Description of Certified Content

NFE's Certificate was amended as follows:

1. Added the following company as a new Member of the Certificate within the meaning of section 325.2(l) of the Regulations (15 CFR 325.2(l)) for the following Export Product: Fresh sweet cherries:

- Griggs Farms Packing, LLC, Orondo, WA

2. Deleted the following companies as Members of the Certificate:

- Peshastin Hi-Up Growers, Peshastin, WA
- Strand Apples, Inc., Cowiche, WA

3. Changed the Export Product coverage for one Member:

- Stemilt Growers, LLC changed Export Product coverage from fresh sweet cherries, fresh apples, and fresh pears to fresh sweet cherries and fresh apples (dropping fresh pears).

4. Modified the Certificate language under Paragraph 2 of the Export Trade Activities and Methods of Operation to read as follows:

''With respect to fresh sweet cherries only, NFE may on behalf of and with the advice of its Members negotiate export prices and quantities and allocate export quotas among growing regions and its Members, in connection with actual or potential bona fide export opportunities. In allocating export quotas among growing regions and its Members, NFE, through employees or agents of NFE who are not also employees of a Member, may receive, and each Member may supply to such employees or agents of NFE, information as to such Member's actual total export shipments of fresh sweet cherries in any previous growing season or seasons, provided that such information is not disclosed by NFE to any other Member. All communications made on behalf of NFE to its Members relating to the allocation of quotas shall be made by an NFE employee or agent who is not also an employee of a Member, and neither the NFE employee/agent or any employee of a Member shall disclose to any other Member the quota allocation of that Member or any other Member.''

