collection, and (4) summarizing data on urban agriculture. The intent is that the resulting methodology and procedures will be integrated into the 2017 Census of Agriculture to collect data on urban agriculture, in addition to traditional agriculture. This data collection includes surveys to be conducted in two urbanized areas: Seattle, Washington and Austin, Texas. The first survey will be conducted in Seattle. The second survey will be conducted in Austin to address methodological issues that remain after analyzing results from the Baltimore and Seattle projects. All results from these surveys will be used for internal purposes only; no publications will be generated. These surveys will be voluntary.

**Authority:** The data will be collected under the authority of 7 U.S.C. 2204(a). Individually identifiable data collected under this authority are governed by Section 1770 of the Food Security Act of 1985 as amended, 7 U.S.C. 2276, which requires USDA to afford strict confidentiality to non-aggregated data provided by respondents. This Notice is submitted in accordance with the Paperwork Reduction Act of 1995, Public Law 104–13 (44 U.S.C. 3501, *et seq.*), and Office of Management and Budget regulations at 5 CFR part 1320.

NASS also complies with OMB Implementation Guidance, ''Implementation Guidance for Title V of the E-Government Act, Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA),'' **Federal Register**, Vol. 72, No. 115, June 15, 2007, p. 33362.

*Estimate of Burden:* This collection of information contains two components. The first component consists of up to 50 cognitive interviews (conducted through personal enumeration) and is intended to develop the questionnaire used to gather data on agricultural activity in urbanized areas. Public reporting burden for this component is estimated to average 60 minutes per response. The second component is a survey conducted in two urbanized areas (Seattle, WA and Austin, TX). The sample sizes for the Seattle and Austin surveys will be 390 and 545, respectively. Public reporting burden for this component is estimated to average 50 minutes per response. For this component, NASS plans to use a combination of mailed pre-survey letters, mailed questionnaires, telephone enumeration, and personal enumeration.

*Respondents:* Individuals and households.

*Estimated Number of Respondents:* 985.

*Estimated Total Annual Burden on Respondents:* 700 hours.

*Comments:* Comments are invited on: (a) Whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility; (b) the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information on those who are to respond, through the use of appropriate automated, electronic, mechanical, technological, or other forms of information technology collection methods.

All responses to this notice will become a matter of public record and be summarized in the request for OMB approval.

Signed at Washington, DC, December 1, 2015.

**R. Renee Picanso,**

*Associate Administrator.*

[FR Doc. 2015–31246 Filed 12–10–15; 8:45 am]

**BILLING CODE 3410–20–P**

## DEPARTMENT OF COMMERCE

### International Trade Administration

### Advisory Committee on Supply Chain Competitiveness: Notice of Public Meetings

**AGENCY:** International Trade Administration, U.S. Department of Commerce.

**ACTION:** Notice of open meetings.

**SUMMARY:** This notice sets forth the schedule and proposed topics of discussion for public meetings of the Advisory Committee on Supply Chain Competitiveness (Committee).

**DATES:** The meetings will be held on January 20, 2016 from 12:00 p.m. to 3:00 p.m., and January 21, 2016 from 9:00 a.m. to 4:00 p.m., Eastern Standard Time (EST).

**ADDRESSES:** The meetings on January 20 and 21 will be held at the U.S. Department of Commerce, 1401 Constitution Avenue NW., Research Library (Room 1894), Washington, DC 20230.

