Supporting Statement Appendix, A Comment Summary for *Pipeline Operator Security Information* 60-day Public Comment Summary and TSA Responses

Commenters	Document ID	Comment and Response
Patrick Coyle	Chemical Facility Security News	**Comment 1**: TSA is underreporting its burden estimate that each of the 100 covered facilities will be reporting 20 incidents per year. **Response 1**: As this comment is regarding one of the requirements that is a new part of the collection, TSA used historical data along with information from owner/operators to make a good faith estimate. Upon the renewal of the ICR, TSA will have actual data to rely upon to estimate the burden.
Patrick Coyle	Chemical Facility Security News	**Comment 2:** TSA is soliciting public comments on this ICR revision notice. As is usual for the TSA, they do not use the Federal eRulemaking Portal (www.Regulations.gov) site for comment submission. They require that comments be emailed (or delivered) to TSAPRA@dhs.gov. **Response 2:** To expedite receipt of responses, TSA requests comments to the 60-day notice be sent to TSAPRA@tsa.dhs.gov. TSA has successfully received public comments on its ICRs via the TSA email address. TSA is complying with the PRA and OMB PRA implementing regulations with respect to its notice and comment process. *See* 5 CFR 1320.8 (d)(1) and 5 CFR 1320.5(a)(1)(iii)(F).
Kimberly Denbow; Matthew J. Agen	American Gas Association (AGA)	**Comment 1:** The Pipeline Security Guidelines encourage pipeline operators to notify the Transportation Security Operations Center ("TSOC"); however, the requirements for notification to the TSOC are very different than the requirements to notify CISA in Security Directive 1. In addition, Security Directive 1 provides that CISA would take all incident reports due to their experience. AGA requests TSA to clearly articulate who and what is the appropriate cyber incident handling authority for TSA and clarify the inconsistencies between TSA's Pipeline Security Guidelines and Security Directive 1. **Response 1:** The primary distinction between the reporting of incidents, TSA's Pipeline Security Guidelines and Security Directive Pipeline 2021-01 is the mandatory reporting of cybersecurity incidents to CISA. TSA continues to encourage all pipeline owner/operators to continue reporting other security incidents, such as physical security incidents, to TSOC. The only distinction here is cybersecurity issues. The commenter has not provided any other examples of inconsistencies.
Kimberly Denbow; Matthew J. Agen	AGA	**Comment 2**: TSA is seeking renewal of the Critical Pipeline ICR for the maximum three-year approval period. As noted above, Security Directive 1 has a stated expiration date of May 28, 2022. Therefore, to the extend this collection relates to Security Directive 1, it should terminate when the directive expires. **Response 2**: The timeline for ICR approvals is set under the PRA and OMB

		implementing regulations; OMB has authority to grant up to a three-year approval period for ICRs, which approval is typically granted. *See* 5 CFR 1320.10 (b). As this ICR includes a voluntary as well as the mandatory collection separate and apart from the mandatory collection stemming from Security Directive Pipeline 2021-01, TSA is requesting a three-year approval period. TSA acknowledges that the security directive (SD) expiration date is currently May 28, 2022; however, that expiration date may be extended under the authority of the TSA Administrator.
Maggie O'Connell	American Fuel & Petrochemical Manufacturers Association Privacy Project, et al. (AFPM)	**Comment 1**: The Associations do not believe a three-year extension to the May 26, 2021, emergency revision is warranted, because TSA is not accurately calculating the burden to the public from the broad scope of applicability for cybersecurity incidents that require reporting across both the information technology (IT) and operational technology (OT) networks. **Response 1**: Please *see* "Response 2" to AGA and "Response 1" to Chemical Facility Security News.
Maggie O'Connell	AFPM	**Comment 2**: …a three-year extension undermines the need for the subsequent two Security Directives (SDs) for pipeline cybersecurity for which the emergency revision is based. As previously stated to the agency, the Associations maintain that, should TSA seek to regulate pipeline cybersecurity, the agency should TSA seek to regulate pipeline cybersecurity, the agency must proceed through regular notice and comment rulemaking. **Response 2:** The provisions of the ICR that apply to compliance with TSA Security Directive Pipeline 2021-01 are in effect until the expiration date of the SD. The provisions of the ICR that apply to voluntary reporting of physical security incidents to the TSA TSOC would be in effect for the three years that the PRA is valid. The TSA Administrator has the authority under 49 USC 114(l)(2) to issue security directives.
Maggie O'Connell	AFPM	**Comment 3:** The Associations appreciate the opportunity to provide feedback during the development of both SDs; however, TSA has not addressed many of the substantive concerns raised in those comments. Among those concerns include a lack of information regarding the threat for which these SDs are based…. the cyberattack on the Colonial Pipeline system… should no longer be used to justify the emergency revision. Similarly, "other emerging threat information" is vague, and despite repeated attempts from the Associations and the Oil & Natural Gas Subsector Coordinating Council (ONG SCC) to receive classified threat briefings, the agency has only just recently responded, but has still yet to schedule such briefing. Without timely, actionable intelligence, pipeline operators cannot defend against the ever-evolving cybersecurity threat, nor can they make appropriate adjustments to their risk-based security programs per the TSA Pipeline Security Guidelines.

