International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605019

Operationalizing NIST CSF 2.0 and TSA Security Directives in Pipeline Cybersecurity

Vilas Shewale

Independent Cybersecurity Researcher, USA

ABSTRACT: As oil and gas pipeline operators in the United States respond to the TSA's cybersecurity rules and prepare for NIST's August 2023 release of cybersecurity guidance and framework updates version 2.0, another level of complexity may be introduced. Over the last two years, TSA guidance has progressed away from prescriptive rules and moved into a more performance-based methodology of instructing operators to document how they have planned for and execute TSA security protocols. The August public draft of NIST guidance (version 2.0) added the sixth Cybersecurity Framework function of Govern and restructured the existing five functions in accordance with a decade of practice. This paper looks into both regulations and identifies their points of alignment, offering some views into how operators can meet the mandates of both without establishing and running dual cybersecurity compliance efforts. This guide is aimed at the pipeline cybersecurity leaders who lead this effort and the engineers who support it, along with the compliance partners they work with. The main goal of this document is to make the regulatory framework more approachable than add new obligations.

KEYWORDS: NIST CSF 2.0, TSA Security Directive, pipeline cybersecurity, governance, ICS, compliance.

I. INTRODUCTION

The cybersecurity regulations surrounding pipeline have changed more in 2.5 years than the two decades that preceded. Since May 2021, there have been no voluntary pipeline security guidelines and the security of pipelines and related infrastructure in the U. S. Is largely mandated and standardized by the Transportation Security Administration, not loosely by the TSA Pipeline Security Guidelines issued in 2011 and updated numerous times over the intervening decades. Mandatory security directives have continued to flow in the wake of the Colonial Pipeline attack, the first mandate came a matter of weeks after the breach. These security directives have continued to change and, as of last month, had reached their most recent major updates, which were released in July 2023.

Simultaneously, as the TSA moves pipeline through its mandate process, NIST has spent the better part of three years preparing version 2.0 of the NIST Cybersecurity Framework. The framework originally was published in 2014 and has been updated to 1.1 in 2018, acting as a common vocabulary for U. S. Critical infrastructure in their efforts to align and manage cybersecurity risks. The 2.0 version was released as public draft on August 8th [1] and includes numerous changes worth considering, among which is a newly defined Govern function appended to the framework's original five functions.

This white paper does three things. Section 2 describes the regulatory context surrounding the issue and what relation exists between the two processes (TSA and NIST CSF). Section 3 explains the changes brought about by NIST CSF 2.0, highlighting points of particular interest. Section 4 explains the status of TSA directives in July 2023. Section 5 juxtaposes NIST CSF 2.0 and TSA pipeline directives, suggesting a unified implementation approach. Section 6 suggests a sequence for operators starting pipeline compliance work now. The paper takes a practical tone throughout, knowing that while a document might matter for its official role, ultimately its worth lies in the program that a company establishes around it.

II. REGULATORY CONTEXT

By federal standards, it happened fairly fast. Pipeline-2021-01, dated late May 2021, asked operators of some of the nation's critical pipelines to tell CISA about cybersecurity breaches, to put in a pipeline cyber boss and to audit all systems for vulnerabilities[2]. The subsequent Pipeline-2021-02 dated July 2021 included specific things operators needed to do, contingency plans, security architects needed to do architecture reviews and so forth. Those tighter rules brought flak from pipeline operators worried about regulators dictating controls that did not take the variety of environments into consideration.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605019

Version A mid-2022 added some time and some clarifications and Version B mid-2022 tweaked both a little. December 2022 Version C reversed direction from prescriptive rules toward performance-based criteria. It established a Cyber Security Implementation Plan which operators would produce, they identified critical cyber systems and explained how selected controls achieve specified security outcomes[3]. Version D mid-2023, which reiterated the directive, offered some tweaks for the audit process. See Figure 1.