NFE's Amended Certificate Membership Is as Follows

1. Allan Bros., Naches, WA
2. AltaFresh L.L.C. dba Chelan Fresh Marketing, Chelan, WA
3. Apple House Warehouse & Storage, Inc., Brewster, WA
4. Apple King, L.L.C., Yakima, WA
5. Auvil Fruit Co., Inc., Orondo, WA
6. Baker Produce, Inc., Kennewick, WA
7. Blue Bird, Inc., Peshastin, WA
8. Blue Star Growers, Inc., Cashmere, WA
9. Borton & Sons, Inc., Yakima, WA
10. Brewster Heights Packing & Orchards, LP, Brewster, WA
11. Chelan Fruit Cooperative, Chelan, WA
12. Chiawana, Inc. dba Columbia Reach Pack, Yakima, WA
13. CMI Orchards LLC, Wenatchee, WA
14. Columbia Fruit Packers, Inc., Wenatchee, WA
15. Columbia Valley Fruit, L.L.C., Yakima, WA
16. Congdon Packing Co. L.L.C., Yakima, WA
17. Conrad & Adams Fruit L.L.C., Grandview, WA
18. Cowiche Growers, Inc., Cowiche, WA
19. CPC International Apple Company, Tieton, WA
20. Crane & Crane, Inc., Brewster, WA
21. Custom Apple Packers, Inc., Quincy, and Wenatchee, WA
22. Diamond Fruit Growers, Inc., Odell, OR
23. Domex Superfresh Growers LLC, Yakima, WA
24. Douglas Fruit Company, Inc., Pasco, WA
25. Dovex Export Company, Wenatchee, WA
26. Duckwall Fruit, Odell, OR
27. E. Brown & Sons, Inc., Milton-Freewater, OR
28. Evans Fruit Co., Inc., Yakima, WA
29. E.W. Brandt & Sons, Inc., Parker, WA
30. FirstFruits Farms, LLC, Prescott, WA
31. Frosty Packing Co., LLC, Yakima, WA
32. G&G Orchards, Inc., Yakima, WA
33. Gilbert Orchards, Inc., Yakima, WA
34. Griggs Farms Packing, LLC, Orondo, WA
35. Hansen Fruit & Cold Storage Co., Inc., Yakima, WA
36. Henggeler Packing Co., Inc., Fruitland, ID
37. Highland Fruit Growers, Inc., Yakima, WA
38. HoneyBear Growers LLC, Brewster, WA
39. Honey Bear Tree Fruit Co LLC, Wenatchee, WA
40. Hood River Cherry Company, Hood River, OR
41. JackAss Mt. Ranch, Pasco, WA
42. Jenks Bros Cold Storage & Packing, Royal City, WA
43. Kershaw Fruit & Cold Storage, Co., Yakima, WA
44. L & M Companies, Union Gap, WA
45. Legacy Fruit Packers LLC, Wapato, WA
46. Manson Growers Cooperative, Manson, WA
47. Matson Fruit Company, Selah, WA
48. McDougall & Sons, Inc., Wenatchee, WA
49. Monson Fruit Co., Selah, WA
50. Morgan's of Washington dba Double Diamond Fruit, Quincy, WA
51. Naumes, Inc., Medford, OR
52. Northern Fruit Company, Inc., Wenatchee, WA
53. Olympic Fruit Co., Moxee, WA
54. Oneonta Trading Corp., Wenatchee, WA
55. Orchard View Farms, Inc., The Dalles, OR
56. Pacific Coast Cherry Packers, LLC, Yakima, WA
57. Piepel Premium Fruit Packing LLC, East Wenatchee, WA
58. Pine Canyon Growers LLC, Orondo, WA
59. Polehn Farms, Inc., The Dalles, OR
60. Price Cold Storage & Packing Co., Inc., Yakima, WA
61. Pride Packing Company LLC, Wapato, WA
62. Quincy Fresh Fruit Co., Quincy, WA
63. Rainier Fruit Company, Selah, WA
64. Roche Fruit, Ltd., Yakima, WA
65. Sage Fruit Company, L.L.C., Yakima, WA
66. Smith & Nelson, Inc., Tonasket, WA
67. Stadelman Fruit, L.L.C., Milton-Freewater, OR, and Zillah, WA
68. Stemilt Growers, LLC, Wenatchee, WA
69. Symms Fruit Ranch, Inc., Caldwell, ID
70. The Dalles Fruit Company, LLC, Dallesport, WA
71. Underwood Fruit & Warehouse Co., Bingen, WA
72. Valicoff Fruit Company Inc., Wapato, WA
73. Washington Cherry Growers, Peshastin, WA
74. Washington Fruit & Produce Co., Yakima, WA
75. Western Sweet Cherry Group, LLC, Yakima, WA
76. Whitby Farms, Inc. dba: Farm Boy Fruit Snacks LLC, Mesa, WA
77. WP Packing LLC, Wapato, WA
78. Yakima Fresh, Yakima, WA
79. Yakima Fruit & Cold Storage Co., Yakima, WA
80. Zirkle Fruit Company, Selah, WA

The effective date of the amendment is July 8, 2020, the date on which NFE's application to amend was deemed submitted.

Dated: October 16, 2020.

Joseph Flynn,

Director, Office of Trade and Economic Analysis, International Trade Administration, U.S. Department of Commerce.

[FR Doc. 2020–23293 Filed 10–20–20; 8:45 am]

BILLING CODE 3510–DR–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 200921–0251]

National Cybersecurity Center of Excellence (NCCoE) Zero Trust Cybersecurity: Implementing a Zero Trust Architecture

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 the Zero Trust Cybersecurity: Implementing a Zero Trust Architecture project. 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 Zero Trust Cybersecurity: Implementing a Zero Trust Architecture project. Participation in the building

block is open to all interested organizations.

DATES: 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 November 20, 2020.

ADDRESSES: The NCCoE is located at 9700 Great Seneca Highway, Rockville, MD 20850. Letters of interest must be submitted to *nccoe-zta-project@list.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 consortium Cooperative Research and Development Agreement (CRADA) with NIST. An NCCoE consortium CRADA template can be found at: *https://nccoe.nist.gov/library/nccoe-consortium-crada-example.*

FOR FURTHER INFORMATION CONTACT: Alper Kerman via email to *nccoe-zta-project@list.nist.gov;* or by telephone at 301–975–0200. Additional details about the Zero Trust Cybersecurity: Implementing a Zero Trust Architecture project are available at *https://www.nccoe.nist.gov/zerotrust.*

SUPPLEMENTARY INFORMATION: Interested parties can access the letter of interest template by visiting the project website at *https://www.nccoe.nist.gov/zerotrust* and completing the letter of interest webform. Completed letters of interest should be submitted to NIST and will be accepted on a first come, first served basis. When the building block has been completed, NIST will post a notice on the NCCoE Zero Trust Cybersecurity: Implementing a Zero Trust Architecture project website at *https://www.nccoe.nist.gov/zerotrust* announcing the completion of the building block and informing the public that it will no longer accept letters of interest for this building block.

