Before the
U.S. Department of Transportation
Pipeline and Hazardous Materials Safety Administration
Office of Pipeline Safety
Washington, D.C.

In the Matter of	)	
	)	CPF No. 3-2022-026-NOPV
Colonial Pipeline Company	)	Notice of Probable Violation
	)	
Respondent.	)	

Request for Hearing, Statement of Issues, and Response to NOPV

I. Introduction

The Pipeline and Hazardous Materials Safety Administration (PHMSA or the Agency) issued a Notice of Probable Violation (NOPV), Proposed Civil Penalty, and Proposed Compliance Order (PCO) to Colonial Pipeline Company (Colonial or the Company) on May 5, 2022. The NOPV alleged seven (7) violations of the control room management (CRM) regulations set forth in 49 C.F.R. § 195.446, proposed a total civil penalty of $986,400 for five (5) of the allegations, and proposed a compliance order associated with six (6) of the allegations. This response is timely.

Colonial is steadfast in its commitment to ensuring public health, environment, and pipeline safety and working with PHMSA toward those goals through the safe operation of its pipeline assets in compliance with the federal pipeline safety regulations. Toward that end, Colonial has cooperated with PHMSA during the two (2) years of CRM inspections on the Colonial pipeline system in 2020 and 2021 as well as during the May 2021 criminal ransomware cyberattack on Colonial's operations, all of which form the basis for the NOPV issued by PHMSA. In keeping with that commitment, Colonial also cooperated with the many other agencies in responding to and investigating the cyberattack, including the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), which is responsible for responding to and facilitating recovery from energy disruptions in collaboration with other parties, and the Federal Bureau of Investigation (FBI).

As part of this overall commitment and pursuant to 49 C.F.R. §§ 190.208 and 190.211, in the event the parties are unable to resolve this matter via an informal conference which Colonial has requested, the Company is filing this response to request an in-person hearing to address the factual and legal issues presented by (1) Items 1, 2, 4, 5, and 7 of the NOPV, (2) the associated proposed civil penalty of $986,400, and (3) the associated PCO obligations. Colonial is, without admission, electing not to contest NOPV Items 3 and 6, including the associated penalty and PCO obligation for Item 3. At a hearing, Colonial will be represented by inhouse counsel as well as outside counsel with Troutman Pepper.

II. Background

Colonial operates the largest pipeline system for refined oil products in the U.S., extending from the coast of Texas to New York, and transporting more than 2.5 million barrels of fuel per day through approximately 5,500 miles of pipeline. As an operator of an interstate transmission hazardous liquid pipeline, Colonial is subject to regulation under the federal Pipeline Safety Act and its implementing regulations, which focus on the safe operation of pipelines to protect the public and the environment. The Company prioritizes pipeline safety and has been recognized for its efforts, most recently as a winner of the 2021 American Petroleum Institute (API) Distinguished Pipeline Safety Awards. API's Pipeline Safety Awards are selected by peers and recognize an operator for its commitment to safety and work to advance a zero incidents culture. As noted by API in its press release, "Colonial Pipeline achieved zero lost-time safety incidents, zero Incidents Impacting People or the Environment (IPE), and added impressive enhancements to its overall [Safety Management System (SMS)] program. SMS enhancements included a robust COVID response program and the expansion of technology to support the company's integrity management around leak detection technologies and opportunities."[1]

Colonial's focus on compliance includes its development and implementation of a written CRM plan pursuant to the Agency's CRM regulations at 49 C.F.R. § 195.446, since their implementation in 2011. The CRM regulations are performance-based, identifying what is required in a CRM plan while providing operators with the discretion to prepare a plan to meet the requirements. PHMSA does not prescribe how pipeline operators should implement the CRM rule and provides minimal guidance for implementation, allowing each operator to effect an approach suitable to its system. PHMSA conducted two (2) rounds of inspections of Colonial's CRM procedures and records over a two (2) year period, first from January 27-November 12, 2020, and again from October 29-November 4, 2021.[2] Although not fully set forth in the Notice or the Pipeline Safety Violation Report (PSVR), these inspections occurred at Colonial locations in Linden, New Jersey; Hebert, Texas; Greensboro, North Carolina; Alpharetta, Georgia; Baton Rouge, Louisiana; Charlotte, North Carolina; and Collins, Mississippi. Due to the COVID-19 pandemic, the majority of the inspections were conducted virtually, which limited the parties' ability to fully engage and relay information and explanations.

