advance notice prior to implementation of the inspection program.'' [2]

Scope of Agreement

See Section I, Product Coverage, of the 2019 Suspension Agreement.

Notification

Consistent with the 2019 Suspension Agreement, this **Federal Register** notice provides 60 days' advance notice prior to the implementation of the inspection program, which has been developed by USDA, in consultation with Commerce, as specified in the 2019 Suspension Agreement. The inspection program, as outlined in Section VII.C of the 2019 Suspension Agreement, will begin 60 days from the date of publication of this notice. Beginning 60 days from the date of publication of this notice, all Fresh Tomatoes from Mexico, with the exception of Tomatoes on the Vine, Specialty tomatoes, and grape tomatoes in retail packages of 2 pounds or less, shall be subject to a USDA inspection for quality and condition defects consistent with Section VII.C of the 2019 Suspension Agreement, and in accordance with USDA procedures as determined by USDA.[3] (*See* Section II of the 2019 Suspension Agreement for definitions of certain terms in the preceding sentence.)

As provided in the 2019 Suspension Agreement, importers of tomatoes subject to inspection must request the USDA inspection and pay the associated USDA fees.[4] USDA will perform inspections (an unrestricted certification) in accordance with its normal practice to determine quality, condition, and grade pursuant to the appropriate USDA standard covering fresh tomatoes and greenhouse tomatoes and using shipping point tolerances.[5] After the USDA inspection, the importer will receive an inspection certificate, which must be maintained by the importer and is subject to submission to, and verification by, Commerce, consistent with the importer's contractual obligation with the Signatory.[6] If a lot of Signatory tomatoes has more defects than the tolerances established in the USDA standards, then the importer may opt either to recondition and re-inspect the lot, or return it to Mexico, consistent with the requirements of the 2019 Suspension Agreement.[7]

Dated: January 30, 2020.

Jeffrey I. Kessler,

Assistant Secretary for Enforcement and Compliance.

[FR Doc. 2020–02166 Filed 2–3–20; 8:45 am]

BILLING CODE 3510–DS–P

[2] *See* Section VII.C.1 of the 2019 Suspension Agreement.

[3] For avoidance of doubt, all loads of Fresh Tomatoes from Mexico that are inspected pursuant to a USDA marketing order are not required to also be inspected pursuant to the inspection program under this section VII.C. *See id.*

[4] *See* Section VII.C.2 of the 2019 Suspension Agreement.

[5] *See* Section VII.C.3 of the 2019 Suspension Agreement.

[6] *See* Section VII.C.4 of the 2019 Suspension Agreement.

[7] *See id.*

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 200113–0015]

National Cybersecurity Center of Excellence (NCCoE) Data Confidentiality Building Block

AGENCY: National Institute of Standards and Technology, Department of Commerce.

ACTION: Notice.

SUMMARY: The National Institute of Standards and Technology (NIST) invites organizations to provide products and technical expertise to support and demonstrate security platforms for two data confidentiality projects within the Data Confidentiality Building Block. The two projects are Data Confidentiality: Identifying and Protecting Assets and Data Against Data Breaches and Data Confidentiality: Detect, Respond to, and Recover from Data Breaches. This notice is the initial step for the National Cybersecurity Center of Excellence (NCCoE) in collaborating with technology companies to address cybersecurity challenges identified under the Data Confidentiality Building Block. Participation in the building block is open to all interested organizations and organizations may participate in one or both data Confidentiality projects.

DATES: Interested parties must contact NIST to request a letter of interest template to be completed and submitted to NIST. Letters of interest will be accepted on a first come, first served basis. Parties interested in participating in both data confidentiality projects must submit a separate letter of interest for each data confidentiality project. Collaborative activities will commence as soon as enough completed and signed letters of interest have been returned to address all the necessary components and capabilities, but no earlier than March 5, 2020. When the building block has been completed, NIST will post a notice announcing the completion of the building block and informing the public that it will no longer accept letters of interest for this building block on the NCCoE Data Confidentiality Building Block website at *https://www.nccoe.nist.gov/projects/building-blocks/data-security/dc-detect-identify-protect_forDataConfidentiality:* Identifying and Protecting Assets and Data Against Data Breaches, and at *https://www.nccoe.nist.gov/projects/building-blocks/data-security/dc-detect-respond-recoverfor_DataConfidentiality:* Detect, Respond to and Recover from Data Breaches.

