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.	)	
	)	

PRE-HEARING BRIEF

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. A single allegation is the basis for the vast majority of the proposed civil penalty for this entire enforcement action: NOPV Item 5 with a proposed civil penalty of $846,300. Notably, PHMSA has only *ever* levied one (1) other proposed civil penalty for an alleged violation of the same provision and it was substantially lower, amounting to less than 3% of the penalty proposed to be assessed to Colonial.

On June 8, 2022, Colonial requested an in-person hearing and the opportunity to convene informal settlement meetings with PHMSA in an effort to resolve this matter in lieu of a hearing. PHMSA scheduled a hearing for October 11, 2022, with an initial due date of October 3, 2022 for submission of pre-hearing materials which was extended by agreement of the parties to October 6, 2022. Through the informal settlement meetings, Colonial has reached an agreement with PHMSA to resolve all issues presented by the NOPV, without admission, with the exception of NOPV Item 5. As such, Colonial is timely filing this pre-hearing brief and relevant supporting documents contesting NOPV Item 5 along with the associated proposed civil penalty and the PCO requirement.[1]

Colonial operates the largest pipeline system for refined oil products in the U.S., consisting of approximately 5,500 miles of pipeline, extending from the coast of Texas to New York. Colonial's system carries more than 2.5 million barrels of fuel per day and plays a key role in the nation's energy supply and provides nearly half of the fuel for the East Coast, including home heating oil, gasoline, aviation fuel, and other refined petroleum products. Colonial understands the significance of the markets it serves, and most importantly, Colonial prioritizes safety in every respect of its culture and its operating responsibilities. The Company embraces a safety-first culture, focused on protecting people, the environment, and the pipeline system itself.

Colonial's commitment to compliance with the federal pipeline safety regulations and continual improvement of its programs, includes implementation of a robust CRM program under 49 C.F.R. § 195.446. An element of the CRM program which is the subject of NOPV Item 5 and this pre-hearing brief is the obligation 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." 49 C.F.R. § 195.446(c)(3) (emphasis added). PHMSA alleges that Colonial has in certain instances failed to prepare, test, and verify a "compliant plan."

[1] Subsequent to the issuance of this NOPV but arising out of the same inspection, PHMSA issued on May 27, 2022, a Notice of Amendment (CPF No. 3-2022-028-NOA) and Warning Letter (CPF No. 3-2022-027WL) both of which alleged issues overlapping with the NOPV and the PCO. In particular, Item 5 of the Notice of Amendment is based on the same facts and legal conclusions as Item 5 of the NOPV and the parties have agreed that the resolution of this Hearing will resolve both Item 5 of the NOPV as well as Item 5 of the Notice of Amendment. *See* Exh. 1, *In re: Colonial Pipeline Co.*, Notice of Amendment, CPF 3-2022-028-NOA at 4-5 (May 27, 2022); Exh. 2, *Colonial Pipeline Co.*, Response to Notice of Amendment at 6-7 (Jun. 27, 2022).

The allegation put forth by PHMSA as the basis for NOPV Item 5 misapplies the applicable law, however, and ignores the relevant facts. The allegation presents as an apparent attempt by the Agency to expand its regulatory reach under the CRM regulations, and, in the process, relies upon a misunderstanding of the facts regarding a May 2021 criminal ransomware cyberattack on Colonial's operations. As such, PHMSA has not met its burden of proof to establish the violation as alleged within NOPV Item 5 as a matter of fact and law. For the reasons set forth below, Colonial requests that PHMSA withdraw NOPV Item 5, the proposed civil penalty, and the associated PCO obligation. In the alternative, Colonial believes that the proposed civil penalty should be substantially reduced.

II. Relevant Factual Background

A. Colonial's CRM Plan and PHMSA Inspections

Consistent with Colonial's focus on compliance, the Company developed a comprehensive written CRM Plan pursuant to the Agency's CRM regulations at 49 C.F.R. § 195.446. Final Rule, *Pipeline Safety: Control Room Management/Human Factors,* 74 Fed. Reg. 63310 (Dec. 3, 2009). At the outset, Colonial's CRM Plan included a provision to address the internal communication plan requirement at 49 C.F.R. § 195.446(c)(3):

> *Testing and verification of internal communications* and manual operations procedures for a controlled shutdown of the pipeline(s) in the event of a loss of SCADA and/or voice communications *shall be conducted at least each calendar year, not to exceed (15) months*.
>
> Due to the complexity of CPC's operations system and rarity of such events, CPC does not have a *specific* internal communication plan *for manual operation* and *will not operate a line or system manually without prior implementation of an internal communication plan*.

Exh. 3, Colonial Pipeline, Co., *Excerpt (pp. 25-26) of CRM Plan, Testing of Internal Communication Plan for Manual Operation, Revision 12.0* at 25 (Jan. 15, 2020) (emphasis added)*; see also* Exh. 4, Colonial Pipeline, Co., *Excerpt (pp. 26-27) of CRM Plan, Testing of Internal Communication Plan for Manual Operation, Revision 13.0* at 26 (Jul. 2, 2020).[2] Colonial's procedures, therefore, required regular testing and verification of internal communications and manual operations procedures for a controlled shutdown. Exh. 3 at 25-26; Exh. 4 at 26-27 (which details the internal communication plan criteria and process to be used in the test).