While the CRM regulations are performance based, the specifics of an operator's CRM program prepared to implement them are highly technical given the reliance on computer software and the supervisory control and data acquisition (SCADA) systems. PHMSA provided Colonial with its post-inspection written preliminary findings in February 2021 and February 2022, and to Colonial's understanding, the parties were still working through the preliminary findings and relevant clarifications, including with respect to internal communications plans, at the time that the NOPV was issued.

---

[1] API Press Release (May 3, 2022), available at https://www.api.org/news-policy-and-issues/news/2022/05/03/2021-api-distinguished-pipeline-safety-awards.

[2] PHMSA has also previously inspected Colonial's CRM plan since the CRM rules first went into effect, and this is the first time PHMSA has made the allegations set forth in the NOPV.

In the midst of the two (2) year inspection period, on May 7, 2021, Colonial was the victim of a criminal ransomware cybersecurity attack. In response to the discovery of the ransom note, Colonial notified, coordinated and cooperated with government and law enforcement at all levels in initiating a thorough investigation – including the Department of Transportation and PHMSA, the FBI, the U.S. Department of Energy and its CESER Office, the Department of Homeland Security (DHS) and its the Transportation Safety Administration (TSA) and Cybersecurity and Infrastructure Security Agency, the White House, the Federal Energy Regulatory Commission, as well as state and local agencies and third party cybersecurity experts. At the time, it was unclear whether the criminals had only infiltrated the information technology (IT) systems of Colonial or whether the attack had reached the operational technology (OT) systems. Given the uncertainty, Colonial proactively took its OT systems, including the SCADA system, offline as a precautionary measure to ensure safe operations, protect sensitive data, and contain the threat. This included effectuating a complete shutdown of its entire 5,500 mile pipeline system using its SCADA system, following its normal operating procedures, and taking the SCADA system off line, for the first time ever.

Over the next five (5) days, Colonial focused on both (1) the methodical, safe and appropriate process of assessing, containing, and addressing the risks to its IT and OT systems and physical assets; and (2) the safe and efficient restoration of the pipeline system while minimizing disruption to customers. In the first instance, to continue to maintain the safety and integrity of pipeline while offline, Colonial undertook and coordinated extensive efforts to physically inspect and monitor thousands of miles of pipe in a few days' time. In the second instance, and in reliance on its CRM procedures, Colonial prepared an internal communications plan for an incremental process to provide adequate means for a safe return to service in a phased approach, with a manual startup of SCADA lines for operations and deliveries to certain markets beginning just two (2) days after the system was shut down. Colonial initiated a full restart in just five (5) days, beginning on May 12, 2021. The short amount of time it took to restart the pipeline was driven entirely by Colonial's paramount and methodical commitment to public safety, including the Company's IT, OT, and physical assets.

There were no delays associated with Colonial's execution of its restart plan; and any suggestion to the contrary in the NOPV is not factually accurate. Rather, the manual startup and full restart was measured, careful, and thoughtful, in full coordination with multiple layers of government and with a focus on public safety, security, and available product and personnel. To Colonial's credit, the attack did not result in any harm to the pipeline, the public, or the environment. Many federal agencies commented on Colonial's expediency, including PHMSA's Deputy Administrator, who recently stated, "[a]s a result of the close collaboration with PHMSA, within days, the pipeline [Colonial] was able to move nearly a million barrels of fuel on a manual basis."[3]

[3] Remarks of Deputy Administrator (May 3, 2022), available at https://www.phmsa.dot.gov/news/remarks-deputy-administrator-brown-before-american-petroleum-institute-cybernetics-conf.

It is against this backdrop that PHMSA conducted its second round of CRM inspections in October-November 2021 and issued the NOPV. Notably, PHMSA has not issued any regulations related to cybersecurity or preparedness in the event of a cybersecurity attack, and PHMSA has not been authorized by Congress to do so. Instead, DHS holds "lead authority, primary responsibility, and dedicated resources for the protection and resilience of critical infrastructure, as well as the security for all modes of transportation," and DHS has delegated that responsibility to the TSA with whom PHMSA is to coordinate on pipeline security issues.[4] Yet the cybersecurity attack is used to support one of the allegations contained in the NOPV – for which PHMSA is seeking the majority of the proposed civil penalty (i.e., 86%) – and the issuance of the NOPV appeared to coincide with the one year anniversary of the cyberattack. In issuing this allegation, the NOPV applies a novel interpretation of the CRM regulations that operators are required to maintain plans for the manual operation of their systems in the event of cyberattacks.