ADDRESSES: The NCCoE is located at 9700 Great Seneca Highway, Rockville, MD 20850. Letters of interest must be submitted to *ds-nccoe@nist.gov* or via hardcopy to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Organizations whose letters of interest are accepted in accordance with the process set forth in the **SUPPLEMENTARY INFORMATION** section of this notice will be asked to sign a separate consortium Cooperative Research and Development Agreement (CRADA) with NIST for each Data Confidentiality Building Block project. An NCCoE consortium CRADA template can be found at: *http://nccoe.nist.gov/node/138.*

FOR FURTHER INFORMATION CONTACT: Jennifer Cawthra via email to *Jennifer.Cawthra@nist.gov;* by telephone 240.328.4584; or by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the Data Confidentiality Building Block are available at *https://www.nccoe.nist.gov/projects/building-blocks/data-security.*

SUPPLEMENTARY INFORMATION:

Background: The NCCoE, part of NIST, is a public-private collaboration for accelerating the widespread adoption of integrated cybersecurity tools and technologies. The NCCoE brings together experts from industry, government, and academia under one roof to develop practical, interoperable cybersecurity approaches that address the real-world needs of complex Information Technology (IT) systems. By accelerating dissemination and use of these integrated tools and technologies for protecting IT assets, the NCCoE will enhance trust in U.S. IT communications, data, and storage systems; reduce risk for companies and individuals using IT systems; and encourage development of innovative, job-creating cybersecurity products and services.

Process: NIST is soliciting responses from all sources of relevant security capabilities (see below) to enter into a Cooperative Research and Development Agreement (CRADA) to provide products and technical expertise to support and demonstrate security platforms for the Data Confidentiality Building Block. The full building block can be viewed at: *https://www.nccoe.nist.gov/projects/building-blocks/data-security.*

Interested parties should contact NIST using the information provided in the **FOR FURTHER INFORMATION CONTACT** section of this notice. NIST will then provide each interested party with a letter of interest template, which the party must complete, certify that it is accurate, and submit to NIST. NIST will contact interested parties if there are questions regarding the responsiveness of the letters of interest to the building block objective or requirements identified below. NIST will select participants who have submitted complete letters of interest on a first come, first served basis within each category of product components or capabilities listed below up to the number of participants in each category necessary to carry out this building block. However, there may be continuing opportunity to participate even after initial activity commences. Selected participants will be required to enter into a consortium CRADA with NIST (for reference, see **ADDRESSES** section above). NIST published a notice in the **Federal Register** on October 19, 2012 (77 FR 64314) inviting U.S. companies to enter into National Cybersecurity Excellence Partnerships (NCEPs) in furtherance of the NCCoE. For this demonstration project, NCEP partners will not be given priority for participation.

Building Block Objective: Establish tools and procedures to defend, detect, and respond to data confidentiality events.

A detailed description of the Data Confidentiality Building Block is available at: *https://www.nccoe.nist.gov/projects/building-blocks/data-security.*

Requirements: Each responding organization's letter of interest should identify which security platform component(s) or capability(ies) it is offering. Responding organizations must submit a separate letter of interest and sign a separate consortium CRADA for each project the responding organization is interested in joining. Letters of interest should not include company proprietary information, and all components and capabilities must be commercially available. Components are listed in section 3 of each of the data confidentiality projects (1) Data Confidentiality: Identifying and Protecting Assets and Data Against Data Breaches, and (2) Data Confidentiality: Detect, and Respond to, and Recover from Data Breaches. (for reference, please see the link in the PROCESS section above) and include, but are not limited to:

- For Data Confidentiality: Identifying and Protecting Assets and Data Against Data Breaches:
- Log collection, collation, and correlation
- Network protection solution
- Network mapping
- Network segmentation
- Network protection
- Browser isolation
- User access controls
- Data management
- Data discovery
- Data inventory
- Data protection
- Protection at rest
* Including file- and system-level encryption
- Protection in transit
- Protection in use
- Protection against the use of removable media
- Policy enforcement
- For Data Confidentiality: Detect, and Respond to and Recover from Data Breaches:
- Monitoring
- File
- Network
- Users
- Event detection
- Exfiltration activity
- Unauthorized activity
- Anomalous activity
- Log collection, collation, and correlation of all activities within the enterprise
- Reporting capability
- Capability to mitigate data loss