Consistent with the text of the regulation and longstanding guidance from PHMSA interpreting it, this provision further evidenced Colonial's intent not to operate its system manually and, as such, the Company was required to maintain specific procedures to safely perform a controlled shutdown of its system and to maintain and monitor its integrity. The reference to complexity of Colonial's

[2] During the course of the PHMSA inspection, Colonial finalized an update to its CRM plan and provided PHMSA with the most recent updated version on July 2, 2022. Colonial's procedural requirements at issue did not change during this time.

system and the need for a specific internal communication plan for manual operation refers to the complexity of the system with respect to conducting manual operations. As with many large pipeline operators, the plan for manual operations following a communications outage or other emergency event will have a number of variables depending upon the extent of the event, the locations at issue, etc. There is no "one size fits all" approach for manual operations under these circumstances and thus Colonial develops event-specific manual operations procedures when necessary. The internal communication plan, in contrast, consists of the criteria set forth in the CRM Plan. When an event occurs in which manual operations are necessary, Colonial develops specific manual operations procedures which are implemented in a Management of Change (MOC) notice which includes the internal communication plan in accordance with the Company's CRM Plan requirements.

This approach, which is supported by a plain reading of the regulations and PHMSA guidance, was driven entirely by Colonial's ultimate goal to maintain safe pipeline operations. As anticipated by PHMSA in promulgating its performance-based regulations, there has always been a need for a flexible approach when or if manual operations can be safely performed by properly accounting for all safety concerns in response to an emergency (i.e., a cyberattack). Recognizing these challenges, Colonial went several steps further than the regulations and prior PHMSA guidance,[3] by committing to prepare an internal communication plan in the event it did proceed with manual operations and outlining numerous criteria for inclusion in the communication process that would be tested. Exh. 3 at 26; Exh. 4 at 27. This safety-first approach is consistent with PHMSA's performance-based regulations that provide operators with appropriate discretion.

Testing and verifications of Colonial's internal communication plans were timely performed under the Company's CRM Plan through actual events, which PHMSA has acknowledged as an acceptable process.[4] In each event in which Colonial tested and verified its internal communication plan, the Company implemented a MOC which included the internal communication plan in accordance with the CRM Plan requirements and event-specific manual operating procedures. The MOCs were communicated to personnel as required reading for personnel sign-off and acknowledgement.

PHMSA inspected Colonial's CRM Plan – including these very provisions – numerous times since the CRM regulations went into effect in 2011. According to PHMSA's website, the Agency has inspected Colonial's CRM eighteen (18) times, twelve (12) of which occurred prior to 2020.[5] Those twelve (12) inspections included a specific review of these same procedures which PHMSA now questions in NOPV Item 5 without ever having previously raised or identified alleged deficiencies or recommendations for improvement.

[3] Infra Section III. Applicable Law: Testing and Verification of Internal Communication Plan.

[4] Infra note 14.

[5] Exh. 5, PHMSA Control Room Management Inspection History of Colonial Pipeline Company; information publicly available at https://primis.phmsa.dot.gov/comm/reports/operator/OperatorIE_opid_2552.html?nocache=323#_Outer Panel_tab_2 (last accessed on Oct. 6, 2022).

With respect to the inspections which resulted in the matter in dispute, they occurred over a two (2) year period, from January 27 – November 12, 2020, and October 29 – November 4, 2021.[6] Following the first inspection in 2020, Colonial was the victim of a criminal ransomware cybersecurity attack on May 7, 2021. It is against this backdrop that PHMSA conducted its second round of CRM inspections in October – November 2021 and issued the underlying NOPV. Surprisingly, however, particularly given PHMSA's sweeping commentary regarding the cyberattack in the narrative allegations of NOPV Item 5, the Agency did not make any inquiries whatsoever regarding the Company's response to the cyberattack during its second round inspection, including whether the alleged lack of an internal communication plan in any way delayed the manual operations or the ultimate restart of the entire system.[7]

B. Colonial's Internal Communication Plan Implementation and Manual Restart in Response to the Cyberattack

In response to the discovery of a ransom note and potential cybersecurity threat on May 7, 2021, Colonial notified, coordinated, and cooperated with government agencies and law enforcement at all levels and hired third party cybersecurity experts to initiate a thorough investigation of and response to the threat. At the outset of the cyberattack, it was unclear whether the criminals had only infiltrated the Company's information technology (IT) systems or whether the attack had reached the operational technology (OT) systems as well. Given the uncertainty, Colonial proactively took its OT systems, including the supervisory control and data acquisition (SCADA) system, offline as a precautionary measure to ensure safe operations, protect sensitive data, and contain the threat.[8] This included effectuating a complete shutdown of its entire 5,500 mile pipeline system using its SCADA system, following its normal operating procedures for a controlled shutdown, and electing – for the first time ever – to take the SCADA system off line.

