Supporting Statement Appendix, A Comment Summary for Critical Facility Information of the Top 100 Most Critical Pipelines 60-day Public Comment Summary and TSA Responses

Commenters	Document ID	Comment and Response
Patrick Coyle	Chemical Facility Security News	**Comment 1**: There is no link provided for the PCSA form, apparently TSA never submitted a copy of that form to OIRA for the emergency approval back in May. Without access to the form, it is impossible to evaluate the amount of time that TSA estimates that it will take to complete the form. TSA should be required to re-submit this 60-day ICR revision notice after making that form publicly available for review. **Response 1**: The ICR documentation, including the TSA Pipeline Cybersecurity Self-Assessment form, which was not finalized at the time the 60-day notice was published, will be available at http://www.reginfo.gov upon its submission to OMB. The public will have an additional opportunity to comment at that time upon publication of TSA's 30-day Federal Register notice.
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 (sic) 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:** TSA requests comments to the 60-day notice be sent to TSAPRA@tsa.dhs.gov due to some technical difficulties in using the eRulemaking portal. 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 questions asked as part of the CFSR are similar to the questions proposed in the Security Directive. The amount of detail and requested information within Security Directive 1, however, requires more defined responses. This can cause these two review forms to appear to not be in sync due to the inconsistency on guidance. AGA recommends that TSA consider having additional consistency and clarity between the forms. If an entity completes a CFSR, then it should not have to complete the TSA Pipeline Cybersecurity Self-Assessment form or vice-versa. **Response 1:** There is no inconsistency in TSA's guidance nor has the commenter provided an example of an inconsistency. The CFSR and the Cybersecurity Self-Assessment form are two distinct collections. The CFSR is a voluntary collection, while the Cybersecurity Self-Assessment form is a mandatory information collection.
Kimberly Denbow;	AGA	**Comment 2:** AGA recommends that TSA consider not leveraging the provided "information to make a global assessment of the cyber risk posture of the

Matthew J. Agen		industry.” Companies had difficulties identifying the appropriate scope for completing the assessment. Organizations may have taken different approaches to completing the assessment based on the lack of guidance provided by TSA to date. Therefore, the various scope perspectives driving responses will result in inconsistencies that will cause the cyber risk posture to potentially be inaccurate. This can cause future TSA decision making to be inaccurate. AGA requests the TSA issue clear guidance and definitions that further define the scope of the Pipeline Cybersecurity Self-Assessment. **Response 2:** TSA does not see any basis for the assertion regarding difficulties identifying the appropriate scope for completing the assessment. In fact, TSA received very few questions from operators on difficulty interpreting questions on the cybersecurity self-assessment required by Security Directive Pipeline 2021-01. The assessment was a one-time requirement that was due to TSA in June 2021 and has been completed by all operators. TSA and CISA are conducting an analysis of the findings of the assessment and understand the limitations of the assessment instrument.
Kimberly Denbow; Matthew J. Agen	AGA	**Comment 3**: TSA is seeking renewal of the Critical Pipeline ICR for the maximum three-year approval period. Due to the fact that the Security Directive 1 has a stated expiration date of May 28, 2022, AGA recommends that the Critical Pipeline ICR renewal should correspond with that expiration date. It is unclear why the renewal is for a longer term than the effectiveness of Security Directive 1. If TSA seeks to extend the term of Security Directive 1, a further renewal can be requested. **Response 3**: The timeline for ICR approvals is set under the PRA and OMB implementing regulations. *See* 5 CFR 1320.10(b). OMB has authority to grant up to a three-year approval for ICRs, which approval is typically granted. As this ICR includes a voluntary 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 as ratified by the Transportation Security Oversight Board.
Kimberly Denbow; Matthew J. Agen	AGA	**Comment 4**: Operators have reported to AGA that the time spent on the Pipeline Cybersecurity Self-Assessment was between 60-150 hours (10 – 25 times the TSA estimate). AGA requests that TSA accurately reflect the excessive amounts of time it took owners/operators to complete the Pipeline Cybersecurity Self-Assessment, update the estimate in the Critical Pipeline ICR, and take the burden on owners/operators into consideration in future directives/regulations. TSA has underestimated the burden on owners/operators to complete the Pipeline Cybersecurity Self-Assessment form. This underestimation also calls into question TSA’s other estimates. TSA should update the estimated burden in the Critical Pipeline ICR (and the Operator Security Information ICR) to reflect the burdens on owners/operators.