III. Colonial Written Responses to NOPV Allegations

As set forth below, Colonial believes that PHMSA misconstrued and inaccurately represented many of the facts underlying the NOPV and, further, that PHMSA has not met its burden of proof to support its allegations with respect to Items 1, 2, 4, 5, and 7 of the NOPV, as well as the associated proposed civil penalty of $986,400 and PCO obligations. Colonial strives to continually improve, consistent with the goals of PHMSA and its regulations, and has without admission made a number of improvements during and since the CRM inspections to address PHMSA's concerns.

A. Item 1 (49 C.F.R. § 195.446(a))

1. PHMSA Allegation

> **§ 195.446 Control room management.**
>
> **(a) *General.* This section applies to each operator of a pipeline facility with a controller working in a control room who monitors and controls all or part of a pipeline facility through a SCADA system. Each operator must have and follow written control room management procedures that implement the requirements of this section...The procedure required by this section must be integrated, as appropriate with the operator's written procedures required by §195.402...**
>
> Colonial failed to follow its procedure, ADM-CPC-008 Rev.2 7/1/2019 Point-To-Point Verification, when documenting a point-to-point verification between SCADA displays and related field equipment, per § 195.446(c)(2), for 87 safety related pressure transmitter alarms for the Linden Station in calendar year 2019.
>
> [. . .]

[4] *See* 6 U.S.C. § 101 *et seq.;* Annex to the Memorandum of Understanding between the Department of Homeland Security and the Department of Transportation concerning Transportation Security Administration and Pipeline and Hazardous Materials Safety Administration Cooperation on Pipeline Transportation Security and Safety" (2020); Department of Homeland Security and Department of Transportation, Memorandum of Understanding Between the Department of Homeland Security and the Department of Transportation on Roles and Responsibilities (Sep. 28, 2004).

A review of the Linden 2019 SRA point-to-point records identified 87 records for pressure transmitters where no documentation was entered for as-found/as-left field. This included 19 records for both addition of new equipment and modification of existing equipment which failed to meet the requirement of procedure ADM-CPC-008 Rev.2 7/1/2019 Point -to-Point Verification.

2. Colonial Response

Colonial respectfully requests that this allegation and the associated proposed civil penalty and PCO obligation for Item 1 be withdrawn. Colonial elected to utilize an all-encompassing process to address regulatory requirements for all safety related alarms, devices, and points. This process goes above and beyond the regulatory requirements to ensure accurate information is displayed from field devices to the controller operating a SCADA system. Contrary to the NOPV, the Company conducted point-to-point verification between SCADA displays and related field equipment as required by Colonial procedures, which exceed the requirements of 49 C.F.R. § 195.446(c)(2) given that the annual calibration of pressure transmitters is a preventative maintenance activity. The records – which were available at the time of inspection – document that Colonial did, in fact, conduct the requisite point-to-point verifications between SCADA displays and related field equipment.

Based on the exhibits to PHMSA's PSVR, it appears that the record that Colonial provided to PHMSA during the inspection inadvertently excluded certain supporting data and contained blank cells due to a .pdf conversion error. In addition, with respect to Colonial's procedure ADM-CPC-008 Rev.2 7/1/2019 Point-to-Point Verification, regarding "Pressure Transmitters and Analog Set-Points," PHMSA points out in the NOPV that "[Section 5.5 states:] **NOTE** the as-found value for Point-to Point Verification documentation in SLM" (emphasis in original). Section 5.7 states: "**NOTE** the as-left value for Point-to-Point Verification documentation in SLM form (emphasis in original)." This language was carried over from other sections of the procedure regarding the Company's Safety Life Cycle Management (SLM) system, but it is not applicable to pressure transmitters and analog set-points and, as a result, is not reflected in the documentation. As such, Colonial has since revised the procedure to remove the references to "as-found" and "as-left" values for pressure transmitters and analog set-points.

B. Item 2 (49 C.F.R. § 195.446(a))

1. PHMSA Allegation

§ 195.446 Control room management.

(a) *General.* This section applies to each operator of a pipeline facility with a controller working in a control room who monitors and controls all or part of a pipeline facility through a SCADA system. Each operator must have and follow written control room management procedures that implement the requirements of this section. The procedures required by this section must be integrated, as appropriate, with the operator's written procedures required by §195.402...

