May 22, 2024
Department of Homeland Security
United States Coast Guard
Docket No. USCG-2022-0802

Subject: The United States Coast Guard's Notice of Proposed Rulemaking, Cybersecurity in the Marine Transportation System, Docket Number USCG-2022-0802.

The National Ocean Industries Association (NOIA) submits this letter to supplement the attached comments jointly filed by NOIA, the American Petroleum Institute (API), the American Gas Association (AGA), the Interstate Natural Gas Association of America (INGAA), and the Offshore Operators Committee (OOC) in response to 33 CFR Parts 101 and 160, Cybersecurity in the Marine Transportation System. NOIA aims to provide additional context and clarity on this matter.

NOIA represents the interests of all segments of the offshore energy industry, including offshore oil and gas, offshore wind, offshore minerals, offshore carbon capture, use and sequestration (CCUS), and other emerging technologies. Our membership includes energy project leaseholders and developers and the entire supply chain of companies that make up an innovative ecosystem contributing to the safe and responsible development and production of offshore energy.

NOIA wholeheartedly endorses initiatives aimed at bolstering cybersecurity measures in the U.S. offshore sector, aligning closely with the objectives outlined in the proposed U.S. Coast Guard (USCG) Rule. Safety stands as a foundational pillar within our industry, intricately woven into every facet of operational protocols and decision-making processes. Historically, offshore platform systems operated in isolation, shielded from cyber threats by their disconnected nature. However, the evolving landscape of offshore energy production has ushered in an era of heightened connectivity, marked by the proliferation of remote monitoring, autonomous control systems, and the Internet of Things (IoT). Consequently, this paradigm shift underscores the imperative for continuous advancements in cybersecurity to safeguard against emerging threats and ensure the integrity and resilience of offshore operations in today's digital age.

The Bureau of Safety and Environmental Enforcement (BSEE) is already in the process of developing regulations to tackle cybersecurity concerns in the offshore sector. **Considering BSEE's specialized expertise and regulatory authority over offshore operations, it is reasonable to exempt offshore facilities from additional cybersecurity regulations pursued by other agencies, such as the USCG.** Having potentially redundant regulations could open the door to confusion over the roles and authorities of BSEE and USCG on the OCS and detract from the universally shared goal of improving cybersecurity in the offshore sector.

BSEE is actively engaged in developing cybersecurity rules tailored to offshore platforms, recognizing its primary role in regulating safety and environmental protection in the offshore oil and gas industry. As affirmed by BSEE Director Kevin Sligh Sr.[1], efforts are underway to mitigate both physical and cyber threats to offshore energy activities, with a dedicated focus on addressing cybersecurity risks. Director Sligh's commitment to this cause, alongside the ongoing collaboration with the BSEE team, underscores the agency's dedication to ensuring robust safety measures across offshore operations.

[1] https://www.bsee.gov/bsee-proactively-addressing-cybersecurity-and-offshore-energy-production-0

The urgency of BSEE's cybersecurity initiatives is further underscored by a recent Government Accountability Office (GAO) report, which recommended the immediate development and implementation of a strategy to address offshore infrastructure risks[2]. This recommendation, concurred with by the Department of the Interior, highlights the need for a comprehensive approach that assesses and mitigates risks, defines objectives and responsibilities, and allocates necessary resources.

The primary focus of BSEE is on safety and environmental protection in the offshore oil and gas industry, ensuring adherence to safety standards and environmental regulations. This specialized focus allows BSEE to have a deeper understanding of the unique challenges and risks associated with offshore platforms compared to the broader responsibilities of the USCG.

Furthermore, BSEE has direct regulatory authority over developing and enforcing regulations related to safety, well integrity, and environmental protection on offshore platforms. In contrast, while the USCG plays a crucial role in maritime safety and security, its regulatory authority primarily extends to vessel operations and navigation, rather than the specific operational aspects of offshore platforms.

BSEE works closely with industry stakeholders, including operators, contractors, and environmental organizations, to develop regulations that are practical, effective, and feasible for offshore operations. This collaborative approach allows BSEE to leverage industry expertise and best practices in developing rules that enhance safety and environmental protection while also considering the operational realities of offshore platforms.

It remains paramount that any cybersecurity regulations extending to offshore facilities are developed with a clear understanding of the operational nuances and existing infrastructure. **Thus, should the USCG continue with its intention to implement the proposed rule in a manner affecting offshore facilities, it is imperative that realistic implementation timelines are established.** These timelines necessitate thorough due diligence and comprehensive cataloging of current systems to ensure practicability and effectiveness in safeguarding both marine transportation and offshore operations.