		Response 4: As this comment addresses a requirement resulting in a new collection, TSA used historical data along with information from owners/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. TSA has provided detailed calculations and explanations in the Information Collection Supporting Statement (SS), which is available for public viewing upon submission to OMB (*see* question 12).
Maggie O'Connell	American Fuel & Petrochemical Manufacturers Association Privacy Project, et al. (AFPM)	**Comment 1**: The Associations do not believe a three-year renewal of the May 26, 2021, emergency revision is warranted given that it undermines the emergent need for an SD. **Response 1**: Please *see* "Response 3" to AGA.
Maggie O'Connell	AFPM	**Comment 2**: TSA is basing the emergency revision on vague cybersecurity threat information that has not been shared so companies can adjust risk-based security programs. Should TSA seek to regulate pipeline cybersecurity, the agency must proceed through regular notice and comment rulemaking. **Response 2:** TSA will use the information collected to analyze the data in order to better evaluate the threat. The Administrator has the authority under 49 USC 114(l)(2) to issue SDs. TSA articulated its justification for the issuance of the SD in Security Directive Pipeline 2021-01.
Maggie O'Connell	AFPM	**Comment 3:** The Associations appreciate TSA's intent in allowing the operator company to apply their methodology to determine asset criticality; however, a more focused approach on designation would eliminate ambiguity between the operator and TSA. Furthermore, the Associations recognize TSA's need to periodically review the Pipeline Security Guidelines to reflect additional criticality criteria, but High Consequence Areas (HCAs) should not be weighed more than other criteria in determining criticality. As HCA is not determinate of criticality for US critical infrastructure, the effect of HCAs on critical infrastructure operations should be the criteria. **Response 3**: TSA and the pipeline industry collaborated on the development of the updated criteria for the designation of critical facilities throughout 2020 resulting in the publication of Change 1 to the TSA Pipeline Security Guidelines in April 2021. The voluntary Guidelines note that natural gas transmission and hazardous liquid pipeline facilities located in HCAs should be considered critical. The information collected will enable TSA to evaluate the issue of criticality, and may make revisions to methodology if appropriate.

Maggie O'Connell	AFPM	**Comment 4:** This emergent requirement supposes that an urgent threat to pipeline systems will otherwise directly impact pipeline systems if not immediately addressed. However, the "ongoing" threat cited by TSA suggests that the threat has been in existence for an extended period of time and therefore does not meet the threshold for an immediate regulatory action such as an SD. **Response 4**: The cybersecurity threat to pipeline is a current and ongoing threat. The Administrator has the authority under 49 USC 114(l)(2) to issue SDs to address threats to transportation security.
Maggie O'Connell	AFPM	**Comment 5:** The inclusion of "other emerging threat information" without clarity or operator knowledge of such threat information weakens the ability of the owner/operator to respond to such threats based on their own risk-based security programs, as outlined in the TSA Pipeline Security Guidelines. **Response 5:** 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.
Maggie O'Connell	AFPM	**Comment 6:** Notably absent from the ICR is a cost-benefit analysis of the measures prescribed in the statutory requirements for issuance of an SD. Safety and security of pipeline operations are the top concern of pipeline operators, and the Associations' members are proactive in improving the security posture of their facilities; however, the measures outlined in the two SDs do not enhance operational security and the TSA Administrator has not presented a cost-benefit analysis justifying the security benefit for these measures. **Response 6**: The ICR does not require a cost-benefit analysis and meets the requirements outlined in 5 CFR 1320.8.
Maggie O'Connell	AFPM	**Comment 7:** The unintended consequences that several of the highly prescriptive measures in the second SD may have on pipeline operational safety and security. During the SD drafting process, the Associations provided specific comments around potential operational concerns that could arise by imposing prescriptive cyber requirements without specific understanding of a company's existing approach or protections. Although some of the compliance timelines have been extended, there remain significant concerns regarding rigid implementation of the SD to pipeline operating systems, which might unnecessarily impact the integrity and reliability of these systems. The Associations urge TSA to work with operators and The Pipeline and Hazardous Materials Safety Administration (PHMSA), to ensure that, as changes are required, operators are not sacrificing one risk to reliability for another. **Response 7:** This ICR covers the information collection requirements for TSA Security Directive Pipeline 2021-01, not Security Directive Pipeline 2021-02.