mitigation measures on an emergency basis.

Kristie Canegallo,

Senior Official Performing the Duties of the Deputy Secretary & Chairman of the Transportation Security Oversight Board.

[FR Doc. 2024–08394 Filed 4–18–24; 8:45 am]

BILLING CODE 9110–9M–P

DEPARTMENT OF HOMELAND SECURITY

6 CFR Chapter I

49 CFR Chapter XII

Ratification of Security Directives

AGENCY: Office of Strategy, Policy, and Plans, Department of Homeland Security (DHS).

ACTION: Notice of ratification of security directives.

SUMMARY: The Department of Homeland Security (DHS) is publishing official notice that the Transportation Security Oversight Board (TSOB) ratified Transportation Security Administration (TSA) Security Directive Pipeline–2021–01C and Security Directive Pipeline–2021–02D, applicable to owners and operators of critical hazardous liquid and natural gas pipeline infrastructure (owner/operators). Security Directive Pipeline–2021–01C, issued on May 22, 2023, extended the requirements of the Security Directive Pipeline-2021–01 series for an additional year. Security Directive Pipeline–2021–02D, issued on July 26, 2023, extended the requirements of the Security Directive Pipeline–2021–02 series for an additional year and amended them to strengthen their effectiveness and address emerging cyber threats.

DATES: The TSOB ratified Security Directive Pipeline–2021–01C on June 21, 2023, and Security Directive Pipeline–2021–02D on August 24, 2023.

FOR FURTHER INFORMATION CONTACT: Thomas McDermott, Deputy Assistant Secretary for Cyber, Infrastructure, Risk and Resilience Policy, at 202–834–5803 or *thomas.mcdermott@hq.dhs.gov*.

SUPPLEMENTARY INFORMATION:

I. Background

A. Cybersecurity Threat

The cyber threat to the country's critical infrastructure has only increased in the time since TSA issued its initial cybersecurity-related security directive (Security Directive Pipeline–2021–01) in response to the Colonial Pipeline incident. Cyber threats to surface transportation systems, including pipelines, continue to proliferate, as both nation-states and criminal cyber groups continue to target critical infrastructure in order to cause operational disruption and economic harm.[1] Cyber incidents, particularly ransomware attacks, are likely to increase in the near and long term, due in part to vulnerabilities identified by threat actors in U.S. networks.[2] Particularly in light of the ongoing Russia-Ukraine conflict,[3] these threats remain elevated and pose a risk to the national and economic security of the United States.

B. Security Directive Pipeline–2021–01C

On May 27, 2021, TSA issued Security Directive Pipeline–2021–01, which was the first of two security directives issued by TSA to enhance the cybersecurity of critical pipeline systems in response to the Colonial Pipeline attack on May 7, 2021. Security Directive Pipeline–2021–01, and the subsequent amendments in this series, required covered owner/operators to: (1) report cybersecurity incidents to CISA; (2) appoint a cybersecurity coordinator to be available 24/7 to coordinate with TSA and CISA; and (3) conduct a self-assessment of cybersecurity practices, identify any gaps, and develop a plan and timeline for remediation.[4] This first security directive went into effect on May 28, 2021, was ratified by the TSOB on July 3, 2021, and was set to expire on May 28, 2022.[5]

On December 2, 2021, TSA issued Security Directive Pipeline–2021–01A, amending Security Directive Pipeline–2021–01, to update the definition of cybersecurity incident covered by the directive's reporting requirement and align it with the definition applicable to the other modes.[6] The TSOB ratified Security Directive Pipeline–2021–01A on December 29, 2021.[7] Security Directive Pipeline–2021–01, as amended by Security Directive Pipeline–2021–01A, was set to expire May 28, 2022. On May 27, 2022, TSA issued Security Directive Pipeline–2021–01B to extend the requirements of Security Directive Pipeline–2021–01A for an additional year.[8] Security Directive Pipeline–2021–01B became effective May 29, 2022 and was set to expire on May 29, 2023. The TSOB ratified Security Directive Pipeline–2021–01B on June 24, 2021.[9]

In light of the continuing threat, TSA determined that the measures required by the Security Directive Pipeline–2021–01, as amended and extended by Security Directive Pipeline–2021–01A and Security Directive Pipeline–2021–01B, remain necessary to protect the Nation's critical pipeline infrastructure beyond Security Directive Pipeline–2021–01B's expiration date of May 29, 2023. On May 22, 2023, TSA issued Security Directive Pipeline–2021–01C to extend the requirements of Security Directive Pipeline–2021–01B for an additional year. Security Directive Pipeline–2021–01C became effective May 29, 2023 and expires on May 29, 2024. Security Directive Pipeline–2021–01C contains no substantive changes from Security Directive Pipeline–2021–01B. Security Directive Pipeline–2021–01C is available online in TSA's Surface Transportation Cybersecurity Toolkit.[10]