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. 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. While verifying the integrity of its system, and in reliance on its CRM

[6] Although not fully set forth in the NOPV or the Pipeline Safety Violation Report (PSVR) prepared by PHMSA, these inspections occurred at seven (7) Colonial locations across its system, most of which were conducted virtually because of the COVID-19 pandemic.

[7] The NOPV, issued near the one (1) year anniversary of the cyberattack, confirms that PHMSA relies heavily on the cyberattack in setting forth the allegations for Item 5, including conclusory statements such as *"*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." Notice of Probable Violation, CPF 3-2022-026-NOPV at 7.

[8] PHMSA incorrectly states in the NOPV that the cyberattack "required the immediate shutdown of the entire pipeline system." *Id.* In actuality, Colonial voluntarily shut down the pipeline under its "stop work authority" philosophy in order to assess the situation and, most importantly, make certain that people, the environment, and the assets are protected. This proactive approach, including the as is the methodical manner in which Colonial protected and ultimately restarted the pipeline, is consistent with what a responsible and safe operator should do in response to an emergency.

procedures, Colonial prepared a specific internal communication plan, the established framework for which had regularly been tested and verified at other locations in response to unrelated actual events (see Table 1.0 below and associated attachments).

To be clear, there was no delay in instituting manual operations or any restart of Colonial's pipeline system, whether due to an alleged lack of or delay in implementing a communication plan. To the contrary, all lead items in response to the manual shutdown of the pipeline were focused on confirming the extent of the cyberattack, containing and remediating that threat, protecting the pipeline while it was idled, and otherwise confirming that the Company could safely restore operations as prudently and expeditiously as possible. Safe operations drove all of those decisions. As Colonial assumes was intended by the regulation, the internal communication plan along with Colonial's restart plan provided the means for the Company to employ a phased approach to safely return its system to service, 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 and OT systems and physical assets.

Again, there were simply no delays associated with Colonial's implementation of an internal communication plan for the restart of its system. Further, Colonial's implementation of an internal communication plan associated with those operations was neither "ad hoc" nor did it "contribute to consequences" associated with the cyberattack; suggestions to the contrary in the NOPV are not factually accurate. The manual startup and full restart were measured, careful, and thoughtful, in full coordination with Company procedures, multiple layers of government engagement, and with a focus on public safety and security.

To Colonial's credit, the cyberattack did not result in any harm to the pipeline, the public, or the environment. No releases to the environment or any other incident occurred during the response. Further, many federal agencies commented on Colonial's expediency, including PHMSA's Deputy Administrator, who publicly acknowledged Colonial's coordination with PHMSA and stated on social media avenues on May 3, 2022 that, "[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."[9] This contrasts with the allegations in NOPV Item 5 as well as the associated press release issued by PHMSA just days later on May 5, 2022, stating that, "[t]he NOPV alleges that failures to adequately plan and prepare for a manual restart and shutdown operation contributed to the national impacts when the pipeline remained out of service after the May 2021 cyber-attack."[10]

[9] Exh. 6, PHMSA, "*Remarks of Deputy Administrator Tristan Brown Before the American Petroleum Institute Control Room and Cybernetics Conference*" (May 3, 2022), available at https://www.phmsa.dot.gov/news/remarks-deputy-administrator-brown-before-american-petroleum-institute-cybernetics-conf.

[10] Exh. 7, PHMSA Press Release, PHMSA 03-22, "*PHMSA Issues Proposed Civil Penalty of Nearly $1 Million to Colonial Pipeline Company for Control Room Management Failures*" (May 5, 2022), available at https://www.phmsa.dot.gov/news/phmsa-issues-proposed-civil-penalty-nearly-1-million-colonial-pipeline-company-control-room.

C. Colonial CRM Continual Improvements

In an effort to continually improve, Colonial has without admission made a number of enhancements during and since the underlying CRM inspections to address PHMSA's concerns. Prior to issuance of the PHMSA NOPV and since, Colonial implemented various recommendations for improvement, exchanged documentation with PHMSA, and convened numerous meetings to discuss and solicit feedback on updated procedures and processes. Colonial has also identified lessons learned from the May 2021 cyberattack and continues to work to incorporate those learnings into relevant procedures and processes.

Specific to the internal communication plan obligation and prior to PHMSA's issuance of the NOPV in May 2022, Colonial attempted to work with PHMSA on updates to the Company's internal communication plan approach. In response to feedback during the inspection, which was initiated by the Southern Region, Colonial prepared and submitted a draft internal communication plan to the PHMSA Southern Region for review in January 2022. Colonial also participated in a subsequent meeting with PHMSA Southern Region in March 2022 to discuss the draft internal communication plan and the associated test and verify framework. The PHMSA Southern Region indicated during this call that the inspection had been transferred to the Central Region and the Southern Region would not be providing further feedback.