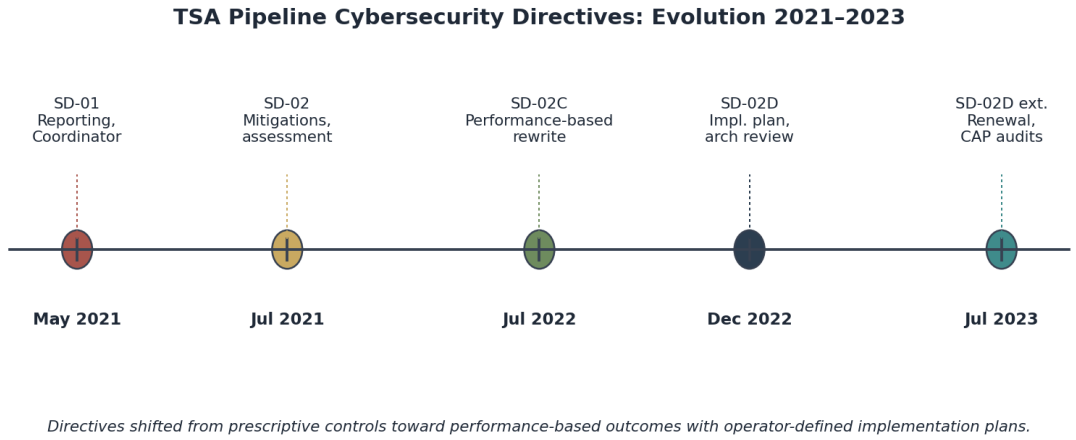

Figure1. Evolution of the TSA pipeline cybersecurity directives, from prescriptive in 2021 to performance-based by late 2022

A performance-based standard does not allow operators to just tick boxes like a prescriptive rule does. It requires the operator to explain why their set of controls works in their environment and persuade a regulator that their solution meets all goals. The execution plan is therefore the most important item. Well-run organizations will come out with a document that meets the requirements of TSA and also gives a common view to all internal stakeholders as to where the program is going. It does not matter whether the Framework has always been voluntary on NIST's side, it is a key document linking a lot of regulations. You see this because the TSA directives cite some of the NIST guidance documents, NIST's C2M2 capability maturity model, which DOE supports, uses the Framework to organize the security capabilities it mentions, many state public utility commissions require their regulated entities to adopt the Framework, numerous vendors also map their products to it, many of the operators that might never use the word "NIST CSF" or even use the Framework have a view on what security ought to look like based on its terminology, such as controls, safeguards, desired outcomes or performance metrics, among others.

III. WHAT'S NEW IN CSF 2.0

The public draft of CSF 2.0 keeps the structure that practitioners have internalized: Functions, Categories, Subcategories, Informative References. The changes are best understood by what they add and by what they signal about NIST's read of where programs need help.

International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605019

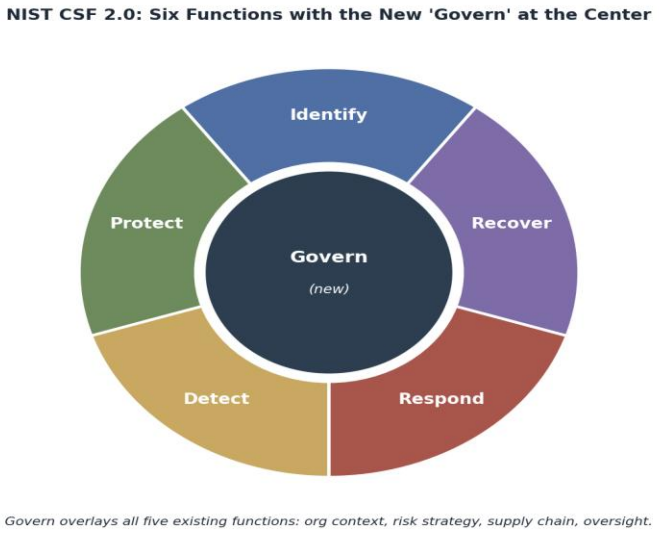

Figure .2 NIST CSF 2.0 retains the five original functions and adds Govern as a sixth, sitting at the center of the others.

3.1 The Govern Function

The core innovation here is the addition of governance. It is actually a consolidation of subcategories previously found under Identify, such as org context, risk management strategy, supply chain risk, oversight and policy, into their own standalone function[1]. The choice makes sense given that regulators have been saying it for years: poorly governed security programs that lack oversight from the board and an explicit, documented risk management strategy perform badly regardless of how well tuned their security tools actually are. Now NIST puts the question "who owns this?" on par with "what technology is in place?" and implicitly asks boards to stop looking over their CISO's shoulder and wonder why this is still so poorly done.

