is hereby given of a meeting of the Advisory Committee to the Deputy Director for Intramural Research, National Institutes of Health.

The meeting will be open to the public, with attendance limited to space available. Individuals who plan to attend and need special assistance, such as sign language interpretation or other reasonable accommodations, should notify the Contact Person listed below in advance of the meeting.

Name of Committee: Advisory Committee to the Deputy Director for Intramural Research, National Institutes of Health.

Date: January 9, 2015.

Time: 1:30 p.m. to 3:00 p.m.

Agenda: To discuss the Advisory Committee to the Deputy Director for Intramural Research Report recommendations on the site visit review of the Office of Animal Care and Use.

Place: National Institutes of Health, Building 1, Room 160, Tele: 866–556–1098, Code 48960, 8600 Rockville Pike, Bethesda, MD 20892, (Telephone Conference Call).

Contact Person: Michael M. Gottesman, Deputy Director, National Institutes of Health, Building One, Room 160, Bethesda, MD 20892, 301–496–1921.

Any interested person may file written comments with the committee by forwarding the statement to the Contact Person listed on this notice. The statement should include the name, address, telephone number and when applicable, the business or professional affiliation of the interested person.

(Catalogue of Federal Domestic Assistance Program Nos. 93.14, Intramural Research Training Award; 93.22, Clinical Research Loan Repayment Program for Individuals from Disadvantaged Backgrounds; 93.232, Loan Repayment Program for Research Generally; 93.39, Academic Research Enhancement Award; 93.936, NIH Acquired Immunodeficiency Syndrome Research Loan Repayment Program; 93.187, Undergraduate Scholarship Program for Individuals from Disadvantaged Backgrounds, National Institutes of Health, HHS)

Dated: December 12, 2014.

Anna Snouffer,

Deputy Director, Office of Federal Advisory Committee Policy.

[FR Doc. 2014–29573 Filed 12–17–14; 8:45 am]

BILLING CODE 4140–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

Prospective Grant of Exclusive License: Multivalent Vaccines for Rabies Virus and Ebola and Marburg (Filoviruses)

AGENCY: National Institutes of Health, HHS.

ACTION: Notice.

SUMMARY: This is notice, in accordance with 35 U.S.C. 209 and 37 CFR 404, that the National Institutes of Health (NIH), Department of Health and Human Services (HHS), is contemplating the grant of a an exclusive license to practice the following invention as embodied in the following patent applications: E–032–2011/0, Blaney et al., ''Multivalent Vaccines for Rabies Virus and Filoviruses'', U.S. Patent Application Number 61/439,046, filed on February 3, 2011, PCT Application Number PCT/US2012/23575, filed on February 2, 2012, U.S. Patent Application Number 13/983,545, filed on August 2, 2013, European Patent Application Number 12702953.6, filed on February 2, 2012, and Canadian Patent Application Number 2826594, filed on February 2, 2012, to Exxell BIO, Inc., having a place of business in Shoreview, Minnesota, United States of America. The patent rights in these inventions have been assigned to the United States of America and Thomas Jefferson University.

DATES: Only written comments and/or application for a license which are received by the NIH Office of Technology Transfer on or before January 20, 2015 will be considered.

ADDRESSES: Requests for a copy of the patent application, inquiries, comments and other materials relating to the contemplated license should be directed to: Peter Soukas, Office of Technology Transfer, National Institutes of Health, 6011 Executive Boulevard, Suite 325, Rockville, MD 20852–3804; Email: *ps193c@nih.gov;* Telephone: (301) 435–4646; Facsimile: (301) 402–0220.

SUPPLEMENTARY INFORMATION: The inventors have developed a new platform based on live or chemically inactivated (killed) rabies virus (RABV) virions containing EBOV glycoprotein (GP) in their envelope. In preclinical trials, immunization with such recombinant RABV virions provided excellent protection in mice against lethal challenge with the mouse adapted EBOV and RABV. More specifically, the inventors have developed a trivalent filovirus vaccine based on killed rabies virus virions for use in humans to confer protection from all medically relevant filoviruses and RABV. Two additional vectors containing EBOV Sudan GP or MARV GP are planned to be constructed in addition to the previously developed EBOV Zaire GP containing vaccine. Live attenuated vaccines have been developed for use in at risk nonhuman primate populations in Africa and inactivated vaccines have been developed for use in humans. One recent use contemplated by the inventors is use of the vaccine candidates to generate polyclonal sera against Filoviruses (*i.e.* Ebola and Marburg).

The prospective exclusive license will be royalty bearing and will comply with the terms and conditions of 35 U.S.C. 209 and 37 CFR 404. The prospective exclusive license may be granted unless, within thirty (30) days from the date of this published notice, NIH receives written evidence and argument that establishes that the grant of the license would not be consistent with the requirements of 35 U.S.C. 209 and 37 CFR 404.

These patent rights are the subject of a previous **Federal Register** notice (see 79 FR 18039, Monday, March 31, 2014).

The fields of use may be limited to production of polyclonal antibodies for prevention/treatment of Filoviruses in humans and non-human animals.

Properly filed competing applications for a license filed in response to this notice will be treated as objections to the contemplated license. Comments and objections submitted in response to this notice will not be made available for public inspection, and, to the extent permitted by law, will not be released under the Freedom of Information Act, 5 U.S.C. 552.