Colonial failed to follow their procedures when conducting and documenting point-to-point verifications in SLM for Safety Related Alarms (SRA) to ensure alarms are accurate and support safe pipeline

> operations, per § 195.446(e)(1) and § 195.428(d). A review of 2019 SRA completed tests for Hebert, Linden, Alpharetta, and Greensboro identified either no documentation for as-found as-left conditions (cells were blank), or it was filled in with N/A or NA. These responses were inclusive for the SLM Reasons for the Point-to-Point related to Addition of New Equipment, Preventative Maintenance, and Modification of Existing Equipment.
>
> [. . .]
>
> The records provided by Colonial represent SRA point to point completed in 2019 for Alpharetta, Greensboro, Linden, and Hebert. Dates with time stamps are included in the document of record. The procedure required point-to-point verifications with documentation of the values as-found and as-left. There was no consideration for no entry (blank spaces) or use of NA or N/A. Colonial failed to follow their procedures when conducting and documenting point-to-point verifications in SLM for Safety Related Alarms.

2. Colonial Response

Colonial respectfully requests that Item 2 be withdrawn, along with the proposed penalty and the PCO obligation, and be reissued as a Notice of Amendment (NOA) consistent with PHMSA's Enforcement Procedures manual. Those procedures clarify that a NOA is "used to notify an operator that its plans or procedures required under 49 [C.F.R.] Parts 192, 193, 195, and 199 are 'inadequate' to assure safe operation of a pipeline facility." *PHMSA Enforcement Procedures, Section 3.1.3.1 (Sep. 15, 2020).* Further, most of the enforcement issued to date related to this provision has been issued as NOAs. *See, e.g., Crestwood Dakota Pipeline, LLC, Notice of Amendment, CPF 3-2015-5001M (Mar. 4, 2015)*; *Koch Pipeline Co., L.P., Notice of Amendment, CPF 3-2017-5007M (Sep. 1, 2017).*

Colonial's response to Item 1 clarifies why certain cells may have inadvertently appeared blank. As to cells that noted "NA" or "N/A," the Company did not initially anticipate that the acronyms "NA" or "N/A" would be used by personnel in completing the documentation in Colonial's SLM system for point-to-point verifications of safety-related alarms. For that reason, the Company did not address the use of those terms in its procedures. The Company has updated its procedures to provide the necessary clarification and instruction as to when and how "NA" or "N/A" should be used when conducting and documenting point-to-point verifications in the SLM application for safety related alarms.

C. Item 3 (49 C.F.R. §195.446(a))

1. PHMSA Allegation

> **§ 195.446 Control room management.**
>
> **(a) *General.* This section applies to each operator of a pipeline facility with a controller working in a control room who monitors and controls all or part of a pipeline facility through a SCADA system. Each operator must have and follow written control room management procedures that implement the requirements of this section. . . .**

> Colonial failed to complete and document verifications of alarm set-point and alarm descriptions in compliance with its procedures when associated field instruments were calibrated or changed, as required by § 195.446(e)(3), for 5 safety related points at the Greensboro facility. They also were not able to verify, for the years 2017, 2018, and 2019, all safety-related alarm set-point values and alarm descriptions were correct.
>
> [. . .]
>
> Colonial failed to complete and document verifications of alarm set-point and alarm descriptions when associated field instruments were calibrated or changed for 5 safety related points.

2. Colonial Response

While Colonial without admission does not contest the allegation in Item 3, the allegation requires clarification. PHMSA mischaracterizes the underlying facts as well as Colonial's procedure. Colonial's procedure is more stringent than the regulations because it requires point-to-point verifications for annual equipment calibrations. As noted above, Colonial's CRM procedures exceed the regulatory requirements to ensure accurate information is displayed from field devices to the controller operating a SCADA system. Colonial's point-to-point verification procedures require that any time a safety related device or point is "touched," a point-to-point verification is required and the correct safety-related alarm set-point values and alarm descriptions are verified.

Colonial is confident that these point-to-point verifications were, in fact, conducted. The Company reviewed its alarm management software and is able correlate alarm descriptions of sample safety related points with SCADA data to confirm the verifications were performed. As part of its effort to continually improve, Colonial has been evaluating ways to enhance documentation and recordkeeping, and is implementing additional measures to utilize new reporting metrics (daily/weekly/monthly) to associate maintenance records with point-to-point verifications. These additional processes and procedures are designed to ensure complete documentation of verifications of alarm set-point and alarm descriptions when associated field instruments were calibrated or changed.