If the USCG determines the proposed rule still applies to offshore facilities, we propose the USCG adopt a multi-year phased approach to facilitate a smooth transition and comprehensive adherence to the regulatory requirements. This approach aims to provide a systematic framework for stakeholders to align with the regulations effectively. A multi-year phased approach could adhere to the following schedule:

- Year 1: Education and Awareness
    - Focus on disseminating information about the specific requirements outlined in 33 CFR Parts 101 and 160.
    - Conduct training sessions and workshops to educate stakeholders on the importance of compliance.
    - Establish communication channels for queries and clarifications regarding the regulations.
- Year 2: Preparation and Planning
    - Encourage stakeholders to assess their current practices and identify gaps in meeting 33 CFR Parts 101 and 160 standards.
    - Develop internal protocols and procedures to align with the regulatory requirements.
    - Facilitate consultations with experts to address any challenges in implementation.
- Year 3: Implementation and Monitoring
    - Initiate the formal implementation of 33 CFR Parts 101 and 160 regulations across all relevant sectors.

[2] https://www.gao.gov/products/gao-23-105789

    - Conduct regular audits and inspections to ensure ongoing compliance.
    - Establish reporting mechanisms for incidents, improvements, and feedback on the implementation process.
- Year 4: Evaluation and Enhancement
    - Evaluate the effectiveness of the phased approach in achieving compliance with 33 CFR Parts 101 and 160.
    - Identify areas for improvement and enhancement based on feedback from stakeholders.
    - Modify strategies and procedures as necessary to streamline compliance processes.
- Year 5: Sustainability and Continuous Improvement
    - Emphasize the importance of sustaining compliance with 33 CFR Parts 101 and 160 regulations.
    - Encourage a culture of continuous improvement through feedback mechanisms and best practice sharing.
    - Monitor industry trends and regulatory updates to adapt practices accordingly.

This multi-year phased approach aims to provide a structured pathway for stakeholders to gradually integrate 33 CFR Parts 101 and 160 requirements into their operations effectively. By following this plan, stakeholders can navigate the complexities of regulatory compliance while ensuring safety, environmental protection, and operational efficiency.

In conclusion, the National Ocean Industries Association (NOIA) offers this letter to supplement the joint comments provided by API, AGA, INGAA, NOIA, and OOC. Our collective membership remains committed to fostering innovation and ensuring the safe and responsible development of offshore energy resources.

We appreciate your consideration of the matter.

Sincerely,

Erik Milito,
President
National Ocean Industries Association

May 22, 2024
Department of Homeland Security
United States Coast Guard
Docket No. USCG-2022-0802

Subject: The United States Coast Guard's Notice of Proposed Rulemaking, *Cybersecurity in the Marine Transportation System,* Docket Number USCG-2022-0802.

The American Petroleum Institute (API), its members, and other like trade associations, to include the American Gas Association, the Interstate Natural Gas Association of America, the National Ocean Industries Association, and the Offshore Operators Committee, (collectively, "Commenters") offer the following comments on the United States Coast Guard's Notice of Proposed Rulemaking, "Cybersecurity in the Marine Transportation System," Docket Number USCG-2022-0802. Commenters represent all facets of the natural gas and oil industry, which supports 10.3 million U.S. jobs and nearly 8 percent of the U.S. economy. The Commenters represent large integrated companies, as well as pipeline, exploration and production, refining, marketing, marine businesses, and service and supply firms. They provide most of the nation's energy and are interested in the increased protection of critical energy infrastructure. The Commenters hope to have constructive dialogue with the Coast Guard to better understand its approach, address areas of the proposal which may need clarification, and resolve how industry can effectively implement a final rule to ensure we are progressing towards the goal of increased cyber security where the risk warrants it.

Commenters are committed to safe, secure, and environmentally responsible operations that eliminate or reduce potential risks to the public, employees, contractors, and operations. Safety and security are key elements in all operations, and we continue to work with regulators across the government to ensure we are operating in a manner that protects critical infrastructure sites, promotes safe practices, meets regulatory requirements, and improves our country's access to reliable energy. The proposed rule has three overarching shortcomings: (1) it did not benefit from sufficient consultation with industry, (2) it is not risk-based nor sufficiently based on the NIST framework, and (3) it is not harmonized with other related regulations and programs, notably from the Transportation Security Administration's (TSA) and from the Cybersecurity and Infrastructure Security Agency (CISA).

