

**NATIONAL OFFSHORE SAFETY ADVISORY COMMITTEE (NOSAC)**  
**CYBERSECURITY/CYBER RISK MANAGEMENT ON THE U.S. OUTER CONTINENTAL**  
**SHELF**

**SC's Findings and Recommendations for Phase I & II of the Task**

## Table of Contents

Background.....	3
Executive Summary .....	4
Phase I .....	4
Phase I .....	8
Responses to Questions 1 - 8 .....	8
Phase II .....	16
Centralized information and data sharing .....	16
Identify the steps and processes required in developing a Cybersecurity / Cyber Risk Program, Benchmarks, and Best Practices.....	20
Industry Definition.....	32
Exhibit A - Acronyms .....	35
Exhibit B – NOSAC CyberSecurity Risk Sub-Committee Recommended Reporting Format.....	37

**NATIONAL OFFSHORE SAFETY ADVISORY COMMITTEE (NOSAC)**  
**CYBERSECURITY/CYBER RISK MANAGEMENT ON THE U.S. OUTER CONTINENTAL**  
**SHELF**

**SC's Findings and Recommendations for Phase I & II of the Task**

## Background

National Offshore Safety Advisory Committee (NOSAC) has been very interested in the topic of cybersecurity and over the past two years has asked the U.S. Coast Guard (USCG) to keep the Committee updated regarding their efforts and actions on this topic. The concern of NOSAC is that the maritime/oil and gas industry as a whole faces a growing threat of potential cyberattacks on the U.S. Outer Continental Shelf (OCS). On December 18, 2014, the USCG published in the Federal Register a request for comment on "Guidance on Maritime Cybersecurity Standards". Respondents were requested to comment on eight (8) questions that would assist USCG in developing policy to help vessel and facility operators identify and address cyber-related vulnerabilities that could contribute to a Transportation Security Incident (TSI). The NOSAC membership generated a Task Statement Draft enabling them to comment on the eight (8) questions, with an additional item allowing them to discuss other cybersecurity related items with the USCG. On April 8, 2015, the NOSAC membership voted unanimously to stand up a SC (SC) for USCG's Task Statement on Cybersecurity on the U.S. OCS, and the following co-chairs were approved, Kelly McClelland and Patrice Delatte.

At the first SC meeting, the consensus of the participants was that the task was focused around how the industry should be identifying and managing the rapidly increasing risk and threat associated with cyber systems and networks in their operations. For this reason, we have titled this task response: "Cybersecurity/Cyber Risk Management on the U.S. Outer Continental Shelf."

The SC conducted nine (9) meetings:

**Phase I** - The SC conducted five (5) meetings:

1. May 12, 2015, with 30 attendees

2. June 18, 2015, with 24 attendees
3. September 15, 2015, with 31 attendees
4. November 17, 2015, with 20 attendees
5. November 18, 2015, (prior to the NOSAC Public Meeting), with 22 attendees

**Phase II** - The SC conducted four (4) meetings:

1. January 5, 2016, with 18 attendees
2. January 14, 2016, with 34 attendees
3. February 25, 2016, with 23 attendees
4. March 29, 2016, with 26 attendees

In addition, Phase II deliberations were divided into Focus Groups that conducted many teleconference meetings to accomplish their objectives.

All meetings allowed participants to call in via teleconference if they were unable to attend in person. SC participants represented offshore supply vessels, drilling contractors, offshore operators, classification societies, law firms, OEM manufacturer, security professionals, ex-military, academia, and industry associations: International Association of Drilling Contractors, American Petroleum Institute (API), and Offshore Marine Service Association. The SC received statement clarification and guidance from U.S. Coast Guard personnel, LCDR Joshua Rose and LT Josephine A. Long.

Additionally, the SC, to assist with the SC deliberations, received information and guidance on the “National Institute of Standards and Technology (NIST)” Framework, information on NIST Cybersecurity Framework Profile (CFP) by the MITRE Corporation, legislation updates from Bernie, Maynard, and Parsons, an insurers’ perspective on covering cyber-related incidents with John L. Wortham Insurance and a presentation from the Oil and Natural Gas Information and Analysis Sharing (ONG-ISAC) group that provided valuable information on this group’s cybersecurity work.

## Executive Summary

### Phase I

At the first SC meeting, the participants agreed that the eight (8) questions presented in the task would provide some valuable information to the USCG, although they felt that there were many other cybersecurity related



items that were not covered that the industry would want to address before concluding the task. Therefore, it was that the task would be completed in two (2) phases: Phase I would address Questions 1-8 of the task and Phase II will provide a detail list of cybersecurity that should be addressed in Question 9.

In Phase I, the SC identified cyber-dependent systems in the maritime industry. Vulnerability identification processes commonly implemented within the industry were provided. It was noted that the degree of monitoring of cyber risk is company dependent and varies in the industry.

The SC provided a non-exclusive list of the cybersecurity standards and guidelines that are currently used by the oil and gas industry for their cyber risk management programs with the NIST Framework for Improving Critical Infrastructure Cybersecurity heading the list, but also including guidance from the International Organization of Standards (ISO), the International Electro-technical Commission (IEC), the American National Standards Institute (ANSI), the SANS Institute, the North American Electric Reliability Council, as well as IMO and USCG publications and regulations. There are currently no industry specific external certifications available for cybersecurity.