D. Item 4 (49 C.F.R. §§ 195.446(a))

1. PHMSA Allegation

> **§ 195.446 Control room management.**
>
> **(a)*General.* This section applies to each operator of a pipeline facility with a controller working in a control room who monitors and controls all or part of a pipeline facility through a SCADA system. Each operator must have and follow written control room management procedures that implement the requirements of this section...**
>
> Colonial pipeline failed to provide a procedure to satisfy the requirements of § 195.446(e)(3) that require verification of the correct safety-related alarm set-point values and alarm descriptions when associated field instruments are calibrated or changed and at least once each calendar year not to exceed 15 months.

[. . .]

The ALM also referenced procedure ADM-CPC-008 Point-to-Point Verification revision 2: 7/1/19 which specifically addressed when point-to-points must be conducted. The procedure did not include the requirement for all points affecting safety to be reviewed or describe a process for the review. This procedure did not reference § 195.446(e)(3), but only provides compliance with § 195.446(c)(2).

2. Colonial Response

Colonial respectfully requests that Item 4 and the associated PCO obligation be withdrawn and disagrees with the mischaracterization that its procedure failed to satisfy the requirements of 49 C.F.R. § 195.446(e)(3). To the contrary, Colonial's procedure *exceeded* the requirements of the regulation by not including "and" following "calibrated or changed" and before "at least once each calendar year." Nevertheless, Colonial has already revised the procedure to address PHMSA's concern.

PHMSA should more appropriately have issued this NOPV item as a NOA, consistent with PHMSA's Enforcement Procedures manual, which clarifies that a NOA is "used to notify an operator that its plans or procedures required under 49 [C.F.R.] Parts 192, 193, 195, and 199 are 'inadequate' to assure safe operation of a pipeline facility." *PHMSA Enforcement Procedures, Section 3.1.3.1 (Sep. 15, 2020).* Further, and as noted above, most of the enforcement issued to date related to this provision has been issued as NOAs. *See, e.g., Crestwood Dakota Pipeline, LLC, Notice of Amendment, CPF 3-2015-5001M (Mar. 4, 2015); UCAR Pipeline Incorporated, Notice of Amendment, CPF 4-2012-1014M (Jun. 26, 2012); Dow Pipeline Co., Notice of Amendment, CPF 4-2012-5024M (Jun. 26, 2012).*

E. Item 5 (49 C.F.R. § 195.446(c)(3))

1. PHMSA Allegation

§ 195.446 Control room management.

> **(c) *Provide adequate information.* Each operator must provide its controllers with the information, tools, processes and procedures necessary for the controllers to carry out the roles and responsibilities the operator has defined by performing each of the following:**
> **(1)...**
> **(3) Test and verify an internal communication plan to provide adequate means for manual operation of the pipeline safely, at least once each calendar year, but at intervals not to exceed 15 months;**

Colonial failed to test and verify its internal communication plan to provide adequate means for manual operation of the pipeline at Linden and Hebert in 2017, 2018, and 2019, at Greensboro in 2018 and 2019, Alpharetta in 2017, Baton Rouge, Collins and Charlotte in 2018, 2019, 2020.

[. . .]

Respondent's failure to test and verify its internal communication plan contributed to consequences that

occurred when, on May 7, 2021, Colonial Pipeline was the victim of a cyber-attack which required the immediate shutdown of the entire pipeline system. After evaluating operating characteristics/limitations throughout the system, as well as societal impact, Colonial identified several main and stub lines for manual restart prioritization and began developing Line/Segment-specific procedures for manual operation. On May 9, 2021, the first of several incremental and segregated restarts of various pipeline segments commenced, with a full system restart achieved on May 12, 2021. The pipeline shutdown impacted numerous refineries' ability to move refined product, and supply shortages created wide-spread societal impacts long after the restart. Since Respondent had not tested and verified an internal communication plan when the cyber-attack occurred, as was required by the regulation, Respondent was not prepared for manual restart and manual operation of its pipeline. Colonial Pipeline's ad-hoc approach toward consideration of a "manual restart" created the potential for increased risks to the pipeline's integrity as well as additional delays in restart, exacerbating the supply issues and societal impacts.

2. Colonial Response

Colonial contests Item 5, the associated proposed civil penalty, and PCO obligation. The regulations at 49 C.F.R. § 195.446(c)(3) require operators to "test and verify an internal communication plan to provide adequate means for manual operation of the pipeline safely, at least once each calendar year, but at intervals not to exceed 15 months." In enforcement and guidance, PHMSA has clarified that the required plans and procedures "must be commensurate with the level of operational performance *intended* by the operator to be maintained while in manual mode." *PHMSA Control Room Management: Inspection Questions (March 1, 2012)* (emphasis added).

