with our practice and with section 705(c)(5)(A) of the Act.

Final Results of the Administrative Review

We find the following net countervailable subsidy rates for the POR January 1, 2018, through December

Company	Subsidy rate (percent *ad valorem*)
Icdas Celik Enerji Tersane ve Ulasim Sanayi A.S. and its cross-owned affiliates [10]	0.32 (*de minimis*)
Kaptan Demir Celik Endustrisi ve Ticaret A.S. and Kaptan Metal Dis Ticaret ve Nakliyat A.S. and their cross-owned affiliates [11]	1.82
Colakoglu Dis Ticaret A.S.	1.82
Colakoglu Metalurji A.S.	1.82

Disclosure 31, 2018:

Commerce intends to disclose the calculations and analysis performed for these final results of review within five days of the date of publication of this notice in the **Federal Register**, in accordance with 19 CFR 351.224(b).

Assessment Requirements

In accordance with section 751(a)(2)(C) of the Act and 19 CFR 351.212(b)(2), Commerce shall determine, and CBP shall assess, countervailing duties on all appropriate entries covered by this review. Commerce intends to issue assessment instructions to CBP no earlier than 35 days after publication of the final results of this review in the **Federal Register**. If a timely summons is filed at the U.S. Court of International Trade, the assessment instructions will direct CBP not to liquidate relevant entries until the time for parties to file a request for a statutory injunction has expired (*i.e.,* within 90 days of publication).

Cash Deposit Requirements

In accordance with section 751(a)(1) of the Act, we also intend to instruct CBP to collect cash deposits of estimated countervailing duties in the amounts shown above for the above-listed companies with regard to shipments of subject merchandise entered, or withdrawn from warehouse, for consumption on or after the date of publication of these final results of review. For all non-reviewed firms, CBP will continue to collect cash deposits of estimated countervailing duties at the all-others rate or the most recent company-specific rate applicable to the company, as appropriate. These cash deposit requirements, when imposed, shall remain in effect until further notice.

Administrative Protective Order

This notice also serves as a final reminder to parties subject to an administrative protective order (APO) of their responsibility concerning the disposition of proprietary information disclosed under APO in accordance with 19 CFR 351.305(a)(3). Timely written notification of the return or destruction of APO materials or conversion to judicial protective order, is hereby requested. Failure to comply with the regulations and terms of an APO is a sanctionable violation.

Notification to Interested Parties

The final results are issued and published in accordance with sections 751(a)(1) and 777(i)(1) of the Act, and 19 CFR 351.213(d)(4) and 19 CFR 351.221(b)(5).

Dated: September 21, 2021.

Christian Marsh,

Acting Assistant Secretary for Enforcement and Compliance.

Appendix

List of Topics Discussed in the Issues and Decision Memorandum

I. Summary
II. Background
III. Scope of the Order
IV. Rescission of Administrative Review, In Part
V. Subsidies Valuation Information
VI. Analysis of Programs
VII. Discussion of the Issues
Comment 1: Whether Commerce Should Countervail Import Duty Exemptions Under the Inward Processing Regime (IPR) Program
Comment 2: Whether Commerce Should Countervail the Provision of Lignite for Less than Adequate Remuneration (LTAR)
Comment 3: Whether Commerce Should Countervail the Provision of Natural Gas for LTAR
Comment 4: Whether Commerce Should Revise the Sales Denominators That It Used in the Preliminary Results for Icdas and Kaptan
Comment 5: Whether Commerce Should Revise its Finding that Nur Gemicilik ve Tic. A.S. (Nur) is a Cross-Owned Input Supplier
Comment 6: Whether Commerce Should Revise Its Finding That Nur's Land Rent Exemption is Countervailable
Comment 7: Whether Commerce Should Reduce Its Calculation of Benefits Attributed to Icdas for Renewable Energy Sources Support Mechanism (YEKDEM) Support by the Amount Reclaimed
Comment 8: Whether Commerce Should Revise Its Benchmark Interest Rate Calculations to Include All Short-Term Commercial Loans in Effect During the POR
VIII. Recommendation

[FR Doc. 2021–20906 Filed 9–24–21; 8:45 am]

BILLING CODE 3510–DS–P

[10] Commerce finds the following companies to be cross-owned with Icdas: Mardas Marmara Deniz Isletmeciligi A.S.; Oraysan Insaat Sanayi ve Ticaret A.S.; Artim Demir Insaat Turizm Sanayi Ticaret Ltd. Sti.; Anka Entansif Hayvancilik Gida Tarim Sanayi ve Ticaret A.S.; Karsan Gemi Insaa Sanayi Ticaret A.S.; Artmak Denizcilik Ticaret Ve Sanayi A.S.; and Eras Tasimacilik Taahhut Ins.Tic.A.S.