Just after issuance of the NOPV, Colonial performed a previously scheduled testing and verification internal communication plan exercise at its Woodbury facility on June 6 – 9, 2022. During a July meeting, Colonial provided relevant documentation to the PHMSA Central Region, including prior testing and verification of its plans and the revised draft internal communication plan. In September 2022, Colonial met again with PHMSA Central Region to discuss proposed internal communication plan exercises and potential additional test measures. Testing and verification exercises were performed later in September 2022 for Lake Charles, Hebert and PAPS, with a tie-in to the Alpharetta Control Center. Additional internal communication plan exercises at various facilities are scheduled this year in October, November, and December.

III. Applicable Law: Testing and Verification of Internal Communication Plan

The CRM regulations are performance-based, identifying minimum requirements in a CRM Plan while providing operators with the discretion to prepare a plan to meet or exceed the requirements in a manner suitable to their systems. PHMSA does not prescribe how pipeline operators should implement the CRM rule and provides only minimal guidance for implementation. In relevant part, the CRM regulation at issue, 49 C.F.R. § 195.446(c)(3), requires 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." (emphasis added).

There is virtually no discussion of this regulation in the rulemaking history. The requirement is plainly worded, requiring an internal communication plan that provides adequate means for manual operations of a pipeline, i.e., *if* an operator elects to manually operate. It requires a communication plan, not a manual operations plan. In subsequent guidance and enforcement, PHMSA clarified that the requisite internal communication plans and procedures "must be

commensurate with the level of operational performance *intended* by the operator to be maintained while in manual mode." Exh. 8, *PHMSA Control Room Management Inspection Form* at 22 (Mar. 1, 2012). Put another way, PHMSA recognizes the need for flexibility in its performance-based rules to allow operators the ability to react appropriately to a SCADA system failure or other disruption on their system. PHMSA specifically advises operators in longstanding FAQ guidance 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.

Exh. 9, *PHMSA Control Room Management Frequently Asked Questions (FAQs),* FAQ C.09, dated Jun. 17, 2011 (Jan. 16, 2018) (emphasis added).

Accordingly, an operator is only required, under the current regulations and related PHMSA guidance, 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* Exh. 10 , *In re: 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."); Exh. 11, *In re: IMTT-Pipeline,* Notice of Amendment, CPF 1-2015-5020M (Nov. 19, 2015) ("if IMMT does not intend to operate in manual mode, then that should be addressed in the CRMP, and a basic plan that describes an orderly shutdown should be included in the CRMP."). More recent enforcement issued in 2021 and 2022 reflects both an increase in PHMSA citing operators for failure to have an internal communication plan and the fact that the regulated community's understanding of the requirement differs significantly from that of PHMSA.[11] In addition, there is no substantive direction or guidance of relevance proffered in those enforcement actions, the vast majority of which were issued as Notices of Amendment or Warning Letters.[12]

The scope of an internal communication plan is also more limited than PHMSA suggests in this enforcement action. There is no mention whatsoever in PHMSA's regulations, enforcement, or

[11] For example, in *In re: Olympic Pipeline Co.,* Notice of Probable Violation, CPF 5-2021-024-NOPV (Jun. 11, 2021), PHMSA found that the operator could not produce documentation to demonstrate that it had tested an internal communication plan at required intervals or that its procedures required such testing. In response, the operator conceded that it did not conduct testing of its loss of communication plan because "[i]n the event of a system-wide SCADA and/or communications failure, [it] will initiate an emergency shut down of the system and will not operate the system." This action shows that industry has interpreted the regulatory requirement at 49 C.F.R. § 195.446(c)(3) differently than PHMSA's recent interpretation of this provision.

[12] *See, e.g.*, *In re: Enbridge Energy, LP*, Notice of Amendment, CPF 3-2022-015-NOA (Jan. 7, 2022) (finding that the operator's procedures for testing and verifying an internal communication plan "did not include any actual or mock exercise in shutting down or manual operation of the pipeline"); *see also In re: Freeport-McMoRan Oil & Gas*, Notice of Amendment, CPF 5-2021-043-NOA (Aug. 2, 2021); *In re: Exxon Mobile*, Notice of Amendment, CPF 3-2021-026-NOA (Apr. 8, 2021).

guidance, that suggests a system or corporate-wide internal communication plan must be tested and verified in each and every control room. Without support in prior enforcement or guidance, PHMSA now alleges that the plan must be tested and verified at each control room location across a pipeline system. In a PHMSA FAQ that addresses the testing and verification of an internal communication plan for manual operation, PHMSA is silent on the issue, describing the intent of the obligation as follows:

> The intent of this requirement is that operators perform exercises or drills to assure that communication plans will be effective during an actual emergency involving loss of all SCADA system functions or other systems relying on SCADA data such as leak detection. Functions that must be verified during testing include, but are not limited to, (1) communication between and among operational and maintenance personnel using voice, fax, messaging, radio, etc., and (2) communication of pipeline operational data such as dial-in polling of field equipment, manually reading gauges and field instrumentation, etc. Note that equipment and modes of communication that are likely to be inoperable during a manual operation scenario should not be used during the test.

