AMERICAN PUBLIC GAS ASSOCIATION

June 18th, 2021

Chuck Phillips
Industry Engagement Manager, Pipeline
Transportation Security Administration (TSA)

Submission via email: Charles.E.Phillips@tsa.dhs.gov

Re: TSA Draft Security Directive 02 - Pipeline Cybersecurity Mitigation Actions, Contingency Testing, and Testing

Chuck:

The American Public Gas Association (APGA) is pleased to respond to the request for comment for *Transportation Security Administration (TSA) Draft Security Directive 02 - Pipeline Cybersecurity Mitigation Actions, Contingency Testing, and Testing (SD 02)*. APGA is the trade association for approximately 1,000 communities across the U.S. that own and operate their retail natural gas distribution entities. They include municipal gas distribution systems, public utility districts, county districts, and other public agencies, all locally accountable to the citizens they serve. Public gas systems focus on cybersecurity in their mission to provide clean, safe, reliable, and affordable energy to their customers.

APGA members appreciate the intent of TSA in drafting this document. However, there are some concerns that need to be raised. At the outset, public natural gas utilities ask for reasonable requirements accomplished in appropriate timelines with a risk-based approach. In the natural gas supply chain, there are varying degrees of hazard, so the mandates overseeing all these aspects should take into account impacts should an incident occur. As well, APGA members have been managing threats on their systems in a risk-based way for many years, developing assessment matrices and adding appropriate redundancies, which is often after obtaining natural gas from the transmission companies, who also have well-established risk management practices. In addition, for the context of this comment request, APGA wants to call attention to a unique feature of public natural gas utilities, specifically their dependence on a city council or utility board for budget approval. Technology upgrades to ensure secure infrastructure are considered when appropriate, but this requires significant time and conversation years in advance of execution.

With regards to SD 02, APGA offers general concerns here. As the turnaround time for responding to SD 01 didn't practically allow enough time for effective responses to TSA, some of the below could be used to address concerns in both SDs.

- It is not appropriate to handle all of these communications between pipeline operators and TSA through an email account. A secure portal for compliance correspondence, uploading responses, etc., should be set up. This protected system should coincide with assurance that information will be sheltered from disclosure laws, regulatory actions,

and Freedom of Information Act (FOIA) requests. As an example, in sharing SD 02 with stakeholders, the password for the encrypted document was delievered by the same mechanism as the document was transmitted. If email is compromised, then the document is unprotected.

- As coordination between TSA and APGA members progresses, TSA will need a contact different from the currently defined, "Cybersecurity Coordinator." From current understanding, "Cybersecurity Coordinator" is an executive, who might respond to a significant threat but is not involved in everyday reporting, which as defined in the SD, includes much more. Or if this understanding of the "Cybersecurity Coordinator" or the incidents needing to be reported is incorrect, further clarity would help. It would also be beneficial to ask operators required to comply with the SDs to also designate a Primary and Alternate Compliance Contact.
- While public natural gas utility operators required to comply with the SDs appreciate some acts of clarification, there is still much confusion over the expansiveness and vagueness of these recent TSA actions. For instance, the TSA Guidelines make a distinction between critical and non-critical assets, but is that the same for the Directives? A service line or regulator serving a residential neighborhood has a very different risk than an interstate transmission line. In addition, public natural gas utilities often manage other services, such as electric, water, wastewater, telecommunications, etc., which are beyond the scope of TSA authority and are regulated by other agencies. What is the responsibility for the operator in securing all these services and communicating with TSA? What is TSA doing to coordinate with the other oversight authorities? One suggestion from APGA is the TSA Guidelines definition of critical could be applied to assets public natural gas utilities operate. If that was the intent of the SDs, please inform the industry.
- Systems or practices are already in place to achieve requirements of SD 02, including password resets, system assessments, etc., and these are on a schedule, which may have provided for their completion just weeks or days ago. Do operators have to do again within the timelines of the directive? That is excessively burdensome, and TSA should consider more practicality in this request.
- APGA members request more consistency in the definitions. TSA's term may not be the industry's term.