**FOR FURTHER INFORMATION CONTACT:** Richard Boll, Office of Supply Chain, Professional & Business Services, International Trade Administration. (Phone: (202) 482–1135 or Email: *richard.boll@trade.gov.*)

**SUPPLEMENTARY INFORMATION:**

*Background:* The Committee was established under the discretionary authority of the Secretary of Commerce and in accordance with the Federal Advisory Committee Act (5 U.S.C. App. 2). It provides advice to the Secretary of Commerce on the necessary elements of a comprehensive policy approach to supply chain competitiveness designed to support U.S. export growth and national economic competitiveness, encourage innovation, facilitate the movement of goods, and improve the competitiveness of U.S. supply chains for goods and services in the domestic and global economy; and provides advice to the Secretary on regulatory policies and programs and investment priorities that affect the competitiveness of U.S. supply chains. For more information about the Committee visit: *http://trade.gov/td/services/oscpb/supplychain/acscc/.*

*Matters To Be Considered:* Committee members are expected to continue to discuss the major competitiveness-related topics raised at the previous Committee meetings, including trade and competitiveness; freight movement and policy; information technology and data requirements; regulatory issues; finance and infrastructure; and workforce development. The Committee's subcommittees will report on the status of their work regarding these topics. The agenda's may change to accommodate Committee business. The Office of Supply Chain, Professional & Business Services will post the final detailed agenda's on its Web site, *http://trade.gov/td/services/oscpb/supplychain/acscc/,* at least one week prior to the meeting. The meetings will be open to the public and press on a first-come, first-served basis. Space is limited. The public meetings are physically accessible to people with disabilities. Individuals requiring accommodations, such as sign language interpretation or other ancillary aids, are asked to notify Mr. Richard Boll, at (202) 482–1135 or *richard.boll@trade.gov* five (5) business days before the meeting.

Interested parties are invited to submit written comments to the Committee at any time before and after the meeting. Parties wishing to submit written comments for consideration by the Committee in advance of this meeting must send them to the Office of Supply Chain, Professional & Business Services, 1401 Constitution Ave, NW., Room 11014, Washington, DC, 20230, or email to *richard.boll@trade.gov.*

For consideration during the meetings, and to ensure transmission to the Committee prior to the meetings, comments must be received no later

than 5:00 p.m. EST on January 12, 2016. Comments received after January 12, 2016, will be distributed to the Committee, but may not be considered at the meetings. The minutes of the meetings will be posted on the Committee Web site within 60 days of the meeting.

Dated: December 7, 2015.

**David Long,**

*Director, Office of Supply Chain and Professional & Business Services.*

[FR Doc. 2015–31195 Filed 12–10–15; 8:45 am]

**BILLING CODE 3510–DR–P**

## DEPARTMENT OF COMMERCE

### National Institute of Standards and Technology

**[Docket Number: 151103999–5999–01]**

### Views on the Framework for Improving Critical Infrastructure Cybersecurity

**ACTION:** Notice; Request for Information (RFI).

**SUMMARY:** The National Institute of Standards and Technology (NIST) is seeking information on the ''Framework for Improving Critical Infrastructure Cybersecurity'' (the ''Framework'').

As directed by Executive Order 13636, ''Improving Critical Infrastructure Cybersecurity'' (the ''Executive Order''), the Framework consists of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Framework was released on February 12, 2014, after a year-long open process involving private and public sector organizations, including extensive industry input and public comments. In order to fulfill its responsibilities under the Cyber Security Enhancement Act of 2014, NIST is committed to maintaining an inclusive approach, informed by the views of a wide array of individuals, organizations, and sectors.

In this RFI, NIST requests information about the variety of ways in which the Framework is being used to improve cybersecurity risk management, how best practices for using the Framework are being shared, the relative value of different parts of the Framework, the possible need for an update of the Framework, and options for the long-term governance of the Framework. This information is needed in order to carry out NIST's responsibilities under the Cybersecurity Enhancement Act of 2014 and the Executive Order.

Responses to this RFI—which will be posted at *http://www.nist.gov/cyberframework/cybersecurity-framework-rfi.cfm*—will inform NIST's planning and decision-making about how to further advance the Framework so that the Nation's critical infrastructure is more secure by enhancing its cybersecurity and risk management.

All information provided will also assist in developing the agenda for a workshop on the Framework being planned by NIST for April 6 and 7, 2016, in Gaithersburg, Maryland. Specifics about the workshop will be announced at a later date.