Exh. 9, PHMSA Control *Room Management FAQs,* FAQ C.07, dated Jun. 17, 2011 (Jan. 16, 2018) (emphasis added).

Further, PHMSA used the cybersecurity attack to bolster its allegations in NOPV Item 5 and the associated excessive proposed civil penalty and corresponding press release. Yet, PHMSA has not issued any regulations related to cybersecurity or preparedness in the event of a cybersecurity attack nor has PHMSA been authorized by Congress to do so. The Department of Homeland Security (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 Transportation Security Administration (TSA) with whom PHMSA is directed to coordinate on pipeline security issues.[13]
.

IV. NOPV Item 5 Should be Withdrawn as a Matter of Fact and Law

Colonial believes that NOPV Item 5 should be withdrawn as a matter of fact and law. In PHMSA's framing of this allegation in the NOPV, the Agency applies a novel interpretation of 49 C.F.R. § 195.446(c)(3) such that PHMSA appears to now require: (1) a manual operations plan which in effect would require operators to manually operate their pipeline systems in the event of loss of SCADA or other communications failure; and (2) testing and verification of such internal communication/manual operations plans at each control room on a pipeline system. Such an interpretation belies the plain language of the regulations. Neither of these alleged requirements

[13] *See* 6 U.S.C. § 101 *et seq.; see also* TSA and PHMSA*, Annex to the Memorandum of Understanding between the DHS and the Department of Transportation Concerning Transportation Security Administration and Pipeline and Hazardous Materials Safety Administration Cooperation on Pipeline Transportation Security and Safety* (Aug. 2006); DHS 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).

have been expressed by the Agency in rulemaking, enforcement, or guidance, whether historically or since issuance of this NOPV.

The facts clearly demonstrate that Colonial had relevant procedures and an internal communication plan, which had been timely tested and verified through actual unrelated events. Consistent with PHMSA regulations, Colonial maintains 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 a specific internal communication plan for manual operation. Exh. 3 at 25-26.

As required by the plain language of 49 C.F.R. § 195.446(c)(3) and consistent with PHMSA's interpretative guidance and prior enforcement, Colonial tested and verified its internal communication plan through actual events throughout its system.[14] In those instances, the Company implemented a MOC containing the internal communication plan and identifying event-specific manual operating procedures. The MOC was disseminated to personnel as required reading for personnel sign-off and acknowledgment, which allowed Colonial to validate the plans. The internal communication plan is consistent, event to event, as the communication elements and process remain the same. The manual operating plans, on the other hand, are more complex and event specific, given the number of variables presented in any emergency situation.

Colonial tests and verifies its internal communication plan through actual events. Since January 2017, the plan has been tested and verified though thirteen (13) actual events and, most recently, one (1) tabletop exercise (see Table 1.0 below).

Table 1.0, Manual Operating Events (2017-Present)[15]

No.	Colonial Facility/Line	Plan Verification Event or Exercise	Date	Months from Previous
1.	Greensboro	HMI Communications – AOP-CPC J32 Loss of Data Communications	Jan. 2017	—

[14] PHMSA inspection guidance clarifies that operators may use actual events to verify these plans, which is consistent with references in enforcement precedent. Exh. 8, *PHMSA Control Room Management Inspection Form* at 22 (Mar. 1, 2012) (indicating that PHMSA would accept a "[r]ecord of actual events when the plan was pressed into service"); *see also In re: Texas Gas Transmission,* CPF 3-2021-017-WL (Apr. 9, 2021) (acknowledging an operator can use actual events and they can be considered a test in place of a drill or exercise, consistent with its plan, and outlining deficiencies in the operator's records of those events). Colonial's CRM Plan provides, "[a]ctual executions of the loss of communication procedures for a controlled shutdown and manual operation may be credited as a test if testing requirements are met." Exh. 3 at 26.

[15] Exh. 12, Colonial Pipeline Company, Greensboro HMI Communications Failure - AOP-CPC-J32 Loss of Data Communications (Jan. 2017); Exh. 13, Colonial Pipeline Company, Alpharetta Control Center - Atlanta Junction Server Failure - AOP-CPC-J32 Loss of Data Communications (Jan. 2018); Exh. 14, Colonial Pipeline Company, Atlanta Junction Server Failure - AOP-CPC-J32 Loss of Data Communications (Jan. 2018); Exh. 15, Colonial Pipeline Company, Alpharetta Control Center - EOP-CC-K30 Complete Loss of Communications (Aug. 2018); Exh. 16, Colonial Pipeline Company, Atlanta Junction Server Failure - AOP-CPC-J32 Loss of Data Communications (Oct. – Nov. 2019); Exh. 17, Colonial Pipeline Company, Houston Server – AOP-CPC-J32 Loss of Data Communications (Apr. 2020); Exh. 18, Colonial Pipeline Company, Alpharetta Control Center RTN Failure AOP-CC-J32 Loss of Data