Dated: December 11, 2014.

Richard U. Rodriguez,

Acting Director, Office of Technology Transfer, National Institutes of Health.

[FR Doc. 2014–29572 Filed 12–17–14; 8:45 am]

BILLING CODE 4140–01–P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[Docket No. USCG–2014–1020]

Guidance on Maritime Cybersecurity Standards

AGENCY: Coast Guard, DHS.

ACTION: Notice with request for comments.

SUMMARY: The Coast Guard is developing policy to help vessel and facility operators identify and address cyber-related vulnerabilities that could contribute to a Transportation Security Incident. Coast Guard regulations require certain vessel and facility operators to conduct security assessments, and to develop security plans that address vulnerabilities identified by the security assessment. The Coast Guard is seeking public input from the maritime industry and other interested parties on how to identify and mitigate potential vulnerabilities to cyber-dependent systems. The Coast Guard will consider these public comments in developing relevant guidance, which may include standards, guidelines, and best practices to protect maritime critical infrastructure.

DATES: Comments must be submitted to the online docket via *http://www.regulations.gov,* or reach the Docket Management Facility, on or before February 17, 2015.

ADDRESSES: Submit comments using one of the listed methods, and see **SUPPLEMENTARY INFORMATION** for more information on public comments.

- Online—*http://www.regulations.gov* following Web site instructions.
- Fax—202–493–2251.
- Mail or hand deliver—Docket Management Facility (M–30), U.S. Department of Transportation, West Building Ground Floor, Room W12–140, 1200 New Jersey Avenue SE., Washington, DC 20590–0001. Hours for hand delivery are 9 a.m. to 5 p.m., Monday through Friday, except Federal holidays (telephone 202–366–9329).

FOR FURTHER INFORMATION CONTACT: For information about this document call or email LT Josephine Long, Coast Guard; telephone 202–372–1109, email *Josephine.A.Long@uscg.mil* or LCDR Joshua Rose, Coast Guard; 202–372–1106, email *Joshua.D.Rose@uscg.mil.* For information about viewing or submitting material to the docket, call Cheryl Collins, Program Manager, Docket Operations, telephone 202–366–9826, toll free 1–800–647–5527.

SUPPLEMENTARY INFORMATION:

Public Participation and Comments

We encourage you to submit comments (or related material) on the questions listed below. We will consider all submissions and may adjust our final policy actions based on your comments. Comments should be marked with docket number USCG–2014–1020, and should provide a reason for each suggestion or recommendation. You should provide personal contact information so that we can contact you if we have questions regarding your comments; but please note that all comments will be posted to the online docket without change and that any personal information you include can be searchable online (see the **Federal Register** Privacy Act notice regarding our public dockets, 73 FR 3316, Jan. 17, 2008).

Mailed or hand-delivered comments should be in an unbound 8½ x 11 inch format suitable for reproduction. The Docket Management Facility will acknowledge receipt of mailed comments if you enclose a stamped, self-addressed postcard or envelope with your submission.

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 the Web site's instructions. You can also view the docket at the Docket Management Facility (see the mailing address under **ADDRESSES**) between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

Discussion

The Coast Guard is developing policy to help vessel and facility operators identify and address cyber-related vulnerabilities that could contribute to a Transportation Security Incident (TSI).[1] Coast Guard regulations require certain vessel and facility operators to conduct security assessments, and to develop security plans that address vulnerabilities identified by the security assessment.[2] Vessel and facility security plans must also address specific security functions, including the following:

- Communications
- Security Training Requirements
- Procedures for vessel/facility interfacing
- Declaration of Security
- Security Systems and Equipment Maintenance
- Security Measures for Access Control
- Security Measures for Handling Cargo
- Security Measures for Monitoring
- Security Incident Procedures

The Coast Guard is seeking public input on the following questions:

(1) What cyber-dependent systems, commonly used in the maritime industry, could lead or contribute to a TSI if they failed, or were exploited by an adversary?

(2) What procedures or standards do vessel and facility operators now employ to identify potential cybersecurity vulnerabilities to their operations?

(3) Are there existing cybersecurity assurance programs in use by industry that the Coast Guard could recognize? If so, to what extent do these programs address vessel or facility systems that could lead to a TSI?

(4) To what extent do current security training programs for vessel and facility personnel address cybersecurity risks and best practices?

(5) What factors should determine when manual backups or other non-technical approaches are sufficient to address cybersecurity vulnerabilities?

(6) How can the Coast Guard leverage Alternative Security Programs [3] to help vessel and facility operators address cybersecurity risks?

(7) How can vessel and facility operators reliably demonstrate to the Coast Guard that critical cyber-systems meet appropriate technical or procedural standards?

(8) Do classification societies, protection and indemnity clubs, or insurers recognize cybersecurity best practices that could help the maritime industry and the Coast Guard address

[1] A *Transportation Security Incident* is defined in 33 CFR 101.105 to mean ''a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.''

[2] 33 CFR parts 104 and 105, subparts C and D.

[3] An *Alternative Security Program* is defined in 33 CFR 101.105 to mean ''a third-party or industry organization developed standard that the Commandant [of the Coast Guard] has determined provides an equivalent level of security to that established by [33 CFR Chapter I, Subchapter H].''