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 Zero Trust Cybersecurity: Implementing a Zero Trust Architecture project. The full building block can be viewed at: *https://www.nccoe.nist.gov/zerotrust.*

Interested parties can access the letter of interest template by visiting the project website at *https://www.nccoe.nist.gov/zerotrust* and completing the letter of interest webform. On completion of the webform, interested parties will receive access to the 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: The objective of this building block project is to produce an example implementation(s) of a zero trust architecture that is designed and deployed according to the concepts and tenets documented in the NIST Special Publication (SP) 800–207, *Zero Trust Architecture.* The proposed proof-of-concept solution(s) will integrate commercial and open source products that leverage cybersecurity standards and recommended practices to demonstrate the use case scenarios detailed in the *Implementing a Zero Trust Architecture* project description at *https://www.nccoe.nist.gov/zerotrust.* This project will result in a publicly available NIST Cybersecurity Practice Guide as a Special Publication 1800 series, a detailed implementation guide describing the practical steps needed to implement a cybersecurity reference implementation.

Requirements: Each responding organization's letter of interest should identify which security platform component(s) or capability(ies) it is offering. 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 the *Zero Trust Cybersecurity: Implementing a Zero Trust Architecture* project description (for reference, please see the link in the Process section above) and include, but are not limited to:

Core Components of Zero Trust Architecture

- *Policy Engine:* The policy engine handles the ultimate decision to grant, deny, or revoke access to a resource for a given subject. The policy engine calculates the trust scores/confidence levels and ultimate access decisions.
- *Policy Administrator:* The policy administrator is responsible for establishing and/or terminating the transaction between a subject and a resource. It generates any session-specific authentication and authentication token or credential used by a client to access an enterprise resource. It is closely tied to the Policy Engine and relies on its decision to ultimately allow or deny a session.
- *Policy Enforcement Point:* The policy enforcement point handles enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource.

Functional Components of Zero Trust Architecture

- The data security component includes all the data access policies and rules that an enterprise develops to secure its information, and the means to protect data at rest and in transit.
- The endpoint security component encompasses the strategy, technology, and governance to protect endpoints (*e.g.,* servers, desktops, mobile phones, IoT devices) from threats and attacks, as well as protect the enterprise from threats from managed and unmanaged devices.
- The identity and access management component includes the strategy, technology, and governance for creating, storing, and managing

enterprise user (*i.e.,* subject) accounts and identity records and their access to enterprise resources.

• The security analytics component encompasses all the threat intelligence feeds and traffic/activity monitoring for an IT enterprise. It gathers security and behavior analytics about the current state of enterprise assets and continuously monitors those assets to actively respond to threats or malicious activity. This information could feed the policy engine to help make dynamic access decisions.

Devices and Network Infrastructure Components of a Zero Trust Architecture

• Assets include the devices/endpoints, such as laptops, tablets, and other mobile or IoT devices, that connect to the enterprise.

• Enterprise resources include data and computer resources as well as applications/services that are hosted and managed on-premise, in the cloud, at the edge, or some combination of these.

Each responding organization's letter of interest should identify how their products help address one or more of the following desired security characteristics and properties in section 3 of the *Zero Trust Cybersecurity: Implementing a Zero Trust Architecture* project description (for reference, please see the link in the PROCESS section above):

• All interactions throughout the proposed architecture are achieved in the most secure manner available, with emphasis on protecting confidentiality and integrity through a consistent identification, authentication, and authorization scheme.

• All interactions throughout the proposed architecture are continually reassessed with possible reauthentication and reauthorization as necessary to mitigate unauthorized access to enterprise resources.