No.	Colonial Facility/Line	Plan Verification Event or Exercise	Date	Months from Previous
2.	Alpharetta	Atlanta Junction Server –AOP-CPC-J32 Loss of Data Communications	Jan. 2018	12
3.	Atlanta	Atlanta Junction –AOP-CPC-J32 Loss of Data Communications	Jan. 2018	0
4.	Alpharetta	Alpharetta Control Center – EOP-CC-K30 Loss of Communications	Aug. 2018	7
5.	Atlanta	Atlanta Junction –AOP-CPC-J32 Loss of Data Communications	Oct.-Nov. 2019	14
6.	Houston	Houston Server – AOP-CPC-J32 Loss of Data Communications	Apr. 2020	5
7.	Alpharetta	Alpharetta Control Center – EOP-CC-K30 Loss of Communications	Apr. 2020	0
8.	Hebert	Herbert Server Failure – AOP-CPC-J32 Loss of Data Communications	Nov. 2020	6
9.	Line 04 Alpharetta	Greensboro to Dorsey- Cyber	May-Nov. 2021	5
10.	Line 34 Alpharetta	Dorsey to Baltimore Washington – Cyber	May-Nov. 2021	0
11.	Line 22 Alpharetta	Greensboro to Selma – Cyber	May-Nov. 2021	0
12.	Line 27 Alpharetta	Mitchell to Norfolk – Cyber	May-Nov. 2021	0
13.	Alpharetta	Alpharetta Control Center Restart for Normal Operations – Cyber	May 2021	0
14.	Woodbury Junction	Internal Communications Tabletop Exercise	Jun. 2022	13

With respect to the criminal ransomware attack, rather than an outright SCADA failure, Colonial was the victim of an unprecedented cyberattack and the Company voluntarily and proactively shut down the entire pipeline system and the SCADA system in accordance with the Company's controlled shutdown procedures. Within only two (2) days of the entire system being voluntarily shut down by Colonial, the Company implemented its internal communication plan and manual operations plan through the MOC process to initiate manual operations where necessary, following its procedures. The full restart was initiated within just five (5) days. Throughout that time and to continue to maintain the safety and integrity of its system while offline, Colonial in parallel undertook and coordinated extensive efforts to physically inspect and monitor thousands of miles of pipe in a few days' time. Every decision by Colonial was driven by a safety-first approach to this event.

Communications (Apr. 2020); Exh. 19, Colonial Pipeline Company, Hebert Server Failure – AOP-CPC-J32 Loss of Data Communications (Nov. 2020); Exh. 20, Colonial Pipeline Company, Line 04 Alpharetta - Greensboro to Dorsey – Cyber (May – Nov. 2021); Exh. 21, Colonial Pipeline Company, Line 34 Alpharetta - Dorsey to Baltimore Washington- Cyber(May – Nov. 2021); Exh. 22, Colonial Pipeline Company, Line 22 Alpharetta - Greensboro to Selma – Cyber (May – Nov. 2021); Exh. 23, Colonial Pipeline Company, Line 27 Alpharetta - Mitchell to Norfolk - Cyber (May – Nov. 2021); Exh. 24, Colonial Pipeline Company, Alpharetta Control Center - Restart for Normal Operations – Cyber (May 2021); Exh. 25, Colonial Pipeline Company, Woodbury Junction, Internal Communications Tabletop Exercise (Jun. 2022).

Despite the fact that PHMSA did not inspect any aspect of the cyberattack or Colonial's response to it, including the internal communication plan utilized by the Company during the cyberattack, the Agency relies on the event and mischaracterizes the facts to bolster its claims in NOPV Item 5 and the associated excessive proposed civil penalty.

1. The NOPV asserts that the Company "failed to test and verify its internal communications." *As demonstrated above, Colonial tested and verified an internal communication plan as required during actual events.*

2. The NOPV avers that the Company's alleged failure "contributed to consequences … of the cyberattack which required the immediate shutdown of the entire pipeline system." *Yet the cyberattack did not require an immediate shutdown; Colonial elected to do that in an abundance of caution. There is no connection that can be made between the implementation of the internal communication plan and the consequences alleged by PHMSA*.

3. The NOPV goes so far to boldly and inaccurately state that Colonial was "not prepared for the manual restart and manual operation of its pipeline" and it was an "ad hoc approach toward consideration of a 'manual restart' [which] 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*." The facts demonstrate otherwise; Colonial undertook extensive efforts to verify the integrity of its system and efficiently initiate the restart of its system through its internal communication and manual operation plans, which were disseminated through the MOC process, to minimize supply and social impacts while ensuring the safety of the public and the environment.*

V. PHMSA's Allegation Inappropriately Expands the Underlying Regulation Without Fair Notice

In NOPV Item 5, PHMSA attempts to transform the general requirement to test an internal communication plan into a requirement for a manual operations plan that must be regularly tested and verified at each and every control room. As reflected by prior enforcement, PHMSA has not provided the regulated community with fair notice of this new and novel interpretation of 49 C.F.R. § 195.446(c)(3). Articulated for the first time through NOPV Item 5, PHMSA now desires to (1) mandate that operators have a plan in place to manually operate their pipeline systems in the event of loss of SCADA or other communications failure and (2) require that internal communication/manual operation plans must be tested and verified at each control room on a pipeline system. There is no basis in the 49 C.F.R. Part 195 regulations for either interpretation.