3.2 Refinements to the Existing Five Functions

"The Identify, Protect, Detect, Respond and Recover categories all get slight rewording, too. Govern replaces much of the Identify category (with its previous Governance subcategories moved out as appropriate). Protect gets clearer language about identity and access management, focusing on use of phishing-resistant MFA. Detect focuses on continuous monitoring and threat intelligence integrated into detection logic. Respond and Recover add language on incident handling and communications, with better clarity on recovery objectives linking to business continuity planning. The most important takeaway is that none of these changes are surprises for anyone who is been paying attention to public commentary and expectations around Framework 1.1 - in essence, these changes just acknowledge what mature programs are already doing in their own way. "

3.3 Implementation Examples and Profiles

There is more guidance added with implementation examples in the 2.0 draft and more encouragement to use profiles. Profiles can be thought of as the Framework customized for an organization's particular situation, its mission and its risk tolerance. NIST intends to issue more industry-specific profiles, for instance in energy and ransomware risk management [4]. For pipeline operators, this will hopefully create a useful starting profile to use, instead of having to create one themselves from nothing, making compliance with NIST and TSA easier.

IV. THE CURRENT STATE OF THE TSA DIRECTIVES

SD Pipeline-2021-02D, the version in force as of mid-2023, organizes its requirements around a set of operator-produced artifacts and assessments.

4.1 The Cybersecurity Implementation Plan

The most critical piece of documentation is the pipeline security plan, which delineates the operator's key cyber systems-those that could severely impact operations or safety if compromised-and the safeguards put in place. The TSA will review these plans and pipeline companies must continuously manage and update them as their security posture

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605019

and technological landscape evolve. Thus, it is not a document you complete and hand in once, it is an ongoing reflection of their current security efforts.

4.2 Network Segmentation Policies and Controls

It says you must properly segment your IT environment from your OT environment and your OT environment from itself. It demands you design this segmentation so a compromise of IT can never be used to reach systems in your OT. The regulation is written performance-based: It is not saying "you can use X brand firewalls" or "you can use VLAN Y configuration. " Instead, you, as an operator, must show that the segmentation you used to achieve compliance is actually working well enough to contain whatever badness it purports to.

4.3 Access Control

On the controls requirements, you will get Privileged account and Multifactor authentication controls. And then there are Controls concerning System credentials. The requirement to push towards phish-resistant Authentication controls while simultaneously killing single-factor authentication access routes for your remote systems is really key here. This is not new, but I imagine those on the Zero Trust agenda are nodding a lot in solidarity.

4.4 Continuous Monitoring and Detection

It should cover both OT and IT, with sensors aware of pipeline-specific industrial protocols and common attack techniques. It requires logs of relevant activity to be retained and to support the IR workflow.

4.5 Cybersecurity Assessment Program

Operators are to have a cybersecurity assessment program to exercise the implementation plan, find deficiencies in it and develop corrective action plans and remediation efforts to improve upon it. Assessments are reported to TSA periodically (TSA will provide an exact cadence). TSA wants this requirement to keep the implementation plan a living document than just static text.

The assessment work will likely involve both internal reviews on a more frequent cadence (weekly, bi-weekly) along with independent assessments by third parties on a longer cadence (e. g. , quarterly, semi-annually, annually). The internal assessment catches drift, while the third-party assessment catches blindness. Operators can choose their methodology for conducting the assessment, however, the directive will expect that they document their methodology, that they track issues to resolution and that assessment results are inputs to updating the implementation plan. Well-run programs will have an assessment artifact that: meets TSA requirements, aids internal audit and supplies inputs to C-suite and board-level risk reports. Poorly run programs will simply have an assessment report file that collects dust and provides a paper trail for any unaddressed deficiencies found under audit.

V. MAPPING CSF 2.0 TO THE TSA DIRECTIVES

The two frameworks are not in tension. They view the same problem through different lenses. The TSA directives are outcome-focused and pipeline-specific. The CSF is sector-agnostic and capability-focused. Figure 3 shows the high-level mapping.