While the Commenters appreciate the Coast Guard's progress on these important issues, Commenters believe that the Coast Guard needs to work with industry to ensure any new requirements are safe, technically feasible, and informed by risk. In general, it appears the aims of the Coast Guard and Transportation Security Administration's (TSA) Security Directives (SDs) largely

align in that they are based on the NIST framework and have the security of operations as a paramount outcome. With that, having two different approaches from federal agencies stands out as an oddity at best. Given that TSA is possibly weeks away from releasing its own NPRM and the Cybersecurity and Infrastructure Security Agency (CISA) has now published its NPRM for cyber incident reporting,[1] the question of full alignment between the three proposals (where appropriate) should be resolved. Given that many operators subject to MTSA also fall under the current TSA SDs, there is now the potential for those operators to be required to follow different paths internally to achieve the same outcome for their assets. As stressed in the National Cyber Security Strategy, agencies should harmonize their rules and programs as often as possible to avoid this type of duplication and burden on the industry.[2] Additionally, the USCG should clarify the disposition of the NVIC Circular No. 01-02 once the cyber regulations in this NPRM are enacted.

Scope

Commenters request the Coast Guard clarify the applicability of this rule to certain facilities that may already be covered under other regulations. The Coast Guard should be explicit in where MTSA starts for cyber security for those facilities subject to TSA Security Directives. The Commenters request the Coast Guard limit docking ship connections to those systems necessary for mooring, emergency operations, and ship-to-shore communications. The Coast Guard should further clarify coverage in tandem with TSA or expressly state that if a facility falls under TSA regulations, it is not subject to the rule. Commenters also share concerns that the inclusion of a subset of offshore facilities creates confusion and potential redundancy for the larger offshore community, given the Government Accountability Office's report[3] recommending the Bureau for Safety and Environmental Enforcement (BSEE) develop a cyber security strategy for the offshore industry. Commenters do not want multiple sets of regulations for different subsets of the offshore industry. Given the shared authority on the Outer Continental Shelf (OCS) by the Coast Guard and BSEE as provided in the Outer Continental Shelf Lands Act (OCSLA), we urgently request the Coast Guard remove the application of this NRPM to offshore facilities subject to 33 CFR 106.

Instead, the Coast Guard and BSEE should, under their existing MOU, develop an Memorandum of Agreement specific to Cybersecurity to better define their respective roles and authorities on the OCS related to Cybersecurity concerns. We believe this is further underpinned by the recommendation in GAO report GAO-23-10578 dated October 2022. In this report, the GAO made the sole recommendation that BSEE "should immediately develop and implement a strategy to address offshore infrastructure risks. Such a strategy should include an assessment and mitigation of risks; and identify objectives, roles, responsibilities, resources, and performance measures, among other things." The most effective way to ensure a robust cybersecurity posture on the OCS is to involve both primary OCS regulators so that a harmonized and holistic approach can be taken. We do not believe this can be done under the current NPRM as it would only apply to thirty-three OCS facilities in the Gulf of Mexico (GOM) and does not address drilling units as they are all foreign-flagged vessels. For context, there are over 1600 OCS facilities in the GOM with over 450 of those being manned facilities. There are 23 OCS facilities on the California OCS with 22 of those being manned and none meeting the compliance threshold for MTSA in 33 CFR 106. Further, OCS

---

[1] https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements

[2] [2] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[3] https://www.gao.gov/products/gao-23-105789

operations (drilling and production) fall under BSEE authorities and most Information Technology/Operational Technology (IT/OT) systems on OCS facilities perform functions related to operations under BSEE authority versus the Coast Guard. Attempting to implement cybersecurity regulations on the OCS via the limited scope of the MTSA will result in an incomplete effort and create the possibility that OCS operators may eventually have to contend with overlapping and potentially dissimilar regulations from two different agencies.

Further, Commenters request the Coast Guard provide its definition of Marine Transportation System (MTS). We are not able to identify an official Coast Guard definition and all references made to the MTS in related Coast Guard policy (e.g., NVIC 02-24) indicate this is limited to "vessels, harbors, ports, and waterfront facilities." Given this, we request clarification from the Coast Guard as to how OCS facilities fit within the context of how it describes (the) MTS. Commenters also recommend that the Coast Guard consider scope segregation (e.g., terminals, platforms, ships) to provide greater clarity on mitigations and risk reduction, as well as provide remediations that can realistically be achieved for the asset.