Both the U.S. Constitution and the Administrative Procedure Act require that a regulation provide a regulated entity with fair notice of the obligations it imposes and be issued pursuant to notice and comment rulemaking. The Constitution of the United States, Amendment 5*;* 5 U.S.C. § 554(b). Courts have found that fair notice requires the agency to have "state[d] with ascertainable certainty what is meant by the standards [it] has promulgated [, . . .] must give [a party] fair warning of the conduct it prohibits or requires, and it must provide a reasonably clear standard of culpability to circumscribe the discretion of the enforcement authority and its agents."

ExxonMobil Pipeline Co. v. U.S. Dep't of Transp., 867 F.3d 564, 578 (5th Cir. 2017) (citing *Diamond Roofing Co, Inc. v. OSHRC*, 528 F.2d at 645, 649 (5th Circ. 1976)).

An agency may not enforce regulations according to "what an agency intended but did not adequately express." *Gates v. Fox Co., Inc. v. OSHRC*, 790 F.2d 154, 156 (D.C. Cir. 1986) (internal citation omitted). "Even if the [Agency's] interpretation were reasonable, announcing it for the first time in the context of this adjudication deprives Petitioners of fair notice. Where, as here, a party first receives actual notice of a proscribed activity through a citation, it implicates the Due Process Clause of the Fifth Amendment." *Fabi Constr. Co. v. Sec'y of Labor*, 508 F.3d 1077, 1088 (D.C. Cir. 2007). Regulated entities are not obligated to "divine the agency's interpretations in advance or else be held liable when the agency announces its interpretations for the first time in an enforcement proceeding and demands deference." *Christopher v. SmithKline Beecham Corp*., 567 U.S. 142, 159 (2012). The basic tenet captured by the cited legal precedent is the concept of fair notice and the prohibition against the government unfairly changing the rules, especially in the context of an enforcement action.

As such, PHMSA's allegation of noncompliance under NOPV Item 5 is arbitrary and capricious, an abuse of discretion, and otherwise not in accordance with law in violation of the Administrative Procedure Act, 5 U.S.C. § 706(2). PHMSA has no reasonable basis for its allegations in NOPV Item 5, particularly the statement 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."

VI. PHMSA's Proposed Civil Penalty Should be Withdrawn

As demonstrated above, Colonial complied with the plain language of 49 C.F.R. § 195.446(c)(3) and followed the only available PHMSA guidance which has been in place since 2011. As such, there is no basis in fact or law to support PHMSA's allegations in NOPV Item 5, the associated proposed civil penalty, or the PCO item. Prior PHMSA enforcement and application of the penalty criteria further support that the proposed civil penalty for this NOPV item of $846,300 is patently unreasonable.

With one exception, PHMSA's prior enforcement for alleged violations of the internal communication plan requirement at issue has been issued as Notice of Amendments, Warning Letters, or at most NOPVs with no penalty and a PCO (typically directing operators to perform the test). Before the issuance of this NOPV to Colonial, the only other proposed civil penalty *ever* issued under this provision sought $22,800 in proposed civil penalties for two (2) years of missed verifications.[16] In contrast, the civil penalty proposed to be assessed to Colonial is *thirty-seven (37) times higher.* Putting aside that the allegations with respect to Colonial are for four (4) years of alleged missed verifications, it is overwhelmingly clear that the issuance of such an inflated civil penalty is inconsistent with prior CRM enforcement precedent under 49 C.F.R. § 195.446(c)(3) and, thus, PHMSA's Pipeline Safety Enforcement Procedures the purpose of which is to "improve PHMSA's consistency in implementing the pipeline enforcement program"

[16] *In re: Navajo Nation Oil and Gas*, Notice of Probable Violation, CPF 3-2022-037-NOPV (Mar. 1, 2022) (alleging a violation of 49 C.F.R. § 195.446(c)(3) for failure to perform inspections in 2019 and 2020 and proposing an associated civil penalty of $22,800).

and with an emphasis on "fairness during an inspection." *PHMSA's Pipeline Safety Enforcement Procedures,* Sec. 3, Selection of Administrative Enforcement Actions at 1 (Sep. 15, 2020).

In addition to the fact that the proposed civil penalty of $846,300 bears no resemblance to the prior enforcement precedent, it similarly bears no resemblance to the penalty criteria or the facts at issue. If not withdrawn, the penalty should be substantially reduced because it does not accurately reflect the mandatory statutory and regulatory penalty assessment criteria. 49 U.S.C. § 60122(b) (outlining civil statutory penalty factors); 49 C.F.R. § 190.225 (detailing civil penalty assessment considerations). In particular, the following factors are not accurately considered and applied in the Agency's proposed civil penalty worksheet: culpability, number of instances of violation (gravity), history of prior offenses, good faith, and "other matters as justice requires." *See* Exh. 26, Colonial Pipeline Company's Comments on PHMSA Proposed Civil Penalty Worksheet.