Each responding organization's letter of interest should identify how their products address one or more of the following desired solution characteristics in section 3 of each of the Data Confidentiality projects (1) Data Confidentiality: Identifying and Protecting Assets and Data Against Data Breaches, and (2) Data Confidentiality: Detect, Respond to, and Recover from Data Breaches (for reference, please see the link in the PROCESS section above):

1. For Data Confidentiality: Identifying and Protecting Assets and Data Against Data Breaches:

- Identify and inventory data and data flows.
- Protect against confidentiality attacks on hosts.
- Protect against confidentiality attacks that occur on the network.
- Protect against confidentiality attacks that occur on enterprise components.
- Protect enterprise data at rest, in transit, and in use.
- Protect the network and remote access capabilities.
- Provide logging and audit capabilities.
- Provide user access controls to data.
- Provide user authentication mechanisms.

2. For Data Confidentiality: Detect, Respond to, and Recover from Data Breaches:

- Monitor the enterprise's user and data activity.
- Detect unauthorized data flows, user behavior, and data access.
- Report unauthorized activity with respect to users and data in transit, at rest, or in use to centralized monitoring and reporting software.
- Analyze the impact of unauthorized behavior and malicious behavior on the network or end points. Determine if a loss of data confidentiality is occurring or has occurred.
- Mitigate the impact of such losses of data confidentiality by facilitating an effective response to a data breach scenario.
- Contain the effects of a data breach so that more data is not exposed.
- Facilitate the recovery effort from data breaches by providing detailed information as to the scope and severity of the breach.

Responding organizations need to understand and, in their letters of interest, commit to provide:

1. Access for all participants' project teams to component interfaces and the organization's experts necessary to make functional connections among security platform components

2. Support for development and demonstration of the Data Confidentiality Building Block in NCCoE facilities which will be conducted in a manner consistent with the following standards and guidance: FIPS 200, FIPS 201, SP 800–53, FIPS 140–2, SP 800–37, SP 800–57, SP 800–61, SP 800–83, SP 800–150, SP 800–160, and SP 800–184.

Additional details about the Data Confidentiality Building Block are available at: *https://nccoe.nist.gov/projects/building-blocks/data-security.*

NIST cannot guarantee that all of the products proposed by respondents will be used in the demonstration. Each prospective participant will be expected to work collaboratively with NIST staff and other project participants under the terms of the consortium CRADA in the development of the Data Confidentiality Building Block. Prospective

participants' contribution to the collaborative effort will include assistance in establishing the necessary interface functionality, connection and set-up capabilities and procedures, demonstration harnesses, environmental and safety conditions for use, integrated platform user instructions, and demonstration plans and scripts necessary to demonstrate the desired capabilities. Each participant will train NIST personnel, as necessary, to operate its product in capability demonstrations. Following successful demonstrations, NIST will publish a description of the security platform and its performance characteristics sufficient to permit other organizations to develop and deploy security platforms that meet the security objectives of the Data Confidentiality Building Block. These descriptions will be public information.

Under the terms of the consortium CRADA, NIST will support development of interfaces among participants' products by providing IT infrastructure, laboratory facilities, office facilities, collaboration facilities, and staff support to component composition, security platform documentation, and demonstration activities.

The dates of the demonstration of the Data Confidentiality Building Block capability will be announced on the NCCoE website at least two weeks in advance at *http://nccoe.nist.gov/.* The expected outcome of the demonstration is to improve data integrity within the enterprise. Participating organizations will gain from the knowledge that their products are interoperable with other participants' offerings.

For additional information on the NCCoE governance, business processes, and NCCoE operational structure, visit the NCCoE website *http://nccoe.nist.gov/.*

Kevin A. Kimball,

Chief of Staff.

[FR Doc. 2020–01993 Filed 2–3–20; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[RTID 0648–XR094]

Marine Mammals; Issuance of Permits

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice; issuance of permits.

SUMMARY: Notice is hereby given that individuals and institutions have been issued Letters of Confirmation for activities conducted under the General Authorization for Scientific Research on marine mammals. See **SUPPLEMENTARY INFORMATION** for a list of names and address of recipients.