[11] Commerce finds the following companies to be cross-owned with Kaptan: Martas Marmara Ereglisi Liman Tesisleri A.S.; Aset Madencilik A.S.; Kaptan Is Makinalari Hurda Alim Satim Ltd. Sti.; Efesan Demir San. Ve Tic. A.S.; and Nur Gemicilik ve Tic. A.S.

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 210914–0185]

National Cybersecurity Center of Excellence (NCCoE) Addressing Visibility Challenges With TLS 1.3

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 letters of interest describing products and technical expertise to support and demonstrate security platforms for the *Addressing Visibility Challenges With TLS 1.3* 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 *Addressing Visibility Challenges With TLS 1.3* project. Participation in the project 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 October 27, 2021.

ADDRESSES: The NCCoE is located at 9700 Great Seneca Highway, Rockville, MD 20850. Letters of interest must be submitted to *applied-crypto-visibility@nist.gov* or via hardcopy to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Interested parties can access the letter of interest template by visiting *https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/cmvp-automation* and completing the letter of interest webform. NIST will announce the completion of the selection of participants and inform the public that it will no longer accept letters of interest for this project at *https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/addressing-visibility-challenges-tls-13.* Organizations whose letters of interest are accepted 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: Tim Polk via phone (301) 975–0225 or email *applied-crypto-visibility@nist.gov;* by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the *Addressing Visibility Challenges With TLS 1.3* project are available at *https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/addressing-visibility-challenges-tls-13.*

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 *Addressing Visibility Challenges With TLS 1.3* project. The full project can be viewed at: *https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/addressing-visibility-challenges-tls-13.*

Interested parties can access the template for a letter of interest by visiting the project website at *https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/addressing-visibility-challenges-tls-13* 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 as accurate, and submit to NIST by email or hardcopy. NIST will contact interested parties if there are questions regarding the responsiveness of the letters of interest to the project 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 project. When the project has been completed, NIST will post a notice on the *Addressing Visibility Challenges With TLS 1.3* project website at *https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/addressing-visibility-challenges-tls-13* announcing the completion of the project and informing the public that it will no longer accept letters of interest for this project. Completed letters of interest should be submitted to NIST and will be accepted on a first come, first served basis. There may be continuing opportunity to participate even after initial activity commences for participants who were not selected initially or have submitted the letter of interest after the selection process. Selected participants will be required to enter into a consortium CRADA with NIST (for reference, see **ADDRESSES** section above).

Project Objective: Deployment of new protocols for exchanging encrypted information, in particular the latest version of the Transport Layer Security (TLS) protocol, TLS 1.3, can impact the ability of some organizations to meet their regulatory, security, and operational requirements due to loss of visibility into the content of communications within their environments. The objective of this project is to demonstrate practical and implementable approaches to help those organizations adopt TLS 1.3 in their private data centers and in hybrid cloud environments while meeting their existing requirements. 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 *Addressing Visibility Challenges with TLS 1.3* project description at *https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/addressing-visibility-challenges-tls-13.* 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 for Letters of Interest: 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 *Addressing Visibility Challenges with TLS 1.3* project description at *https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/addressing-visibility-challenges-tls-13* and include, but are not limited to:

- Network infrastructure, such as firewalls, routers and switches, and load balancers
- Physically hosted and cloud-based servers, network-attached storage, application servers, web servers, databases, and identity management systems
- Additional components required to achieve visibility (*e.g.,* traffic collection or sensors), as identified in proposed solutions

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 *Addressing Visibility Challenges with TLS 1.3* project description at *https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/addressing-visibility-challenges-tls-13:*