International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605019

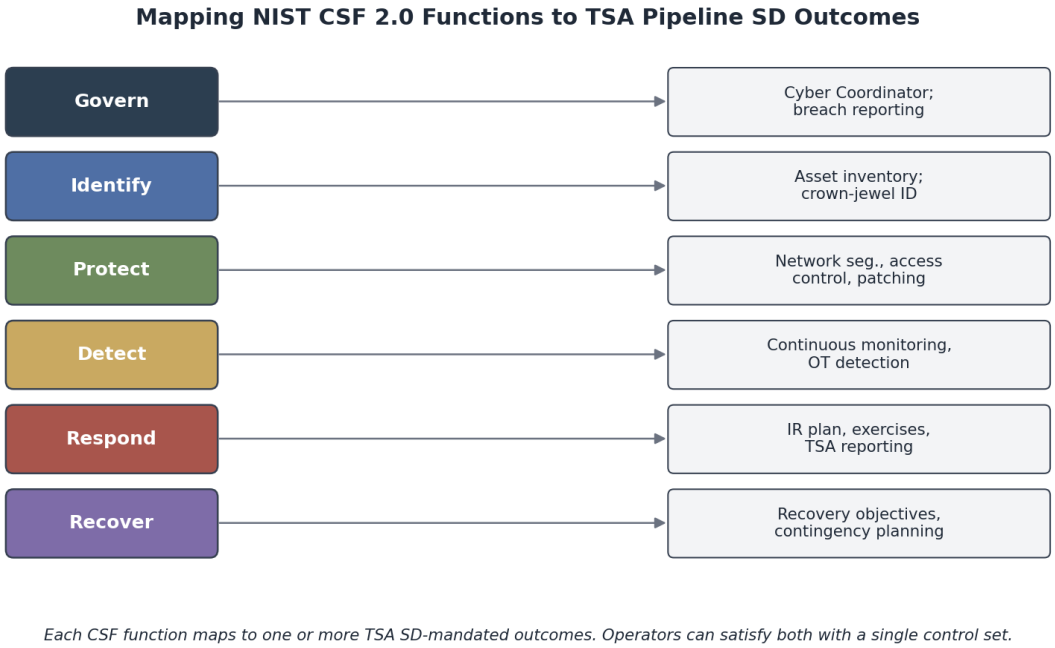

Figure.3. High-level mapping of NIST CSF 2.0 functions to TSA SD-mandated outcomes.

Govern naturally fulfills the NIST Directive requirements for a cybersecurity coordinator role, cybersecurity for the board and the expected reporting pace. The Identify function directly corresponds to TSA's need for critical cyber systems identification and the compilation of an asset inventory. The Protect function is the workhorse for segmentation, limiting user and system access and patching requirements. The Detect function covers continuous monitoring requirements. The Respond and Recover functions line up with incident response plans and recovery elements required by the TSA directives. The mapping is not neat, several TSA requirements are lifted from more than one CSF function and some subcategories in CSF also serve more than one TSA outcome. In practice, this allows one integrated set of controls to cover both TSA requirements and CSF implementation, while avoiding the dual maintenance of control evidence inventories for programs that integrate this compliance from the beginning.

There are two additional areas where these standards are in alignment. The first involves the supply chain. CSF 2.0 builds on the supply chain category in the new Govern function and TSA expects operators to carry out plans covering third-party access to systems and vendor security. Operators that established supply chain risk management practices in 2022 ahead of general cybersecurity regulatory trends (covered by this author in reference [5]) can reuse those practices, plans and controls for both TSA directives and CSF compliance. Second is ransomware. NIST released a Ransomware Risk Management Profile in February 2022 and CSF 2.0 generally reflects its recommendations [6]. The TSA assessment process inevitably involves looking at how well prepared operators are for a ransomware incident. A ransomware playbook that incorporates the NIST Ransomware Risk Management Profile and is tested on the same TSA assessment schedule covers more of the regulatory bases at a lower administrative burden than managing several disparate plans.

VI. IMPLEMENTATION SEQUENCE

If operators kick off the alignment activity today, they will end up with a defendable approach:

1. Take stock of all critical systems and rank them by their level of critical importance. This assessment is key to the TSA deployment plan and the CSF Identify section, forming a baseline for everything afterward.
2. Develop the necessary organizational policies, risk management plan, approach to supply chain risk and report format required by the Board. This fulfills the requirements of CSF Govern and the TSA for a designated coordinator and overview structure. Getting this in place ahead of time provides context for all the technical work that follows.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605019

3. In order of priority dictated by the threat landscape, strengthen key technical controls. Priority should be on phish-resistant authentication for the most important privileges, IT/OT network segmentation and pervasive monitoring of IT systems, IT applications and IT hardware assets. For each control, link its strengthening to both CSF-recommended subcategories and identified TSA program requirements to make the evidence compilation simple.
4. Develop and carry out a cybersecurity program with assessments. The outcomes will create correction action plans that will inform the revision of the next implementation plan. The cycle will then be complete.