More to the point, PHMSA specifically advises that

> If an operator does not intend to continue operating the pipeline in the event of a catastrophic SCADA failure, then only procedures to safely perform a controlled shutdown and maintain and monitor pipeline integrity need to be in place. If an operator chooses to continue all, or partial, pipeline operations in the event of a catastrophic SCADA failure, the rule requires that operators have some reliable means to monitor and operate the pipeline system manually.

PHMSA Control Room Management Frequently Asked Questions (FAQs), FAQ C.09, (Jan. 16, 2018) (emphasis added). As such, an operator is only required to develop an internal communication plan to provide for an adequate means to manually operate its system *if* the operator plans on manually operating its system after a catastrophic SCADA failure. *Id.; see also Buckeye Partners, LP, Notice of Amendment , CPF 1-2014-5001M (Apr. 2, 2014)* ("If, Buckeye does not intend to operate in a manual mode then that should be addressed in the Control Room Management Plan and a basic plan should be included as well."). Further, there is nothing in PHMSA's regulations, enforcement, or guidance, that suggests a system or corporate-wide internal communications plan must be tested and verified in every control room.

Consistent with the plain language of 49 C.F.R. § 195.446(c)(3) and PHMSA's longstanding interpretation, guidance, and application of it, Colonial maintained a procedure for the controlled shutdown of its system in the event of a catastrophic SCADA system failure, which included provisions for maintaining and monitoring of pipeline integrity. Colonial's processes and procedures further provided that if the Company elected to manually operate its system in the event

of a SCADA failure, the Company would develop an internal communication plan for manual operation. As required by the regulation and consistent with its procedure, Colonial tested and verified the communication plan annually, not to exceed fifteen (15) months, through actual events throughout its system where the Company prepared internal communications plans for manual operations following a shutdown which allowed Colonial to validate the plans. *Colonial "OLT Policy for Manual Operation of a Pipeline System" and "Control Room Management Plan - Internal Communication Plan for Manual Operation."* This process allows the Company to assess the unique circumstances related to any failure or shutdown of its SCADA system to determine whether to continue manually operating its system and, if the Company elects to manually operate its system, to develop an internal communication plan accounting for those circumstances.

The need for flexibility in reacting to either a SCADA system failure or shutdown is paramount due to the complexity of Colonial's pipeline system which transports a variety of different products. The largest and one of the most complicated refined products pipeline system in the U.S., Colonial's pipeline system consists of 5,500 miles of pipeline which carries more than 2.5 million barrels of fuel per day between Texas and New York. The pipeline consists of four (4) main lines, two (2) of which primarily transport gasoline products and the other two (2) which transport a variety of distillate products, as well as a number of lateral pipelines (thirty-three (33) in total). In total, the system transports more than *eighty six (86) different types of products*, approximately twenty (20) of which are transported regularly, which are generally batched in five (5) day cycles, with a mix of products and grades depending on market demand. Further, the ability to run any portion of the system manually at any given point in time depends on a number of factors, including availability of product and personnel as well as safety considerations.

In this instance, Colonial was the victim of an unprecedented criminal ransomware cybersecurity attack. Shortly after discovery of the ransom note, the Company voluntarily and proactively shut down the entire 5,500 miles of pipeline system and the SCADA system, following its controlled shutdown procedures, in an abundance of caution to ensure the ongoing safety of the public and of those systems. It was not known whether the criminals infiltrated just Colonial's IT systems or whether the attack extended to the Company's OT systems. As such, taking those systems, including SCADA, offline was critical to containing the threat and limiting impacts to the public and the environment. This was the first time that Colonial has ever fully shut down the entire pipeline system in this manner, using SCADA and taking the SCADA system off line.

Colonial then proceeded, in coordination with PHMSA and other federal, state, and local agencies, to undertake and coordinate extraordinary efforts to (1) physically inspect and monitor thousands of miles of pipe over a several day period in order to maintain the safety and integrity of the system while it was offline, and (2) methodically assess, contain and address the risks to its IT and OT systems and physical assets. Further, and consistent with its procedures and PHMSA regulations, Colonial then developed and implemented an internal communication plan for the manual operation of its system through use of Management of Change (MOC) processes to assess and prepare for a safe manual restart. By developing this internal communication plan for the manual operation of its system at this time, Colonial was able to tailor its plan to address and carefully consider the unique circumstances presented by the cyberattack. All of this activity notwithstanding, within just two (2) days of the system being shut down, Colonial was able to

initiate manual operations where possible. The full restart, which was followed by manual operations, was initiated in just five (5) days.