- Proposed contributions must support addressing security, operational, or compliance requirements where traffic is encrypted between one or more sets of components in the demonstration architecture. For example, a solution might focus on achieving visibility into information exchanges between cloud-hosted application servers to support troubleshooting. Alternatively, a solution might analyze information exchanges between physically hosted web servers with hardware security modules and cloud-based services relying on software-based cryptographic modules to monitor for fraudulent transactions. Solutions are not required to address all challenges or all components in the architecture, although comprehensive solutions are strongly encouraged.
- The use of visibility technologies within the enterprise data center environment is generally acceptable in ways that visibility technologies on the public internet may not be. However, contributions that forgo forward secrecy within the enterprise must be deployable in a manner that preserves forward secrecy for information exchanges over the internet if they are to be accepted.
- While visibility challenges are not limited to a single protocol, the focus for this project is TLS 1.3. Proposed contributions must be compatible with TLS 1.3, excepting those solutions relying upon an alternative network security protocol as a replacement for TLS. That is, proposed contributions that modify TLS 1.3 or restrict enterprises to earlier version of TLS will not be considered.
- Contributions must support scalable solutions.
- Contributions must support solutions that are relatively easy to implement/deploy.
- Contributions must support solutions that are protocol agnostic.
- Contributions must support solutions that are usable in real time and post-packet capture.
- Contributions must support solutions that are effective for both security and troubleshooting purposes.
- Contributions must support solutions that are widely available and supported in mainstream commercial products and services.
- The baseline criteria apply across the full range of scenarios described in the project description, but some characteristics are more relevant to different categories of solutions than others. Specific characteristics relevant to different classes of solutions include:
  - For solutions that achieve visibility through endpoint mechanisms (*e.g.,* logging) or network architectures (middle boxes, overlays, or mesh service architectures), components need to support demonstration of scalability, ease of deployment, and reliable and timely access to information. For example, scalability and reliable access to historical information would be an area of interest for centralized logging solutions.
  - For solutions that achieve visibility through key management mechanisms that share keys to facilitate TLS decryption, components need to support demonstration that security of keys and data against misuse or compromise and assurance that recorded traffic is not indefinitely at risk of compromise. Specifically, components would need to support demonstration that (1) the security of systems and procedures used to transmit, store, provide access to, and use the keys, and (2) mechanisms that ensure comprehensive deletion of decryption keys when established temporal or data protection limits are met.
  - For solutions that achieve visibility through analysis of encrypted data, components would need to support demonstrating the capabilities and limitations of these emerging tools with respect to each of the four scenarios.
  - For solutions that rely on alternative network security protocols, components would need to support demonstrating scalability, usability, and ease of deployment. If the solution also includes key management mechanisms to share keys for decryption, the properties identified above would need to be demonstrated.
- For all cases, support for demonstration of management, operational, and technical security controls that compensate and mitigate any potential new risks that may be introduced into the environment will be required.

In their letters of interest, responding organizations need to acknowledge the importance of and 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 *Addressing Visibility Challenges with TLS 1.3* project will be conducted in a manner consistent with the most recent version of the following standards and guidance: FIPS 200, SP 800–37, SP 800–52, SP 800–53, SP 800–63, and SP 1800–16. Additional details about the Addressing *Visibility Challenges with TLS 1.3* project are available at *https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/addressing-visibility-challenges-tls-13.*

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 *Addressing Visibility Challenges with TLS 1.3* 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 *Addressing Visibility Challenges with TLS 1.3* 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 *Addressing Visibility Challenges with TLS 1.3* 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 solutions that address *Visibility Challenges with TLS 1.3* 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/.*

Alicia Chambers,

NIST Executive Secretariat.

[FR Doc. 2021–20907 Filed 9–24–21; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[RTID 0648–XB445]

Nominations for the 2022–2025 General Advisory Committee and the Scientific Advisory Subcommittee to the United States Delegation to the Inter-American Tropical Tuna Commission

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

ACTION: Notice; request for nominations.

SUMMARY: National Marine Fisheries Service, on behalf of the Secretary of Commerce, is seeking nominations for the General Advisory Committee (GAC) to the U.S. delegation to the Inter-American Tropical Tuna Commission (IATTC or Commission), as well as to a Scientific Advisory Subcommittee (SAS) of the GAC. The purpose of the GAC and its SAS is to provide public input and advice to the U.S. delegation to aid in the formulation of policy and positions for meetings of the IATTC and its subsidiary bodies. The SAS shall also function as the National Scientific Advisory Committee provided for in the Agreement on the International Dolphin Conservation Program.

DATES: Nominations must be received no later than November 29, 2021.