Clarity of Terms

The Coast Guard should endeavor, whenever possible, to harmonize definitions with other existing regulations and guidance. The 2023 National Cyber Security Strategy explained why this is important, "Our strategic environment requires modern and nimble regulatory frameworks for cybersecurity tailored for each sector's risk profile, harmonized to reduce duplication, complementary to public-private collaboration, and cognizant of the cost of implementation."[4] For continuity, Commenters recommend that all definitions align with the NIST Computer Security Resource Center (CSRC). As published, some of the definitions in this proposal lack clarity. For example, under Section 101.615—Definitions, it is unclear what a "significant number of individuals" is or what could be considered under "Other potential operational disruption."

Commenters note that in section (160.202) Hazardous Conditions, it is not recommended to include cyber incidents to the series of "Hazardous Conditions." Unintended consequences could include an oversharing of sensitive information in the area during a cyber event that is not truly affecting marine operations such as a loss of confidential information. If cybersecurity were to be added to the series of "hazardous conditions," it would be important to note that additional reporting requirements outside of CISA reporting noted below would not be recommended. Furthermore, the Coast Guard may want to confirm the application of this definition to marine terminals or outer continental shelf (OCS) facilities. Much of this section falls under vessel requirements and may cause confusion.

Regarding the two reporting options for which the Coast Guard has requested comments, Commenters are comfortable with either option, as long as the National Response Center (NRC) and CISA are sharing the information. Industry has a long history of reporting to the NRC but Commenters also recognize that the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)[5] will soon be in effect, which might supersede any NRC reporting based on the text of the CIRCIA final rule. Furthermore, some industry members are already reporting to CISA, either based

[4] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[5] https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements

on the TSA's Security Directive 2021-01C or voluntarily. As stated in the NPRM, Commenters agree that duplicative reporting should not be required. Regarding reporting of ransomware payments, that should be addressed between the operator and law enforcement, as appropriate, and in line with the rules of active investigations, as well as any forthcoming CIRCIA requirements. Now that CISA has published their NPRM for CIRCIA, USCG should work closely with CISA to harmonize their respective reporting requirements, as directed by the National Cyber Security Strategy. The Coast Guard should also clarify that the reporting requirements are for the MTSA covered facility or vessel and not for any other corporate events not impacting a MTSA facility or vessel.

There is also some confusion about the definition of the cyber security officer. It is unclear whether this is required to be a singular person and whether they would be responsible for 24/7 response. Some of the covered facilities are very large, complex industrial operations, requiring large teams to address what is laid out for one person in the proposed rule. It may be difficult for some operators to consolidate their information technology (IT) and operational technology (OT) functions that are often managed at an enterprise level for IT and locally for OT. The NPRM states: "The most important duties a CySO would perform include ensuring development, implementation, and finalization of a Cybersecurity Plan; auditing and updating the Plan; ensuring adequate training of personnel; and ensuring the U.S.-flagged vessel, facility, or OCS facility is operating in accordance with the Plan and in continuous compliance with this subpart." These duties are currently often managed across multiple organizational units, requiring many different skill sets. While many operators are used to conducting exercises and drills under the Oil Pollution Act of 1990 requirements, those personnel would not be appropriate to create and maintain a cyber security plan with technical and operational requirements. The expectation that the individual or their alternate is reasonably accessible is acceptable. Therefore, Commenters recommend the addition of alternate cybersecurity contacts. While we acknowledge the Coast Guard allows for designation of responsibilities, we encourage the Coast Guard to provide a longer implementation time to ensure all of the roles and responsibilities can be identified by the operator, resourced, trained, and implemented adequately. The Coast Guard should also consider changing the wording from responsible for to accountable for, to acknowledge how these requirements will be staffed and implemented.

Commenters note that Backup is currently defined as " a copy of physical or virtual files or databases in a secondary location for preservation." The primary issue with the concept of backup within the proposed rule is it lacks the flexibility to rebuild or re-instantiate a system from something other than a backup. When restoring from backups, time can be a limiting factor. Therefore, we commend the Coast Guard broaden this proposed definition, as well as remove the prescriptive requirement of all backups taking place offsite. The Coast Guard should also recognize that it may not be feasible for most operators to test backups (i.e. restoring onto systems), especially frequently. Tools can be used to check if backups are successful, but it would not be risk-justified to do full tests. Based on risk, it may be appropriate to backup locally due to network constraints.