**DATES:** Comments must be received by 5:00 p.m. Eastern time on February 9, 2016.

**ADDRESSES:** Written comments may be submitted by mail to Diane Honeycutt, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899. Online submissions in electronic form may be sent to *cyberframework@nist.gov* in any of the following formats: HTML; ASCII; Word; RTF; or PDF. Please include your name and your organization's name (if any), and cite ''Views on the Framework for Improving Critical Infrastructure Cybersecurity'' in all correspondence. Comments containing references, studies, research, and other empirical data that are not widely published should include copies of the referenced materials. Please do not submit additional materials.

All comments received in response to this RFI will be posted at *http://www.nist.gov/cyberframework/cybersecurity-framework-rfi.cfm* without change or redaction, so commenters should not include information they do not wish to be posted (*e.g.,* personal or confidential business information).

**FOR FURTHER INFORMATION CONTACT:** For questions about this RFI contact: Diane Honeycutt, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899 or *cyberframework@nist.gov.* Please direct media inquiries to NIST's Office of Public Affairs at (301) 975–2762.

**SUPPLEMENTARY INFORMATION:** NIST is authorized by the Cybersecurity Enhancement Act of 2014 [1] to ''facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure.'' [2] In carrying out this function, NIST is directed to ''coordinate closely and regularly with relevant private sector personnel and entities, critical infrastructure owners and operators, and other relevant industry organizations.'' [3] NIST has taken this approach since February 2013 when Executive Order 13636, ''Improving Critical Infrastructure Cybersecurity'' [4] tasked the Secretary of Commerce to direct the Director of NIST to lead the development of the Framework.

NIST developed the Framework by using information collected through a Request for Information (RFI) that was published in the **Federal Register** (78 FR 13024) on February 26, 2013; a series of five open public workshops; [5] and a 45-day public comment period in response to a draft version of the Framework announced in the **Federal Register** (78 FR 64478) on October 29, 2013. A final version of Framework 1.0 was published on February 12, 2014, after a year-long, open process involving private and public sector organizations, including extensive industry input and public comments, and announced in the **Federal Register** (79 FR 9167) on February 18, 2014. NIST subsequently solicited information on Framework users' experiences through an RFI published in the **Federal Register** (79 FR 50891) on August 26, 2014 as well as another workshop held on October 29 and 30, 2014, at the University of South Florida.

In addition to extensive outreach and providing responses to inquiries, NIST has made information about the Cybersecurity Framework available on its Web site at *http://www.nist.gov/cyberframework/* to assist organizations in learning more about using the Framework. This includes an Industry Resources page (available at *http://www.nist.gov/cyberframework/cybersecurity-framework-industry-resources.cfm*), listing publicly available materials developed by organizations other than NIST that support use of the Framework. NIST does not necessarily

---

[1] Public Law 113–274 (2014): *http://www.gpo.gov/fdsys/pkg/PLAW-113publ274/pdf/PLAW-113publ274.pdf.*

[2] *Id.,* codified in relevant part at 15 U.S.C. 272(c)(15). Congress's intent was to codify NIST's role in Executive Order No. 13636: ''Title I would codify certain elements of Executive Order 13636 by directing the National Institute of Standards and Technology (NIST) to develop a framework of voluntary standards designed to reduce risks arising from cyberattacks on critical infrastructure that is privately owned and operated.'' S. Rep. No. 113–270, at 9 (2014).

[3] *Id.,* codified in relevant part at 15 U.S.C. 272(e)(A)(i).

[4] Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity, 78 FR 11739 (Feb. 19, 2013).

[5] NIST, Gaithersburg April 3, 2013; Carnegie Mellon University May 29–31, 2013; University of California San Diego July 10–12, 2013; University of Texas Dallas September 11–13, 2013; North Carolina State November 14–15, 2013.