Most notably, PHMSA categorized the alleged violation of 49 C.F.R. § 195.446(c)(3) as a "deliberate decision not to comply." That is simply incorrect and without basis, as explained above, coupled with the fact that Colonial's CRM Plan has been subject to inspection by PHMSA numerous times without any cited deficiencies for the internal communication plan approach. To the extent that NOPV Item 5 and associated penalty are not withdrawn, the point range for the culpability factor, at a minimum, should be significantly reduced from the assigned and unsupported value of 400 to 2. As demonstrated by the record, Colonial was actively complying with the requirements relevant to an internal communication plan as articulated by PHMSA in prior guidance and enforcement. In addition, PHMSA alleges a failure to test the plan in 18 instances based on a theory – never before articulated in the regulations, guidance, or enforcement – that verification of the internal communication plan is required at each and every control room. PHMSA also inaccurately included within the "history of prior offenses" an enforcement action that was reversed following a petition for reconsideration. This error reduces the number of prior violations from "4-5" to "2-3" on the worksheet, with an overall factor adjustment from 7 to 5. PHMSA further failed to properly account for Colonial's good faith efforts to comply with 49 C.F.R. § 195.446(c)(3), given its approach to test and verify internal communication plans during prior unrelated events. Finally, with respect to other matters as justice may require, it is simply unreasonable to issue a penalty thirty-seven (37) times higher than the only other penalty issued by PHMSA for the same allegation, particularly in light of the Company's efforts to address PHMSA's concerns prior to the issuance of the NOPV.

VII. PHMSA Has Not Satisfied its Burden of Proof

PHMSA bears the burden of proving by a preponderance of the evidence all elements of a proposed violation in an enforcement proceeding. *In re: Butte Pipeline Co*., Final Order, CPF 5- 2007-5008 (Aug. 17, 2009) ("PHMSA carries the burden of proving the allegations set forth in the Notice, meaning that a violation may be found only if the evidence supporting the allegation outweighs the evidence and reasoning presented by Respondent in its defense."). In this action, PHMSA has not met its burden to prove by a preponderance of the evidence that Colonial did not comply with requirements of 49 C.F.R. § 195.446(c)(3), or that 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 or that internal communication plans must be tested and verified at each control room separately.

Further, the Pipeline Safety Act (PSA) does not authorize a finding of liability simply because an event such as a release or a cyberattack occurred. 49 U.S.C. § 60101 *et seq.* As such, PHMSA may not find that Colonial failed to comply with 49 C.F.R. § 195.446(c)(3) or support an inflated penalty simply because a criminal cyberattack occurred. While Congress has in some instances provided for strict liability in other statutes; the PSA is not one of them. *ExxonMobil Pipeline Co.,* 867 F.3d at 577-78 ("The fact that the [a] release occurred, while regrettable, does not necessarily mean that [the operator did not] abide by the pipeline integrity regulations in considering the appropriate risk factors. If it did, then an operator that experiences a seam-related pipeline leak on its pipeline system could never escape liability under pipeline integrity regulations, thus nullifying the regulations and creating a strict liability regime that Congress has not authorized. [. . .] The unfortunate fact of the matter is that, despite adherence to safety guidelines and regulations, oil spills still do occur.").

VIII. Summary and Request for Relief

Colonial is steadfast in its commitment to pipeline safety and stands by its response to the 2021 cyberattack, which prioritized safety of people, the environment, and the pipeline itself. Colonial takes exception to PHMSA's unfounded expansion of its regulatory authority under NOPV Item 5, the Agency's suggestion that Company had an "ad hoc" approach to its return to service, and that Colonial's measured, methodical, and thoughtful response to the criminal cyberattack in any way contributed to the consequences of the attack or delayed the Company's return to service of its pipeline system. Colonial further believes that PHMSA's excessive proposed civil penalty of $846,300 for this single NOPV item is unwarranted and unsupported by the law, the facts, prior enforcement precedent, and the Agency's own enforcement procedures. In short, PHMSA has failed to meet its burden of proof for NOPV Item 5.

For all of the reasons identified above, and in consideration of other matters as justice may require, Colonial respectfully requests that NOPV Item 5 be withdrawn, along with the associated PCO requirement, and that the associated proposed civil penalty be withdrawn or, in the alternative, significantly reduced.

Date: October 6, 2022

Respectfully submitted,

BRACEWELL LLP

/s/ Catherine D. Little

Catherine D. Little, Esq.
Annie Cook, Esq.
2001 M Street NW, Suite 900
Washington, D.C. 20036-3310
Telephone: (202) 828-5800
Email: Catherine.Little@Bracewell.com
Annie.Cook@Bracewell.com

Counsel for Colonial Pipeline Company