Commenters note that KEV is currently defined as: "Known Exploited Vulnerability, or KEV, means a computer vulnerability that has been exploited in the past." Many vulnerabilities are in theory known and potentially exploited in the past. This proposed definition lacks the important reference to the CISA Known Exploited Vulnerability Catalog[6]. Commenters also note that Multifactor

[6] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Authentication (MFA) is currently defined as "a layered approach to security data and applications where a system requires a user to present a combination of two or more credentials to verify their identity for login." While this proposed definition originates from the current CISA definition, MFA is more appropriately defined as something you know (such as a password) and something you have (such as a token) or something you are (biometrics). This proposed definition should be adjusted accordingly. The Coast Guard should also acknowledge that MFA is not always technically feasible. MFA for control systems in the OT zone can introduce serious risk. In an emergency, the top priority is swift, reliable access to the control system by the local operators. MFA could be a requirement for outside access such as remote support for diagnostics by the vendor. However, MFA should not be required for local operators. As TSA discovered during the implementation of Pipeline -2021-02A, there are pieces of equipment in the operating environment that were not manufactured with the ability to have MFA. Hence the changes to Pipeline -2021-02C, which provides more performance-based measures to achieve the same outcomes. Capturing firmware levels on isolated hardware can also be burdensome and not reduce risk. Additionally, Principle of least privilege is currently defined as "an individual should be given only those privileges that are needed to complete a task. Further, the individual's function, not identity, should control the assignment of privileges." The first sentence is an appropriate definition. The second clarifying sentence is overly prescriptive and confusing and should be removed. The Coast Guard should review these requirements in the framing of risk to the operations to ensure that any measures are increasing safety and security and reducing overall risk.

Cyber Security Plan Requirements

Commenters note that in its current form, the rule lacks scoping, and specifically, criticality. It is recommended to align with other cybersecurity frameworks that require the identification of "Critical Cyber Systems" providing the operator the ability to focus scope to what is important for the given organization. The proposed rule would then allow the operator, through their plan, to outline how security measures are applied to these Critical Cyber Systems. The concept of "secure everything the same way," is not risk-based and sets the rule up for failure. For instance, should unmanned tank barges, with negligible cyber infrastructure be included in this proposed rule? Additionally, there is a lack of clarity whether one plan for a fleet is acceptable, or if each facility and vessel requires its own plan. Commenters request the Coast Guard explicitly address this issue. It is also not clear why the results of the Cyber Assessment would sit in the Cyber Plan. It would be safe to say that the plan should address risks/vulnerabilities found in the assessment; but including potentially very sensitive risks in the plan document seems unwise and may open a path to compromise if control of the plan was inadvertently lost. The assessment itself should be highly protected. Commenters also note that changes to the Cyber Assessment should drive updates to the Cyber Plan. It's not clear why changes in the Plan would force an Assessment (presumably, the plan addresses the assessment as noted above). The proposal, as written, seems backwards. Commenters request clarity from the Coast Guard regarding plan audits and when resubmittal is required. A table illustrating the process and timeline would be helpful.

The Commenters have significant concerns about the process for plan submission and approval. While we respect the experience and authority of the Captain of the Port (COTP), Officer in Charge, Marine Inspections (OCMI) for U.S. facilities and OCS facilities, or to the U.S. Coast Guard's Marine Safety Center, we do not have confidence that they have the technical expertise to review and

approve what will be highly technical cyber security plans. Nowhere in the proposed rule has the Coast Guard laid out how, internally or at the local level, they are planning to implement and execute the proposed rule. As industry has experienced with the TSA Security Directives, significant technical expertise and personnel are required on the government's side to implement a rule such as this. There are also concerns with the process to address deficiencies. 60 days appears to be an arbitrary number. In complex operational environments, it is often the case that changes cannot be made in arbitrary timelines. For example, patching in OT environments needs to be tested first in test environments, often involving the vendor to maintain service level agreements.