		Response 3: TSA recognizes our responsibility to share timely, relevant threat information with pipeline operators. This however is not required for operators to fulfill the collection requirements of this Information Collection Request. TSA will use the information collected to analyze the data in order to better evaluate the threat. TSA articulated its justification for the issuance of the security directive in Security Directive Pipeline 2021-01.
Maggie O'Connell	AFPM	**Comment 4:** The statutory authority under which TSA may issue SDs requires the TSA Administrator to determine that "a regulation or security directive must be issued immediately [emphasis added] in order to protect transportation security." This emergent requirement supposes that an urgent threat to pipeline systems will otherwise directly impact pipeline systems if not immediately addressed. As of July 19, 2021, the issuance date of the second SD, no timely threat information had been shared with industry. Meanwhile, the "ongoing" threat cited by TSA suggests that the threat has existed for an extended period of time and therefore does not meet the threshold for an immediate regulatory action such as an SD. **Response 4**: Please *see* "Response 3" to AFPM.
Maggie O'Connell	AFPM	**Comment 5:** While the Associations do not oppose the appointment of cybersecurity coordinators, TSA should, through this ICR, consider the company's additional resource burden for maintaining that position, with no clear benefit to the security posture of the pipeline system. TSA should also consider the realities of how large, integrated companies with multiple operational segments are organized. Designating a single, corporate-level official in a multi-operational enterprise is less appropriate than at the functional level. **Response 5:** TSA disagrees with this assertion. The requirement to appoint cybersecurity coordinators is not onerous and falls under regular business policy and practice. There is no requirement in Security Directive Pipeline 2021-01 that restricts responsibilities as a cybersecurity coordinator to be the sole responsibility of the designated individual. TSA encourages the appointment of alternate(s) for the cybersecurity coordinator to alleviate the need for one individual to be available 24/7 without exception.
Maggie O'Connell	AFPM	**Comment 6:** TSA is requiring all affected pipeline operators to report cybersecurity incidents or "potential" cybersecurity incidents on both their IT and OT systems to CISA within 12 hours using the CISA reporting system. Congress gave TSA authority over pipeline security. The SD, however, exceeds TSA's authority to the extent it requires reporting of cybersecurity incidents on corporate IT systems that are not directly linked to pipeline OT. The encroachment of the SD's application to the entire corporate IT system is beyond the jurisdiction of the agency. **Response 6**: TSA has broad statutory responsibility and authority to safeguard

		the nation's transportation system, including pipelines. *See*, e.g., 49 U.S.C. 114(d), (f), (l), (m). As was seen in the attack on the Colonial pipeline system, an attack on a corporate Information technology (IT) system has the potential to impact operations and directly affect national and economic security. CISA and TSA evaluations of pipeline companies have consistently found connections between corporate IT and Operational Technology (OT). Thus an attack on an IT system has the potential to impact pipeline operations.
Maggie O'Connell	AFPM	**Comment 7:** TSA must avoid designing regulations that would require reporting of otherwise minor, nonmaterial incidents. This volume of information may overwhelm CISA with massive amounts of low-value data. **Response 7:** TSA supports the collection of reporting of all relevant incidents to ensure situational analysis and review by CISA and TSA as required in Security Directive Pipeline 2021-01. To date, there is no indication that the volume of reports overwhelms CISA. TSA will continue to coordinate with CISA on all matters regarding the collection.
Maggie O'Connell	AFPM	**Comment 8**: The Associations also believe the 12-hour reporting timeframe is aggressive and far too short. **Response 8**: TSA disagrees with this assertion. TSA and CISA support the 12-hour reporting timeframe as required in Security Directive Pipeline 2021-01. Time is of the essence in stopping the spread and potential impact of a cyber-incident. The reporting time period is 12 hours after a cybersecurity incident is identified. The expediency of reporting incidents affecting pipelines is supported by the critical role of this industry in national security, including the economy, and the need to maintain confidence in the availability of fuel. The SD indicates that when required information is not available at the time of the report that "Owner/Operators must submit an initial report within the specified timeline and supplement as additional information becomes available."
Maggie O'Connell	AFPM	**Comment 9**: The Associations feel that affected entities should be afforded strong liability and disclosure protections given the breadth of the reporting requirements. **Response 9:** TSA appreciates all comments. Your comment, however, is outside the scope of this Information Collection Request.