ADDRESSES: Nominations should be directed to Barry Thom, Regional Administrator, NMFS West Coast Region, and may be submitted by any of the following means:

- Email *RegionalAdministrator.WCRHMS@noaa.gov* with the subject line: ''General Advisory Committee and Scientific Advisory Subcommittee nominations''

FOR FURTHER INFORMATION CONTACT: William Stahnke, West Coast Region, NMFS, at *william.stahnke@noaa.gov,* or at (562) 980–4088.

SUPPLEMENTARY INFORMATION:

General Advisory Committee

The Tuna Conventions Act (TCA) provides that the Secretary of Commerce, in consultation with the Secretary of State, shall appoint a ''General Advisory Committee'' to advise the U.S. delegation to the IATTC. The GAC shall be composed of no more than 25 individuals who shall be representative of the various groups concerned with the fisheries covered by the IATTC, including non-governmental conservation organizations, providing an equitable balance among such groups to the maximum extent practicable. Members of the GAC shall be invited to attend all non-executive meetings of the U.S. delegation to the IATTC and at such meetings shall be given the opportunity to examine and be heard on all proposed programs of investigation, reports, recommendations, and regulations of the Commission.

The Chair of the Pacific Fishery Management Council's (Pacific Council) Advisory Subpanel for Highly Migratory Fisheries and the Chair of the Western Pacific Fishery Management Council's (Western Pacific Council) Advisory Committee shall be ex-officio members of the GAC by virtue of their positions advising those Councils. GAC members will be eligible to participate as members of the U.S. delegation to the Commission and its working groups to the extent that the Commission rules and space for delegations allow.

Meetings of the GAC, except when in executive session, shall be open to the public, and prior notice of meetings shall be made public in timely fashion. In accordance with Public Law 114–81, the GAC shall not be subject to the Federal Advisory Committee Act (5 U.S.C. App.).

Individuals appointed to serve as a member of the GAC shall serve without pay. While away from their homes or regular places of business to attend meetings of the GAC, they shall be allowed travel expenses, including per diem in lieu of subsistence, in the same manner as persons employed intermittently by the Federal Government are allowed expenses under 5 U.S.C. 5703. In addition, individuals appointed to serve as a member of the GAC shall not be considered Federal employees except for the purposes of injury compensation or tort.

Scientific Advisory Subcommittee

The TCA also provides that the Secretary of Commerce, in consultation with the Secretary of State, shall appoint persons to serve on the subcommittee of the GAC, referred to here as the ''Scientific Advisory Subcommittee''. The SAS shall be composed of no fewer than 5 and no more than 15 qualified scientists with balanced representation from the public and private sectors, including non-governmental conservation organizations. In determining whether a person is a qualified scientist the Secretary may consider, among other things, advanced degrees and/or publications in fields such as fisheries or marine science.

National Scientific Advisory Committee

The SAS shall also function as the National Scientific Advisory Committee which is required to be established pursuant to Article XI of the Agreement on the International Dolphin Conservation Program (AIDCP). In this regard, the SAS shall perform the functions of the National Scientific Advisory Committee as specified in Annex VI of the AIDCP. These functions include, but are not limited to:

(1) Receiving and reviewing relevant data, including data provided to NMFS by IATTC staff;

(2) Advising and recommending measures and actions to the U.S. Government that should be undertaken to conserve and manage stocks of living marine resources in the eastern Pacific Ocean;

(3) Making recommendations to the U.S. Government regarding research needs related to the eastern Pacific Ocean tuna purse seine fishery;

(4) Promoting the regular and timely full exchange of data among the AIDCP Parties on a variety of matters related to the implementation of the AIDCP; and

(5) Consulting with other experts, as necessary, in order to achieve the objectives of the AIDCP.

Members of the SAS/National Scientific Advisory Committee shall receive no compensation for their service.

General Provisions

Each member of the GAC shall be appointed for a term of three years, starting from the date of the appointment, and may be reappointed. The Secretary of Commerce and the Secretary of State shall provide the GAC with relevant information concerning fisheries and international fishery agreements. The Secretary of Commerce shall provide to the GAC such administrative and technical support services that are necessary for its effective functioning in a timely manner.

Procedures for Submitting Applications

Applications for the GAC and the SAS/National Scientific Advisory Committee should be submitted to NMFS West Coast Region (see **ADDRESSES**). This request for applications is for first time nominees,