Often the patch may need to be delayed until a maintenance period or downtime can be scheduled. We propose the term "without delay" be removed to allow updates for patches and system outages to be a risk-based decision the company makes. Companies should be allowed the flexibility to follow internal protocol / procedures to address these issues. Commentors also have concerns that the proposal requires that operations "remains in compliance with the submitted Cybersecurity Plan" while simultaneously allowing the COTP, OCMI, or MSC to await subsequent review and approval from the Coast Guard before accepting the Cybersecurity Plan. It is unclear how operations can "remain in compliance" with a plan that has not yet been accepted. While we appreciate the flexibility for "each owner or operator to determine what constitutes a "major amendment" as appropriate for their organization based on types of changes to their security measures and operational risks," this creates its own uncertainty. In the final rule, the Coast Guard should be more explicit or provide thresholds or examples of what it considers "major." Factors such as cost and operational burden should be considered (e.g., more operators/employees, more equipment). The threshold may be a percent of the current cyber budget since each company will be different. This will also provide clarity for the COTP who will be interpreting the rule. The Coast Guard should also clarify what systems require penetration testing, as there are very different consequences for IT versus OT. Commenters note that penetration testing is challenging for OT in general as entire sites must be shut down to perform such testing. Penetration testing in OT environments also raises safety concerns if operations are impacted that cause physical repercussions. Commenters suggest the Coast Guard consider accepting penetration testing of the same architecture but in a lab environment or penetration testing of the IT environment only which may be allowed in non-critical systems.

Specific to section (101.650(b)(2)) Macros: The statement "ensure applications running executable code must be disabled by default on critical IT and OT systems" is unclear and needs adjustment. It appears it may be referring to how applications that allow additional code to execute should be governed, but this is unclear. Additionally, specific to 101.650(c)(2)) Data Security Measures: The requirement that "All data, in transit and at rest, must be encrypted using a suitably strong algorithm" lacks scope and intent. This requirement, as worded, is not feasible without appropriate scope. It is recommended to apply scope delineators such as "Sensitive data on critical cyber systems…"

Cyber Security Measures

Generally, Commenters advise the Coast Guard to take a risk and performance based, rather than a prescriptive approach, to cyber security measures. The evolution of TSA's SD2 from the first version,

A, to the current version, D, is a considerable example of the difficulty of prescriptive requirements in complex IT and OT environments. Allowing operators to determine the best measures to reach certain outcomes is more effective and efficient. For example, allowlisting poses an issue for IT systems, due to the quantity of applications. Allowlisting would require support from, testing, and approval from the various vendors. Operators cannot make such a change on their own and vendors currently do not support this. Beyond allowlisting, there are a number of compliance issues with regards to modifying, configuring, patching, etc. systems which are entirely -- and only -- accessible by the vendors. This affects a great deal of an operator's ability to control compliance as the vendors themselves are the only entities with such access. This is likely a legacy error based on this part's derivation from parts 104 and 105 in which owner/operators *do* have the ability to control physical security.

Regarding, "all data, in transit and at rest, must be encrypted using a suitably strong algorithm" (101.650): the Coast Guard should clarify if it is referring to OT system data as well as IT data. Requiring that all data in transit (presumably all transit) be encrypted removes the ability to inspect traffic at network boundaries for the purposes of anomaly detection. The Coast Guard should acknowledge that encryption within the OT zone could inhibit smooth communication between critical control systems. No encryption should be required for data that remains within the OT zone. If encryption is used for data leaving the OT zone, it does deny the vessel owner the ability to inspect the traffic. Only data exposed outside of internal networks in transit and at rest, and confidential and sensitive data within company networks at rest, should be encrypted. Encrypting traffic would consume limited bandwidth. It is reasonable however to require encryption on internet traffic that is departing the vessel. Additionally, this sub-section does not specify if decryption at boundary transitions is acceptable. The requirement for control measures to limit access to restricted areas and detect unauthorized introduction of devices capable of damaging U.S.-flagged vessels, U.S. facilities, OCS facilities, or ports is not appropriate for critical systems requiring physical interaction to access. In fact, this creates an attack scenario in which a malicious insider may disable access to critical systems by simply repeatedly failing logons until the system is locked out even for legitimate users. The Coast Guard should consider that in OT control systems there is typically a general account for "operator" that is tied to a role onboard not an individual. The operator account has limited privileges. Superuser access is reserved by the vendor. The existence of a superuser account is not a threat. The requirement for individual credentials in the OT space (control systems) does create a safety hazard. In an emergency, swift common access to the controls is paramount. Compensating controls such as strong network segmentation mitigate against the need for individual credentials in the OT zones.

Commenters suggest the Coast Guard use already developed language from TSA Security Directive (SD) Pipeline -2021-02D to describe minimum Account Security Measures. Conducting a cybersecurity assessment for every facility annually is excessive, especially if the facility or systems have not changed significantly. Commenters suggest a cybersecurity assessment should be required at least every 5 years or if the facility and/or systems undergo significant changes. Requiring operators to document and mitigate any unresolved vulnerabilities is an unobtainable ask when considering IT and OT systems - just because a device or application has a vulnerability doesn't mean that it is exploitable or a risk to the specific local system or environment. Commenters have concerns over the implied timeframe to mitigate these vulnerabilities immediately. In some cases, such as lifecycle upgrades of assets, it can take one more business cycle to complete due to planning, budgeting, funding and execution. Also, the order of applied

mitigations should be risk-based across the entire program, not just from the findings of an audit or an individual exercise.