C. Security Directive Pipeline–2021–02D

On July 19, 2021, TSA issued Security Directive Pipeline-2021–02, the second security directive TSA issued in response to the attack on Colonial Pipeline. This directive required owner/operators to implement additional

[1] Annual Threat Assessment of the U.S. Intelligence Community, Office of the Director of National Intelligence, 10, 15 (February 2023); Press Release 23–530, *Justice Department Announces Court-Authorized Disruption of Snake Malware Network Controlled by Russia's Federal Security Service,* Department of Justice, issued on May 9, 2023, available at *https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-snake-malware-network-controlled;* Joint Cybersecurity Advisory (AA23–144a), *People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection,* released by CISA on May 24, 2023.

[2] Alert (AA22–040A), *2021 Trends Show Increased Globalized Threat of Ransomware,* released by CISA on February 10, 2022 (as revised).

[3] Joint Cybersecurity Alert—Alert (AA22–011A), *Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure,* released by CISA, the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) on January 11, 2022 (as revised); Joint Cybersecurity Alert—Alert (AA22–110A), *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure,* released cybersecurity authorities of the United States, Australia, Canada, New Zealand, and the United Kingdom on April 20, 2022 (as revised).

[4] Security Directive Pipeline–2021–01: Enhancing Pipeline Cybersecurity.

[5] 86 FR 38209.

[6] During TSA's development of cybersecurity actions applicable to other transportation modes, TSA made a determination to modify the definition of cybersecurity incident it had used in the first security directive following industry input and consultation with DHS cybersecurity experts.

[7] 87 FR 31093.

[8] 88 FR 36919. Security Directive Pipeline–2021–01B also extended the deadline by which cybersecurity incidents must be reported to CISA from 12 hours to 24 hours after an incident is identified. This change aligned the reporting timeline for critical pipeline entities to mirror the reporting requirements applicable to other surface transportation entities and aviation entities.

[9] *Id.*

[10] TSA Surface Transportation Cybersecurity Toolkit, *available at https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit.*

cybersecurity measures to prevent disruption and degradation to their infrastructure in response to the ongoing threat, including a number of specific, prescribed mitigation measures.[11] On December 17, 2021, TSA issued Security Directive Pipeline–2021–02B, revising Security Directive Pipeline–2021–02 to provide additional flexibility to owner/operators in complying with certain requirements. The TSOB ratified Security Directive Pipeline–2021–02B on January 13, 2022.[12]

On July 21, 2022, TSA issued Security Directive Pipeline–2021–02C, transitioning the requirements of the previous versions in the series to be more performance-based and less prescriptive. The performance-based approach enhanced security by mandating that critical security outcomes are achieved while allowing owner/operators to choose the most appropriate security measures for their specific systems and operations. The directive became effective on July 27, 2022, and was set to expire on July 27, 2023. The TSOB ratified Security Directive Pipeline–2021–02C on August 19, 2022.[13]

Security Directive Pipeline–2021–02C identified critical security outcomes that covered parties must achieve. To ensure that these outcomes are met, the directive requires owner/operators to:

- Establish and implement a TSA-approved Cybersecurity Implementation Plan (CIP) that describes the specific cybersecurity measures employed and the schedule for achieving the security outcomes identified;
- Develop and maintain an up-to-date Cybersecurity Incident Response Plan (CIRP) to reduce the risk of operational disruption, or the risk of other significant impacts on necessary capacity, as defined in the directive, should the Information and/or Operational Technology systems of a gas or liquid pipeline be affected by a cybersecurity incident; and
- Establish a Cybersecurity Assessment Program (CAP) and submit an annual plan that describes how the owner/operator will proactively and regularly assess the effectiveness of cybersecurity measures and identify and resolve device, network, and/or system vulnerabilities.

In light of the continuing threat, TSA issued Security Directive Pipeline–2021–02D on July 26, 2023, extending the requirements of Security Directive Pipeline–2021–02C for an additional year. The directive became effective on July 27, 2023, and expires on July 27, 2024.