• Access to an enterprise resource is assessed on a per-session basis and authorized specifically for that enterprise resource.

• Access requests are evaluated dynamically based on organizational policies and rules for accessing enterprise resources, including the observable state of:

a. Subject identity (*e.g.,* user account or service identity with associated attributes)

b. requesting asset (*e.g.,* laptop, mobile device, server) device characteristics (*e.g.,* software version installed, security posture, network location, time/date of request, previously observed behavior, and installed credentials)

c. requested resource (*e.g.,* server, application, service) characteristics

• Enterprise assets and resources are continuously monitored and reassessed in order to maintain them in the most secure states possible.

• Log and event data generated about the current state of enterprise assets, resources, and interactions throughout the proposed architecture are collected and leveraged for better policy alignment and enforcement to increase the enterprise's overall security posture.

• Secure access to corporate resources, hosted either on-premise or within a cloud environment, as well as to non-corporate resources on the internet are provided without the use of conventional network and network perimeter access and security solutions.

• Integration with various directory protocols and identity management services (*e.g.,* Lightweight Directory Access Protocol [LDAP], OAuth 2.0, Active Directory, OpenLDAP, Security Assertion Markup Language) is demonstrated.

• Integration with security information and event management tools through common application programming interfaces is demonstrated.

• Desired enterprise device security characteristics are demonstrated, including:

a. Maintaining data protection at rest and in transit

b. remediating device vulnerabilities that could result in unauthorized access to data stored on or accessed by the device, and misuse of the device

c. mitigating malware execution on the device that could result in unauthorized access to data stored on or accessed by the device, and misuse of the device

d. mitigating the risk of data loss through accidental, deliberate, or malicious deletion or obfuscation of data stored on the device

e. maintaining awareness of and responding to suspicious or malicious activities within and against the device to prevent or detect a compromise of the device

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 Zero Trust Cybersecurity: Implementing a Zero Trust Architecture building block will be conducted in a manner consistent with the following standards and guidance: FIPS 200, SP 800–37, SP 800–53, SP 800–63, and SP 800–207. Additional details about the Zero Trust Cybersecurity: Implementing a Zero Trust Architecture project are available at *https://www.nccoe.nist.gov/zerotrust.*

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 Zero Trust Cybersecurity: Implementing a Zero Trust Architecture project. 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 Zero Trust Cybersecurity: Implementing a Zero Trust Architecture project. 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 Zero Trust Cybersecurity: Implementing a Zero Trust Architecture project capability will be announced on the NCCoE website at least two weeks in advance at *https://nccoe.nist.gov/.* The expected outcome will demonstrate how the components of the Zero Trust Architecture can provide security capabilities to mitigate identified risks and meet industry sectors' compliance requirements. 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 *https://nccoe.nist.gov/.*

Kevin A. Kimball,

Chief of Staff.

[FR Doc. 2020–23292 Filed 10–20–20; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[RTID 0648–XA554]

Takes of Marine Mammals Incidental to Specified Activities; Taking Marine Mammals Incidental to the U.S. Coast Guard's Base Los Angeles/Long Beach Wharf Expansion Project, Los Angeles, California

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

ACTION: Notice; proposed incidental harassment authorization; request for comments on proposed authorization and possible renewal.

SUMMARY: NMFS has received a request from the U.S. Coast Guard (Coast Guard) for authorization to take marine mammals incidental to the Base Los Angeles/Long Beach Wharf Expansion Project in Los Angeles, California. Pursuant to the Marine Mammal Protection Act (MMPA), NMFS is requesting comments on its proposal to issue an incidental harassment authorization (IHA) to incidentally take marine mammals during the specified activities. NMFS is also requesting comments on a possible one-year renewal that could be issued under certain circumstances and if all requirements are met, as described in Request for Public Comments at the end of this notice. NMFS will consider public comments prior to making any final decision on the issuance of the requested MMPA authorizations and agency responses will be summarized in the final notice of our decision.

DATES: Comments and information must be received no later than November 20, 2020.