The Coast Guard should consider requiring a vulnerability program that owners/operators would establish to assess vulnerabilities and take action if and when needed. Commenters also note that there is already a well-established process through CISA to share KEVs, and the Coast Guard should not require another one in this rulemaking.

Regarding the Coast Guard's suggested requirements for cyber security training for personnel, the Commenters believe these requirements are overly broad for the workforce. This appears to be excessive training on current knowledge of threats/countermeasures. Requiring all personnel with access to IT or OT systems essentially covers all personnel in some capacity. Expecting all personnel to recognize and detect cybersecurity threats and all types of cyber incidents and to recognize techniques used to circumvent cybersecurity measures would be to essentially make all personnel cyber security experts. While we recognize that everyone should practice good cyber hygiene, these requirements should only apply to those personnel identified by the CySO based on the risks of personnel access levels.

Drills and Exercises

Commenters suggest drill frequency should be based on the risk of the facility, and where risk is low, aligned with current exercise requirements under the NPREP guidelines:

> "The National Preparedness for Response Exercise Program (PREP) was developed to establish a workable exercise program that meets the intent of section 4202(a) of the Oil Pollution Act of 1990 (OPA 90), amending section 311 (j) of the Federal Water Pollution Control Act (FWPCA), by adding subsection (6) and subsection (7) for spill response preparedness (33 United States Code (U.S.C.) § 1321 (j)). PREP was developed to provide a mechanism for compliance with the exercise requirements, while being economically feasible for the U.S. Government and oil industry to adopt and sustain."[7]

The Coast Guard should also explore what is gained by the prescribed frequency. The goal should be to balance resources to achieve objectives. The Coast Guard should clarify if drills are a comprehensive (meaning the entirety of cybersecurity capabilities outlined in the Cybersecurity Plan) test of duties and implementations. By this interpretation, drills will require that all operations be halted every 90 days to conduct the drill for the duration of the drill. A comprehensive drill will potentially encompass days or weeks, during which the facilities and vessels will be unable to conduct their intended operations. Additionally, it is uncommon for all vessels involved to be in port during a single period, which means drills will involve vessels underway. If during a drill operators need to suspend operations for portions of the system they are drilling, this could be incredibly challenging as outages are required (103.635)(a)(1). Table-top exercises will not and cannot be a "full test of the cybersecurity program". By definition, exercises of this nature are simulated, scripted events that test processes associated with communications, incident response, and decision-making. The "full cybersecurity program" -- as detailed throughout this notice -- involves technologies, training, audit, vulnerability management and many more aspects of cyber security. Table-top exercises were defined as

[7] https://www.phmsa.dot.gov/national-preparedness/national-preparedness-response-exercise-program-prep

an exercise choice in 103.635. This sub-section declares table-top exercises to be a requirement. The Coast Guard should clarify if this supersedes 103.635 (103.650)(3)(g)(3).

Supply Chain Management

Commenters support efforts to secure the supply chain for our critical energy operations but the Coast Guard should also recognize the daunting challenge that poses for the country. As acknowledged by the Administration's initiative to bolster cyber security at U.S. ports,[8] much of the supply chain for the maritime transportation system is not based in the U.S. The Coast Guard should work with operators to ensure that while they are addressing risk, they need to also remain reliable. Requirements should focus on the most at-risk operations and equipment, with an acknowledgement that not all risks can be drawn down in the supply chain. The broad language in this section does not reflect what may be possible and what might not be in terms of supply chain management. The Coast Guard should ensure that their efforts, with the rest of the federal agencies, are providing the most current threat information on supply chain vulnerabilities.

Feasibility of Network Segmentation

The Coast Guard should focus on risk as it relates to network segmentation. Some communications may be necessary between IT and OT systems that can be accomplished without introducing risk. Operators should have the flexibility to document how they can accomplish this without an overly prescriptive prohibition. Commenters encourage the Coast Guard to propose a language specific to shipping that considers the unique operating environment and realities, vendor maturity of the marine industry, and the fact that vessels are not always ashore. This proposal should aim to align with international marine cybersecurity standards and the efforts of marine classification societies to improve maritime cyber security. Vessel OT cybersecurity management differs from other types of critical infrastructure given how ships are designed and built, and cybersecurity controls in place currently are unique to vessels. In OT environments, vessel cybersecurity risk is managed through perimeter security, pathway maintenance, rigorous segmentation and other safeguards not accurately captured or accounted for in this proposal. Commenters also propose vendor accountability/compliance for OT-specific requirements. The Coast Guard should partner with vendors, DHS and CISA to further the progress of vessel cybersecurity.