In addition to extending the performance-based requirements, Security Directive Pipeline–2021–02D includes several revisions intended to strengthen the effectiveness of the directive's requirements and allow greater ability to respond to changing threats. Security Directive Pipeline–2021–02D modified the requirements related to CIRPS and CAPS to provide greater clarity and strengthen their effectiveness and to ensure the provisions related to defining Critical Cyber Systems allow flexibility to respond to emerging and evolving threats. The security directive also contains several other clarifications and refinements of the existing requirements. The revisions contained in the directive were made following engagement with covered entities and in consultation with federal partners. Security Directive Pipeline–2021–02D is available online in TSA's Surface Transportation Cybersecurity Toolkit.[14]

II. TSOB Ratification

TSA has broad statutory responsibility and authority to safeguard the nation's transportation system.[15] The TSOB—a body consisting of the Secretary of Homeland Security, the Secretary of Transportation, the Attorney General, the Secretary of Defense, the Secretary of the Treasury, the Director of National Intelligence, or their designees, and a representative of the National Security Council—reviews certain TSA regulations and security directives as consistent with law.[16] TSA issued Security Directive Pipeline–2021–01C and Security Directive Pipeline–2021–02D under 49 U.S.C. 114(*l*)(2)(A), which authorizes TSA to issue emergency regulations or security directives without providing notice or the opportunity for public comment where ''the Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security.'' Security directives issued pursuant to the procedures in 49 U.S.C. 114(*l*)(2) ''shall remain effective for a period not to exceed 90 days unless ratified or disapproved by the Board or rescinded by the Administrator.'' [17]

Following the issuance of Security Directive Pipeline–2021–01C on May 22, 2023, the chair of the TSOB convened the board to review the directive. In reviewing Security Directive Pipeline–2021–01C, the TSOB reviewed the required measures extended by the directive and the continuing need for TSA to maintain these requirements pursuant to its emergency authority under 49 U.S.C. 114(*l*)(2) to prevent the disruption and degradation of the country's critical transportation infrastructure. The TSOB also considered whether to authorize TSA to extend the security directive beyond its current expiration date of May 29, 2024, subject to certain conditions, should the TSA Administrator believe such an extension is necessary to address the evolving threat that may continue beyond the original expiration date.

Following its review, the TSOB ratified Security Directive Pipeline–2021–01C on June 21, 2023. The TSOB also authorized TSA to extend the security directive beyond its current expiration date, should the TSA Administrator determine such an extension is necessary to address the evolving threat that may continue beyond the original expiration date. Such an extension is subject to the following conditions: (1) there are no changes to the security directive other than an extended expiration date; (2) the TSA Administrator makes an affirmative determination that conditions warrant the extension of the directive's requirements; and (3) the TSA Administrator documents such a determination and notifies the TSOB.

After TSA issued Security Directive Pipeline–2021–02D on July 26, 2023, the chair of the TSOB again convened the board to review that directive. In reviewing Security Directive Pipeline–2021–02D, the TSOB reviewed the amended required measures extended by the directive as well as the continuing need for TSA to maintain these requirements pursuant to its emergency authority under 49 U.S.C. 114(*l*)(2) to protect critical transportation infrastructure. Again, the TSOB also considered whether to authorize TSA to extend Security Directive Pipeline–2021–02D beyond its current expiration date of July 27, 2024, subject to the same conditions, should the TSA Administrator believe such an extension is necessary to address the threat.

[11] Security Directive Pipeline–2021–02 became effective on July 26, 2021, and was ratified by the TSOB on August 17, 2021.

[12] *See* 87 FR 31093 (May 23, 2022).

[13] *See* 88 FR 36919 (May 6, 2023). The TSOB also authorized TSA to extend Security Directive Pipeline–2021–02C beyond its expiration date of July 27, 2023, subject to certain conditions, including that such an extension would make no changes other than the extension of the expiration date.

[14] TSA Surface Transportation Cybersecurity Toolkit, *available at https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit.*

[15] *See, e.g.,* 49 U.S.C. 114(d), (f), (*l*), (m).

[16] *See, e.g.,* 49 U.S.C. 115; 49 U.S.C. 114(*l*)(2)(B).

[17] 49 U.S.C. 114(*l*)(2)(B).

The TSOB ratified Security Directive Pipeline–2021–02D on August 24, 2023. The TSOB also authorized TSA to extend the security directive beyond its current expiration date, should the TSA Administrator determine such an extension is necessary to address the evolving threat that may continue beyond the original expiration date. Such an extension is subject to the following conditions: (1) there are no changes to the security directive other than an extended expiration date; (2) the TSA Administrator makes an affirmative determination that conditions warrant the extension of the directive's requirements; and (3) the TSA Administrator documents such a determination and notifies the TSOB.

Kristie Canegallo,

Senior Official Performing the Duties of the Deputy Secretary & Chairman of the Transportation Security Oversight Board.

[FR Doc. 2024–08393 Filed 4–18–24; 8:45 am]

BILLING CODE 9110–9M–P

DEPARTMENT OF AGRICULTURE

Food and Nutrition Service

7 CFR Parts 210, 220, 225, and 292

[FNS–2023–0029]

RIN 0584–AE96

Establishing the Summer EBT Program and Rural Non-Congregate Option in the Summer Meal Programs

AGENCY: Food and Nutrition Service (FNS), Department of Agriculture (USDA).