ADDRESSES: Comments should be addressed to Jolie Harrison, Chief, Permits and Conservation Division, Office of Protected Resources, National Marine Fisheries Service. Comments should be sent to *ITP.Meadows@noaa.gov.*

Instructions: NMFS is not responsible for comments sent by any other method, to any other address or individual, or received after the end of the comment period. Comments received electronically, including all attachments, must not exceed a 25-megabyte file size. Attachments to electronic comments will be accepted in Microsoft Word or Excel or Adobe PDF file formats only. All comments received are a part of the public record and will generally be posted online at *https://www.fisheries.noaa.gov/permit/incidental-take-authorizations-under-marine-mammal-protection-act* without change. All personal identifying information (*e.g.,* name, address) voluntarily submitted by the commenter may be publicly accessible. Do not submit confidential business information or otherwise sensitive or protected information.

FOR FURTHER INFORMATION CONTACT: Dwayne Meadows, Ph.D., Office of Protected Resources, NMFS, (301) 427–8401. Electronic copies of the application and supporting documents, as well as a list of the references cited in this document, may be obtained online at: *https://www.fisheries.noaa.gov/permit/incidental-take-authorizations-under-marine-mammal-protection-act.* In case of problems accessing these documents, please call the contact listed above.

SUPPLEMENTARY INFORMATION:

Background

The MMPA prohibits the ''take'' of marine mammals, with certain exceptions. Sections 101(a)(5)(A) and (D) of the MMPA (16 U.S.C. 1361 *et seq.*) direct the Secretary of Commerce (as delegated to NMFS) to allow, upon request, the incidental, but not intentional, taking of small numbers of marine mammals by U.S. citizens who engage in a specified activity (other than commercial fishing) within a specified geographical region if certain findings are made and either regulations are issued or, if the taking is limited to harassment, a notice of a proposed incidental take authorization may be provided to the public for review.

Authorization for incidental takings shall be granted if NMFS finds that the taking will have a negligible impact on the species or stock(s) and will not have an unmitigable adverse impact on the availability of the species or stock(s) for taking for subsistence uses (where relevant). Further, NMFS must prescribe the permissible methods of taking and other ''means of effecting the least practicable adverse impact'' on the affected species or stocks and their habitat, paying particular attention to rookeries, mating grounds, and areas of similar significance, and on the availability of the species or stocks for taking for certain subsistence uses (referred to in shorthand as ''mitigation''); and requirements pertaining to the mitigation, monitoring and reporting of the takings are set forth.

The definitions of all applicable MMPA statutory terms cited above are included in the relevant sections below.

National Environmental Policy Act

To comply with the National Environmental Policy Act of 1969 (NEPA; 42 U.S.C. 4321 *et seq.*) and NOAA Administrative Order (NAO) 216–6A, NMFS must review our proposed action (*i.e.,* the issuance of an IHA) with respect to potential impacts on the human environment.

This action is consistent with categories of activities identified in Categorical Exclusion B4 (IHAs with no anticipated serious injury or mortality) of the Companion Manual for NOAA Administrative Order 216–6A, which do not individually or cumulatively have the potential for significant impacts on the quality of the human environment and for which we have not identified any extraordinary circumstances that would preclude this categorical exclusion. Accordingly, NMFS has preliminarily determined that the issuance of the proposed IHA qualifies to be categorically excluded from further NEPA review.

We will review all comments submitted in response to this notice prior to concluding our NEPA process or making a final decision on the IHA request.

Summary of Request

On July 2, 2020, NMFS received an application from the Coast Guard requesting an IHA to take small numbers of five species of marine mammals incidental to pile driving associated with the Base Los Angeles Long Beach Wharf Expansion Project in Los Angeles, California. The application was deemed adequate and complete on October 5, 2020. The Coast Guard's request is for take of a small number of five species of marine mammals by Level A and/or Level B harassment. Neither the Coast Guard nor NMFS expects serious injury or mortality to result from this activity and, therefore, an IHA is appropriate.

Description of Proposed Activity

Overview

The purpose of the project is to expand the existing wharf and other base infrastructure for hosting two additional offshore patrol cutters. The existing 1255-foot (383 meters (m)) long