Burden

This rule, if enacted, will be a considerable burden for some operators, with questionable cyber security benefits, given the shortcomings of the proposed rule outlined in the rest of the comment letter. The Coast Guard should allow appropriate time and flexibility for operators to understand the requirements, develop plans, exercise, and implement those plans. Commenters encourage the Coast Guard to provide enough time for facilities to prepare for related inspections following this rulemaking (for example, TSA gives about a month or more whereas recently the Coast Guard has given only a week). The Commenters encourage a collaborative approach as this will be a new experience for both the Coast Guard and many of the operators. The commenters also have concerns related to the burden on the Coast Guard. As noted earlier, this proposed rule does not address what resources the Coast Guard will use to implement

[8] https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/21/fact-sheet-biden-harris-administration-announces-initiative-to-bolster-cybersecurity-of-u-s-ports/

this rule. The technical expertise needed to review and approve cyber security plans for more than 13,000 facilities and vessels is considerable for a service that is already overburdened and understaffed.

Also, as it concerns OCS facilities, the Coast Guard does not delineate between these and (waterfront) facilities in their assessment of impact and associated economic analysis. Instead, they are grouped together or collectively referred to as "facilities" with a total affected population of 3411 representing 1708 owners and operators. Given the known deficiencies with the Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database (see GAO-20-562, published July 16, 2020) Commenters have serious concerns regarding the accuracy of the Coast Guard's economic analysis of this proposed rulemaking. USCG District Eight has all 33 CFR 106 compliant OCS facilities in their Area of Responsibility (AOR), and these are inspected by their OCS OCMI Division. This number of OCS facilities is currently 33, operated by 9 different entities. Additionally, it does not appear the Coast Guard identified the government costs associated with inspecting these OCS facilities. Historically, District Eight has accomplished this via a commercial helicopter contract they maintain but this cost does not appear to be captured in the NPRM. Likewise, the NPRM does not accurately contemplate the limited onsite inspection time USCG OCS Inspectors spend on OCS facilities. They usually only make short day trips, and these are further constrained by distance offshore (travel time), weather, and the need to balance MTSA oversight with inspecting other items under the USCG's purview. Commenters understand USCG District Eight has reduced its commercial helicopter budget substantially and the Coast Guard is joining BSEE on their offshore trips using the BSEE commercial helicopter contract. Since this will reduce the number of USCG Offshore Inspectors who can attend an inspection and be driven by BSEE's schedule, we believe this will further encumber the Coast Guard's ability to adequately oversight existing MTSA plan implementation, let alone the additional oversight required by this NPRM.

Conclusion

The Commenters look forward to further dialogue and engagement with the Coast Guard as they review the comments and consider how to move forward. As with the TSA's Security Directive implementation, developing cyber security rules for industry is best done in close consultation with those operating the systems, and with risk at the top of mind. The Coast Guard should be careful to avoid prescriptive requirements that could impact operational reliability, safety, or the environment. Requirements should be based on existing guidance and in harmonization with other requirements and laws. As noted in the White House's press release, "America's prosperity is directly linked to maritime trade and the integrated network of ports, terminals, vessels, waterways, and land-side connections that constitute the Nation's Marine Transportation System (MTS)."[9] Any rules that impact the reliability of this system must be carefully considered from a perspective of risk to critical assets and systems. Cyber security should not come at the cost of reliability. The commenters fully support the goal of a safe and secure MTS and are committed to working constructively with the Coast Guard and industry members to achieve that goal.

Sincerely,

Suzanne Lemieux
Director, Security and Emergency Management
American Petroleum Institute

[9] https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/21/fact-sheet-biden-harris-administration-announces-initiative-to-bolster-cybersecurity-of-u-s-ports/

Kimberly Denbow
Vice President, Security & Operations
American Gas Association

Maggie O'Connell
Director of Security, Reliability, and Resilience
Interstate Natural Gas Association of America

Erik Milito
President
National Ocean Industries Association

Stephanie Kusinski
Environmental and CCS Manager
Offshore Operators Committee