ACTION: Interim final rule, extension of comment period.

SUMMARY: The USDA Food and Nutrition Service is extending for 120 days the public comment period on the interim final rule, ''Establishing the Summer EBT Program and Rural Non-Congregate Option in the Summer Meal Programs'', which published in the **Federal Register** on December 29, 2023. This action extends the public comment period from April 29, 2024, to August 27, 2024, to give the public additional time to prepare and submit comments.

DATES: The comment period of the interim final rule published December 29, 2023, at 88 FR 90230, is extended through August 27, 2024. To be assured of consideration, written comments on this interim final rule must be received on or before August 27, 2024.

ADDRESSES: The Food and Nutrition Service invites interested persons to submit comments on this interim final rule. Comments may be submitted by any of the following methods:

- *Federal eRulemaking Portal:* Go to *https://www.regulations.gov.* Follow the online instructions for submitting comments.
- *Mail:* Send comments to Community Meals Policy Division, Food and Nutrition Service, 1320 Braddock Place, Alexandria, VA 22314.
- All written comments submitted in response to this interim final rule will be included in the record and will be made available to the public. Please be advised that the substance of the comments and the identity of the individuals or entities submitting the comments will be subject to public disclosure. USDA will make the written comments publicly available on the internet via *https://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: J. Kevin Maskornick, Division Director, Community Meals Policy Division, USDA Food and Nutrition Service, 1320 Braddock Place, Alexandria, VA 22314; telephone: 703–305–2537.

SUPPLEMENTARY INFORMATION: The Food and Nutrition Service is extending the public comment period on the interim final rule ''Establishing the Summer EBT Program and Rural Non-Congregate Option in the Summer Meal Programs'', which published on December 29, 2023, at 88 FR 90230. The Consolidated Appropriations Act, 2023 required the Secretary of Agriculture to make available an option to States to provide summer meals for non-congregate meal service in rural areas with no congregate meal service and to establish a permanent Summer Electronic Benefits Transfer for Children Program (Summer EBT) for the purpose of ensuring continued access to food when school is not in session for the summer. This interim final rule amends the Summer Food Service Program (SFSP) and the National School Lunch Program's Seamless Summer Option (SSO) regulations to codify the flexibility for rural program operators to provide non-congregate meal service in the SFSP and SSO, collectively referred to as the summer meal programs. This rule also establishes regulations and codifies the Summer EBT Program in the Code of Federal Regulations.

This action extends the public comment period to August 27, 2024, to provide additional time for the public, including State administering agencies, Territories, and Indian Tribal Organizations, as well as program participants and beneficiaries, and other stakeholders, to prepare and submit comments. Because the interim final rule became effective immediately upon publication, stakeholders are already taking active steps to implement its provisions. Extending the comment period ensures that these stakeholders are able to provide robust feedback on the entirety of the interim final rule's provisions, and that this feedback is reflective of their implementation experiences in advance of and during Summer 2024. Receipt of informed public input accounting for the first year of operations under the new Program rules will be vital when the Food and Nutrition Service considers future rulemaking to finalize the provisions of the interim final rule.

Cynthia Long,

Administrator, Food and Nutrition Service.

[FR Doc. 2024–08369 Filed 4–18–24; 8:45 am]

BILLING CODE 3410–30–P

NUCLEAR REGULATORY COMMISSION

10 CFR Part 72

[NRC–2023–0220]

RIN 3150–AL05

List of Approved Spent Fuel Storage Casks: FuelSolutions™ Spent Fuel Management System, Certificate of Compliance No. 1026, Renewal of Initial Certificate and Amendment Nos. 1 Through 4

AGENCY: Nuclear Regulatory Commission.

ACTION: Direct final rule.

SUMMARY: The U.S. Nuclear Regulatory Commission (NRC) is amending its spent fuel storage regulations by revising the Westinghouse Electric Company LLC FuelSolutions™ Spent Fuel Management System listing within the ''List of approved spent fuel storage casks'' to renew the initial certificate and Amendment Nos. 1 through 4 to Certificate of Compliance No. 1026. The renewal of the initial certificate of compliance and Amendment Nos. 1 through 4 for 40 years revises the certificate's conditions and technical specifications to address aging management activities related to the structures, systems, and components important to safety of the dry storage system to ensure that these will maintain their intended functions during the period of extended storage operations.

DATES: This direct final rule is effective July 3, 2024, unless significant adverse comments are received by May 20, 2024. If the direct final rule is withdrawn as