ADDRESSES: The Letters of Confirmation and related documents are available for review upon written request or by appointment in the following office:

Permits and Conservation Division, Office of Protected Resources, NMFS, 1315 East-West Highway, Room 13705, Silver Spring, MD 20910; phone (301) 427–8401; fax (301) 713–0376.

FOR FURTHER INFORMATION CONTACT: Office of Protected Resources, Permits and Conservation Division, (301) 427–8401.

SUPPLEMENTARY INFORMATION: The requested Letters of Confirmation have been issued under the authority of the Marine Mammal Protection Act of 1972, as amended (16 U.S.C. 1361 *et seq.*), and the regulations governing the taking and importing of marine mammals (50 CFR part 216). The General Authorization allows for *bona fide* scientific research that may result only in taking by Level B harassment of marine mammals. The following Letters of Confirmation (LOC) were issued in Fiscal Year 2019 (October 1, 2018–September 30, 2019).

File No. 21910: Issued to California Wildlife Center (Principal Investigator: Jennifer Brent), 26026 Pimma Road, Calabassas, CA 91302, on October 1, 2018, to obtain baseline data on marine mammal health and populations in remote areas of Malibu to better aid future studies on ocean stock health and to identify previously unreported cases of human interaction and previously tagged animal migration. This work specifically targets the U.S. stock of California sea lion (*Zalophus californianus*), the California breeding stock of northern elephant seal (*Mirounga angustirostris*), and the California stock of harbor seal (*Phoca vitulina*). The LOC expires on September 30, 2023.

File No. 19826–03: Issued to Deanna Rees, Naval Undersea Warfare Center, Division Newport, 1176 Howell Street, Newport, RI 02841, on November 1, 2018, to conduct surveys of gray (*Halichoerus grypus atlantica*) (Western North Atlantic stock), harbor (Western North Atlantic stock), and harp (*Pagophilus groenlandicus*) (Western North Atlantic stock) seals in the northeast. The amended LOC adds aerial surveys of pinnipeds via vertical take-off and landing unmanned aircraft systems (UAS). The LOC expires on January 31, 2021.

File No. 22198–01: Issued to Samuel Wasser, Ph.D., Center for Conservation Biology, University of Washington, Seattle, WA 98195, on November 21, 2018, extended the expiration date of the LOC for one year. Research activities include vessel surveys targeting killer whales (*Orcinus orca,* West Coast Transient stock) within the inland waters of Washington State. The objectives do not change from those previously authorized under LOC No. 22198. The amended LOC clarifies the expiration date relative to the effective date of new Permit No. 22141 (84 FR 22111, May 16, 2019); the LOC subsequently expired on April 30, 2019.

File No. 18218–03: Issued to Dolphin Research Center, (Principal Investigator: Armando Rodriguez), 58763 Overseas Highway, Grassy Key, FL 33050, on November 29, 2018, extended the expiration date of the LOC for one year. The research includes close approach, photo-identification, behavioral observations, passive acoustics, and focal follows of coastal and bottlenose dolphins (*Tursiops truncatus*) (Florida Bay Stock) in coastal waters of the middle Florida Keys. The objectives do not change from those previously authorized under LOC No.18218–02. The LOC was subsequently terminated on February 5, 2019, when a new LOC (No. 22587, see below) was issued to Dolphin Research Center.

File No. 22081: Issued to Institute for Marine Mammal Studies (Principal Investigator: Mobashir Solangi, Ph.D.), P.O. Box 207, Gulfport, MS 39502, on December 3, 2018, to study cetaceans during vessel and aerial surveys using photo-identification, behavioral observations, photography, filming, and passive acoustic recordings. Research may occur from Lake Borgne, Louisiana to the Alabama/Mississippi state line, including Mississippi, Chandeleur, and Breton Sounds and adjacent waters. The target species is bottlenose dolphins; however research would also occur if any of the following species were observed: Atlantic spotted dolphin (*Stenella frontalis*), pantropical spotted dolphin (*S. attenuata*), spinner dolphin (*S. longirostris*), and pygmy sperm whale (*Kogia breviceps*). The LOC expires on December 1, 2023.

File No. 22587: Issued to Dolphin Research Center (Principal Investigator: Armando Rodriguez), 58763 Overseas Highway, Grassy Key, FL 33050, on February 5, 2019 to continue vessel surveys for close approach, photo-identification, behavioral observations, passive acoustics, and focal follows of