The response to the cybersecurity attack was an extraordinary and well-organized undertaking by the Company, aided by experts, governmental agencies, including PHMSA, and public officials. There was no delay, despite PHMSA's suggestions to the contrary. Considering the circumstances, particularly the unprecedented nature of the event and the size and complexity of Colonial's pipeline system, it is remarkable that it took Colonial only *five (5) days* to initiate a full restart the pipeline, from the identification of the cyberattack on May 7, 2021, to the commencement of restart on May 12, 2021, in accordance with CRM regulations and Colonial's procedures. Throughout this entire process, Colonial maintained its commitment to safety and developed a plan for the manual restart of its system in consideration of the complexities of the cyberattack.

Notably, PHMSA has not issued any regulations related to cybersecurity or preparedness in the event of a cybersecurity attack and PHMSA has not been authorized by Congress to do so. DHS holds lead authority and primary responsibility for the protection of critical infrastructure, and the security for all modes of transportation; DHS has delegated that responsibility to the TSA with whom PHMSA is to coordinate on pipeline security. Yet PHMSA relies on the cybersecurity attack to support its allegations in Item 5 and the associated proposed civil penalty, which represents the vast majority of the entire NOPV penalty (i.e., $846,300 out of a total penalty of $986,400).

For all of these reasons, including Colonial's compliance with the requirements of 49 C.F.R. § 195.446(c)(3), the Company requests that PHMSA withdraw this NOPV Item, associated proposed civil penalty, and PCO obligation. Alternatively, and at a minimum, the civil penalty should be significantly reduced given that there was no "deliberate decision not to comply with the applicable requirement" as asserted by PHMSA in the civil penalty worksheet. Colonial disputes this representation given that it carefully designed its CRM processes and procedures to comply with 49 C.F.R. § 195.446(c)(3) as clarified by PHMSA guidance and enforcement. PHMSA itself has inspected Colonial's CRM plan and procedures several times beginning in 2013 and yet has never questioned Colonial's approach until now.

F. Item 6 (49 C.F.R. § 195.446(c)(4))

1. PHMSA Allegation

§ 195.446 Control room management.

(c) Provide adequate equipment. **Each operator must provide its controllers with the information, tools, processes and procedures necessary for the controllers to carry out the roles and responsibilities the operator has defined by preforming each of the following:**

(1)...

(4) Test any backup SCADA systems at least once each calendar year, but at intervals not to exceed 15 months;

Colonial failed to test the SCADA backup servers at the Linden, Hebert, and Greensboro field operations control rooms at least once each calendar year, but at intervals not to exceed 15 months, for the years 2017, 2018, and 2019, in compliance with its operating procedures and § 195.446(c)(4). [. . .]

After PHMSA inspectors identified this issue, Colonial developed procedures and performed tests of their servers to meet the requirements of this section.

2. Colonial Response

Without admission, Colonial does not contest NOPV Item 6. As noted by PHMSA in the NOPV and as part of the Company's efforts to continually improve, Colonial developed new procedures following the identification of this issue in January 2020 for backup server testing. Colonial implemented the new procedure and process for testing the server backup of the SCADA system beginning in July 2020, to satisfy its obligations under 49 C.F.R. § 195.446(c)(4). Colonial devoted substantial resources to developing and implementing the updated procedure and completed testing of all field control rooms across the entire system by the end of 2020. Records of the testing are available for review.

G. Item 7 (49 C.F.R. § 195.446(e)(2))

1. PHMSA Allegation

§ 195.446 Control room management.

(e) *Alarm management.* Each operator using a SCADA system must have a written alarm management plan to provide for effective controller response to alarms. An operator's plan must include provisions to:

(1) . . . .

(2) Identify at least once each calendar month points affecting safety that have been taken off scan in the SCADA host, have had alarms inhibited, generated false alarms, or that have had forced or manual values for periods of time exceeding that required for associated maintenance or operating activities;

Colonial for Greensboro, Hebert and Linden failed to identify and record, at least monthly, all points affecting safety that had been taken off scan in the SCADA host; all points that have had alarms inhibited; or that have had forced or manual values for periods of time exceeding that required for associated maintenance or operating activities, per § 195.446(e)(2), for the years 2017, 2018 and 2019. [. . .]

