U.S. Department of Homeland Security
Arlington, VA 20598

Transportation Security Administration

ACTION

MEMORANDUM FOR: Dominic Mancini
Deputy Administrator
Office of Information and Regulatory Affairs
Office of Management and Budget

THROUGH: Elizabeth Cappello
Deputy Chief Information Officer,
Department of Homeland Security

ELIZABETH A CAPPELLO Digitally signed by ELIZABETH A CAPPELLO Date: 2022.07.27 10:56:09 -04'00'

FROM: Yemi B. Oshinnaiye
Assistant Administrator
Chief Information Officer
Authorizing Official
Office of Information Technology
Transportation Security Administration

OPEYEMI B OSHINNAIYE Digitally signed by OPEYEMI B OSHINNAIYE Date: 2022.07.26 12:48:31 -04'00'

SUBJECT: Emergency Information Collection Request (ICR): Pipeline Corporate Security Review (1652-0056)

## Purpose

The memorandum seeks the Office of Management and Budget (OMB) approval of the Transportation Security Administration's (TSA's) request for an emergency revision under the Paperwork Reduction Act (PRA) to OMB Control Number 1652-0056, Pipeline Corporate Security Review (PCSR), to address cybersecurity risks and the ongoing cybersecurity threat to pipeline systems and associated infrastructure.

## Background

During the last few years, malicious cyber actors have demonstrated their willingness to conduct cyber-attacks against critical infrastructure by exploiting the vulnerability of Operational Technology and Information Technology systems and assets.

On May 8, 2021, the Colonial Pipeline Company announced that it had halted its pipeline operations due to a ransomware attack. This attack received national attention as it temporarily disrupted critical supplies of gasoline and other refined petroleum products throughout the East Coast. Such attacks pose significant threats to the country's infrastructure and economic well-being. Since then the federal government has been working closely with industry partners to address the threat.

Due to the cybersecurity threat to pipeline systems and associated infrastructure and in coordination with the Cybersecurity and Infrastructure Security Agency (CISA), TSA issued two Security Directives (SDs) in 2021 to Owners and Operators of a hazardous liquid and natural gas pipeline or liquefied natural gas facilities notified by TSA that their pipeline system or facility is critical. The SDs were issued under the authority of 49 U.S.C. 114(*l*)(2), which states:

> Notwithstanding any other provision of law or executive order (including an executive order requiring a cost-benefit analysis), if the Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security, the Administrator shall issue the regulation or security directive without providing notice or an opportunity for comment and without prior approval of the Secretary.

TSA issued the first SD, Pipeline-2021-01, on May 27, 2021. It required the reporting of cybersecurity incidents, designate a cybersecurity coordinator, and to conduct a cybersecurity risk assessment. The second SD, Pipeline-2021-02, was issued on July 19, 2021. Since issuance, TSA revised SD Pipeline-2021-02 twice in December 2021 to make some minor clarifications and extend deadlines (2021-02A and 2021-02B). The changes did not impact the collection requirements. Both of these SDs apply to Owners and Operators of hazardous liquid and natural gas pipelines or a liquefied natural gas facility notified by TSA that their pipeline system or facility is critical.

The pipeline sector continues to face a significant cybersecurity threat. Recent Joint Cybersecurity Advisories from CISA, the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA) highlight this threat:

- February 7, 2022: The Office of the Director for National Intelligence released the *Annual Threat Assessment of the U.S. Intelligence Community,* which noted that "China almost certainly is capable of launching cyber-attacks that would disrupt critical infrastructure services within the United States, including against oil and gas pipelines and rail systems."[1]
- March 24, 2022: CISA, FBI, and the Department of Energy (DOE) released Joint Cybersecurity Advisory (AA22-083A), *Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector.*[2]
- March 24, 2022: The FBI's Cyber Division released a Private Industry Notification (PIN 20220324-001), *Triton Malware Remains Threat to Global Critical Infrastructure Industrial Control Systems (ICS),* which warned that Russian actors continue to conduct activity targeting the global energy sector.
- April 13, 2022: CISA, FBI, NSA and DOE released Joint Cybersecurity Advisory (AA22-103A), *APT Cyber Tools Targeting ICS/SCADA Devices,* which warned that certain advanced persistent threat (APT) actors have exhibited the capability to gain full

[1] 2022 Annual Threat Assessment of the U.S. Intelligence Community (dni.gov)
[2] https://www.cisa.gov/uscert/ncas/alerts/aa22-083a

system access to multiple industrial control system (ICS)/supervisory control and data acquisition (SCADA) devices.[3]

- On April 20, 2022: CISA, FBI, NSA, and International Partners issued Joint Cybersecurity Advisory (AA 22-110A), *Demonstrated Threats and Capabilities of Russian State-Sponsored and Cyber Criminal Actors.*[4]
- June 7, 2022: CISA and NSA released Joint Cybersecurity Advisory (AA22-158A), *People's Republic of China (PRC) State-Sponsored Cyber Actors Exploit Network Providers and Devices,* which identified the use of publicly known vulnerabilities in order to establish a broad network of compromised infrastructure.[5]

To protect against this escalating cybersecurity threat, TSA is preparing to issue SD Pipeline-2021-02C, which would cancel and supersede SD Pipeline-2021-02B. SD Pipeline-2021-02C contains several collections of information that require TSA to amend its currently approved OMB control number 1652-0056, Pipeline Corporate Security Review (PCSR). There is no change to the collection requirements regarding the voluntary Pipeline Corporate Security Review Program (PCSR). TSA is requesting emergency approval for a revision of OMB Control Number 1652-0056 to update the information collection requirements from SD Pipeline-2021-02C.

TSA respectfully requests that OMB grant TSA's request for emergency clearance for a revision to TSA's 1652-0056 Pipeline Security collection in order to address this emergency need to protect transportation security consistent with TSA's responsibilities and authorities. It is imperative that TSA issue this SD as soon as possible to effectuate these goals.

[3] https://www.cisa.gov/uscert/ncas/alerts/aa22-103a
[4] https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
[5] https://www.cisa.gov/uscert/ncas/alerts/aa22-158a