VII. COMMON PITFALLS

The first is treating the implementation plan as a piece of paper, than as an ongoing control system. The plan should be the program, always. When the organization only remembers to update it in conjunction with the annual review for the TSA, ignoring the plan for 364 days of the year, the program wanders, the audit turns into a painfest and the remediation loop never closes. A successful program embeds the plan within the change control process such that when you change the environment in a material way, the plan gets updated days later, not months later.

The second trap is creating redundant evidence chains. If an organization maintains a separate set of documents and inventories for TSA, mapping to NIST, internal audit and board reports, then the company has three or four over-lapping, independently-tracked inventories that will drift away from the real environment at three or four independent rates. You need to identify everything in the asset inventory, tag it with the appropriate CSF sub-category and mark where it impacts the TSA implementation plan. This central repository for evidence will save the organization enormous effort down the road. There is a cost to do this, but a larger, less obvious cost of not doing it.

Third is not investing enough in monitoring and detecting on the OT side of the environment. The Detect function in CSF 2.0 requires the monitoring extend down into the OT environment, as does the continuous monitoring requirements in the TSA mandates. Companies that install IT grade SIEM and say they have covered their bases usually do not survive the audit inspection with these requirements. Remediation involves installing OT aware sensors and controls, building out OT-specific use cases, training analysts on industrial protocols and it takes 12-18 months. Doing so proactively is cheaper than doing it under the gun of an audit inspection.

The fourth pitfall is letting the governance follow, than lead, the technical activities. CSF 2.0 emphasizes a Govern function in CSF 2.0 and the TSA requires a coordinator and ongoing oversight activities based upon active executive management engagement. If policy documents get signed and locked away and the executives themselves are not involved on an ongoing basis, these programs can fall out of favor and lose funding when the budget gets difficult to stretch. Work in Govern is your political capital for the program. Treat this as a first-class deliverable.

VIII. CONCLUSION

There are a few big, big changes coming down in approximately the next year or so. 2.0 is slated to be published in early 2024 and the TSA security directives will keep changing over the next few years. Operators who treat these as distinct compliance exercises instead of two facets of the same security exercise, are probably going to spend a lot more money, document way more than they need to and probably be less defensible during audits. Because of the performance-based focus both top-down and bottom-up, the more that operators know exactly what they are doing and precisely why they are doing it and the more they have their documentation in order - painful though that is - the better their auditors will treat them, the higher that their CISO will trust them and generally the better their security program is. Next two years will be busy! Anyone that started to get ready earlier should be grateful.

REFERENCES

[1] National Institute of Standards and Technology, “The NIST Cybersecurity Framework 2.0,” Initial Public Draft, August 8, 2023.
[2] U.S. Department of Homeland Security, Transportation Security Administration, “Security Directive Pipeline-2021-01: Enhancing Pipeline Cybersecurity,” May 28, 2021.
[3] U.S. Department of Homeland Security, Transportation Security Administration, “Security Directive Pipeline-2021-02C and Pipeline-2021-02D,” December 2022 and July 2023.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605019

[4] National Institute of Standards and Technology, "Cybersecurity Framework Concept Paper: Potential Significant Updates to the Cybersecurity Framework," January 2023, and Discussion Draft, April 2023.
[5] V. Shewale, "Third-Party and Supply Chain Risk in Oil & Gas," December 2022.
[6] W. Barker, K. Scarfone, W. Fisher, and M. Souppaya, "Ransomware Risk Management: A Cybersecurity Framework Profile," NIST Interagency Report 8374, February 2022.
[7] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.1, April 2018.
[8] U.S. Department of Energy, "Cybersecurity Capability Maturity Model (C2M2)," Version 2.1, June 2022.
[9] U.S. Cybersecurity and Infrastructure Security Agency, "Cross-Sector Cybersecurity Performance Goals," October 2022, updated March 2023.
[10] U.S. Government Accountability Office, "Critical Infrastructure Protection: TSA Should Ensure That Pipeline Operators Address Cybersecurity Recommendations," GAO-22-104733, January 2022.
[11] U.S. Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation, "DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks," Joint Advisory AA21-131A, May 2021.
[12] American Petroleum Institute, "API Standard 1164: Pipeline Control Systems Cybersecurity," third edition, 2021.
[13] U.S. Department of Homeland Security, "Transportation Systems Sector-Specific Plan," most recent revision.
[14] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule, and M. Thompson, "Guide to Operational Technology (OT) Security," NIST Special Publication 800-82 Revision 3, Final Public Draft, April 2023.