There was no attempt to review the SCADA logs or SharePoint log monthly, as evidence by the lack of records. There were no records to evidence any monthly review for points off scan, point that have had alarms inhibited, or that have had forced or manual values for period of time exceeding that required for associated maintenance or operating activities.

2. Colonial Response

Colonial requests that this NOPV Item 7, associated civil penalty, and PCO obligation, be withdrawn. PHMSA alleges that there was no attempt by Colonial to review the SCADA logs or SharePoint log on a monthly basis. The regulation at 49 C.F.R. § 195.446(e)(2) requires that the Company identify at least once every calendar month instances where points affecting safety have been taken off scan in the SCADA host, have had alarms inhibited, generated false alarms, or that

have had forced or manual values for periods of time exceeding that required for associated maintenance or operating activities.

Colonial has had a process in place to document points which were disabled or taken out of service, in its Disabled Safety Device / Point Tracking Log. Where no such conditions occurred in a given month, there was no documentation or events to be reviewed or recorded. In other words, the very lack of records in this instance demonstrates Colonial's compliance, as well as the effectiveness of its CRM program. To address PHMSA's concerns and without admission, on a going forward basis, Colonial will include an entry in its documentation to account for those months where no conditions have occurred in that month.

IV. Statement of Issues

A. Whether based on the facts and applicable law, PHMSA has met its burden to prove by a preponderance of the evidence that Colonial did not comply with 49 C.F.R. § 195.446 for NOPV Items 1, 2, 4, 5, and 7.

B. Whether PHMSA provided due process and fair notice, as required by the U.S. Constitution and the Administrative Procedure Act, in issuing alleged violations of 49 C.F.R. § 195.466 for NOPV Items 1, 2, 4, 5, and 7 based on the facts and the applicable law.

C. Whether PHMSA's allegations of noncompliance are arbitrary and capricious, an abuse of discretion, or otherwise not in accordance with law in violation of the Administrative Procedure Act, 5 U.S.C. § 706(2), constitute disparate treatment of similarly situated parties without reasoned explanation and substantial evidence in the record.

D. Whether there is any basis in the 49 C.F.R. Part 195 regulations for PHMSA to require that operators plan for the manual operation of a pipeline.

E. Whether the Pipeline Safety Act, 49 U.S.C. § 60101 et seq., authorizes a finding of liability simply because a cybersecurity attack occurred.

F. Whether PHMSA has a reasonable basis for its statement in NOPV Item 5 that "Colonial Pipeline's ad-hoc approach toward consideration of a 'manual restart' created the potential for increased risks to the pipeline's integrity as well as additional delays in restart, exacerbating the supply issues and societal impacts."

G. Whether the proposed civil penalty of $986,400 associated with NOPV Items 1, 2, 5, and 7 should be withdrawn or reduced to accurately reflect the statutory and regulatory penalty assessment criteria required under 49 U.S.C. § 60122(b) and 49 C.F.R. § 190.225 and to align with penalties issued in prior relevant PHMSA enforcement.

H. Whether the NOPV, proposed civil penalty, and PCO contradict PHMSA's Pipeline Safety Enforcement Procedures with respect to fair and consistent enforcement.

I. Whether the terms and timeframes of the PCO obligations for Items 1, 2, 4, 5, and 7 are necessary or reasonable or consistent with PHMSA's Pipeline Safety Enforcement Procedures.

V. Summary and Request for Relief

Colonial takes it commitment to pipeline safety seriously. For all of the reasons identified above, and in consideration of other matters as justice may require, Colonial respectfully requests that NOPV Items 1, 2, 4, 5, and 7 be withdrawn, along with the associated PCO items, and that the associated proposed penalties be withdrawn or significantly reduced. Colonial takes particular exception at the suggestion that there was any delay in the Company's response to the cyberattack and to PHMSA's reliance on the cyberattack to exponentially increase the proposed civil penalty. In advance of the requested hearing, and pursuant to 49 C.F.R. § 190.209, Colonial requests a copy of the complete case file in this matter to the extent there are any documents in addition to the PSVR, related exhibits, and the Proposed Civil Penalty Calculation Worksheet which have already been provided to Colonial upon its previous request.

Respectfully submitted,

Troutman Pepper, LLP
Catherine Little, Esq.
Annie Cook, Esq.
600 Peachtree Street NE, Suite 3000
Atlanta, GA 30308
(404) 885-3000
Catherine.Little@troutman.com
Annie.Cook@troutman.com

Counsel for Colonial Pipeline Company

Date: June 6, 2022