The request for responses for SD 02 was rather quick, as well, but APGA did have time to correspond with our members on concerns. Because of the still, fast turnaround, below are just the names of the sections of the SD, with the comment listed immediately following.

ACTIONS REQUIRED

A. Implementing Mitigation Measures

- 1a. Requiring public natural gas utilities to exchange equipment that will not allow password resets may require the replacement of entire systems. This is an unreasonable expectation for multiple reasons, not least of which is modifications of systems will be a multi-year effort. Also, there are supply chain implications in mandating replacement of systems. Many cybersecurity threats can be mitigated by updating passwords. APGA suggests TSA mandate a regularly-scheduled password change after this one-time reset.

- 1b. "Verbal" confirmation seems redundant, as operators have processes that accomplish this same objective already in place.
- 2a. It is not possible to deploy multi-factor authentication (MFA) across all information technology (IT) and operational technology (OT) systems in 90 days. With this aggressive timeline, TSA is not accounting for the procurement process, which only takes place after specifications have been written, as well as the budgeting/approval processes that are often out of the control of a municipal utility, given their oversight from a city council or utility board.
- 2e. TSA should consider that running antivirus programs on OT systems may negatively impact integrity and safety. A very fast response time is required or the systems will assume there is a malfunction and no longer communicate with slow devices. Flexibility in how this requirement is implemented should be allowed, given the variability of OT systems. Generally speaking, it is allowed for some sections of the SD 02, but those parts, as well as the whole document should include some type of "technical feasibility exception" process to document where these requests from TSA just aren't practical.
- 2g. Due to limited resources and the size of all IT systems, this policy is impractical. For instance, patches must be tested, and it may not be prudent to implement because they cause disruption to existing processes, and as seen with Microsoft, may have bugs themselves. Some APGA members typically wait for a second update from Microsoft before executing a patch, after they are tested. TSA should consider allowing companies to have a mitigation plan if deciding not to implement a patch. As an example, for APGA members that have electric utility services, the North American Energy Reliability Council (NERC) gives 28 days to evaluate and another 28 days to implement or develop a mitigation plan.
- 2.h. and 2.i. These requests are complex to implement and would take much longer than the time allowed. APGA members have limited resources, especially personnel, which will be required to comply with all these deadlines concurrently.

B. Implementing a Cybersecurity Contingency/Response Plan

- APGA does not argue with the request to have a response plan. However, the same staff will have to complete all the requirements of Section A and Section B, in the aggressive timelines. This same personnel cannot reasonably complete both in the time mandated by TSA. APGA suggests completion of Section B requirements first and have much longer to complete Section A, with consideration to allow for more, appropriate time to finalize the requirements of both.

C: Conducting Industrial Control System Cybersecurity Architecture Design Review

- While it is unknown the number of companies needed to comply with the SDs, APGA is assuming, at a minimum, the "Top 100" will be required to complete. Given that, it is impractical for 100 pipeline operators to hire consultants to evaluate their systems in 180 days. APGA is unsure if there are even enough qualified people to do this work, and this is on top of the months to write specifications, evaluate potential vendors, and negotiate contracts. The

architecture of industrial control systems (ICS) do not change frequently. APGA would suggest TSA conduct these reviews, initially with their own staff to ensure quality and consistency, and then "as needed," when a change to the architecture of the system is to be implemented. Public natural gas utilities would willingly notify TSA of these projects and support a scheduled review. As mentioned earlier as an example, NERC could also be looked to in this situation, as they only assess bulk electric systems (BES) when major changes to control systems are made and must be "recertified."

In addition to the input offered above, APGA supports the technical feedback of the other trade associations within the oil and natural gas sector. APGA has worked for many years with colleagues at those organizations, and in this proceeding, would like to echo the valuable feedback they have submitted. Please consider all the feedback submitted by APGA and the additional valuable stakeholders represented by the oil and natural gas trade associations.

Thank you for any consideration of industry input. Public gas utilities play a critical role in delivering Americans the energy they need through an existing secure, safe, and reliable pipeline infrastructure. APGA and its members look forward to partnering in this important work in securing America's clean energy future.

Respectfully submitted,

Dave Schryver
President & CEO
American Public Gas Association