Regarding training programs for MOU and facility personnel that addresses cybersecurity risks and best practices, the SC found these to again be company-dependent. The SC identified that cybersecurity awareness training should target the general users of systems, as well as their supervisors. This training should include third parties/subcontractors that are system users. Corporate office personnel also require cyber awareness training, including senior company management. Remote access training should include: password integrity; knowledge of facility or equipment being remotely accessed; mutual understanding of the changes or upgrades as they are being made; and monitoring of audit logs of session. The SC recommends that product vendors include information on the cyber risks of their technologies in all training provided to their maritime customers.

The SC recommends that all businesses have policies and procedures to ensure the integrity of both their enterprise (business) and operational (process) networks. Contamination vectors that could threaten the networks should be defined and discussed, with mitigation implemented pursuant to the NIST Framework Core Functions (Identify, Protect, Detect, Respond and Recover). The SC recommends a Response and Recovery Plan that is understood by users that will allow them to secure operations, fully assess the type and severity of the incident, and take action in accordance with the Plan, which will allow them to make a decision concerning

system recovery. Knowledge of potential failures, as well as drills, when possible, should be a part of the training once the Response and Recovery Plan is in place.

Regarding Alternate Security Programs (ASP), the participants in this SC were not involved with these programs, but felt that ASPs give groups of similar vessels and/or facilities an alternative way to comply with the MTSA and that model could be utilized by the USCG in the cybersecurity arena.

The SC recommends that companies use a risk based assessment process to determine the threat to their individual business and process control systems that includes: identifying the cyber risks; providing action to mitigate risk; implementing preventive actions; training employees on the process; and ensuring business practices are in place by implementing an audit system. The USCG, in consultation with industry, should clearly define objectives for company cybersecurity/cyber risk programs and the critical systems to be addressed by those programs.

Classification societies have been working on guidance and risk based measures to address cyber threats in the industry, but as of the date of this task response none have been published. Classification societies are currently conducting some marine software certifications. Insurers and protection and indemnity clubs are currently collecting information from clients by questionnaire and are still working to determine cost vs. risk.

For Phase II the subcommittee divided into four (4) focus groups. The deliberation of those groups follows:

- Centralized Information and Data Sharing
- Identify the Steps and Processes required in developing a Cybersecurity/Cyber Risk Program
- Best Practices: Cyber Security Risk and Cyber Risk Management
- Industry Definitions

*Note: In final deliberations, Steps and Processes and Best Practices were combined into one section.*

Below are the recommendation from the focus groups:

- Centralized Information and Data Sharing
  - Recommend voluntary data sharing system
  - Must have mechanism for anonymous reporting
  - Should communicate feedback and trend analysis to the industry

- Recommend modified US-CERT form
- Reporting to be encouraged and publicized by USCG
- Identify the steps and processes required in developing a Cybersecurity / Cyber Risk Program, Benchmarks, and Best Practices
  - A voluntary and risk-based approach to managing cybersecurity
  - The use of NIST Framework
  - All offshore industry companies should have a Cybersecurity / Cyber Risk Management program which is based specifically on their offshore (and other) assets
  - Comprised of a set of elements that cover all five Framework Functions, but are tailored to the specific set of assets and potential threats that a given company faces
  - Key Cybersecurity Aspects and Controls of the Offshore Oil and Natural Gas Industry - Ten key high-level controls or practices for the O&G industry
    - Digital Controls for Critical Systems
    - Assessment of Vulnerability Management in Software Development
    - Patching and Anti-Virus Protection for Process Control Networks (PCN).
    - Segmentation of Process Control Networks
    - Set-up of a Specialized Process Control Network (PCN).
    - Restricted Access to Programmable Logic Controller (PLC).
    - Restrictions and Monitoring for Vendor Access to Original Equipment Manufacturer (OEM) Systems
    - Redundancy of Systems, based on Criticality of Systems and Risk Assessment
    - Periodic onsite cyber related drills
- *Test and Assessments*
  - Test and assess process exists
  - Demonstrate how changes to the controls systems are managed and accessed
  - Demonstrate relevant Cybersecurity training of the personnel involved with critical control systems
  - Conduct test / assessments to identify opportunities for improvement
  - Capture and report internally when test and/or assessment results
- Industry Definitions
  - **Cyber breach of security** – An incident that has not resulted in a transportation security incident, in which security measures have been circumvented, eluded, or violated. *(Source: 33 CFR 101.105)*
  - **Cyber suspicious attack** - An action on or through an information system that has resulted in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. *(Source: Cybersecurity Information Sharing Act of 2016, Pub. L. No. 114-113, Title 1, § 102(5), however, removing the reference to the 1<sup>st</sup> Amendment of the Constitution of the U.S. and substituting the words, “has resulted” in place of the words “may result”).*



- **Vulnerability(ies)** – The probability that threat capability exceeds the ability to resist threat. (Source: *The Open Group Risk Taxonomy*)

## Phase I

The NOSAC SC issues the following responses to the assigned eight (8) questions that would assist USCG in developing policy to help vessel and facility operators identify and address cyber-related vulnerabilities that could contribute to a Transportation Security Incident (TSI). Additionally, the SC has included a response to Task Item 9 regarding related cybersecurity matters as Phase II of the task.

## Responses to Questions 1 - 8

### 1. **What cyber-dependent systems, commonly used in the maritime industry, could lead or contribute to a transport security incident (TSI) if they failed, or were exploited by an adversary?**

The SC recognizes the USCG's partnership with NIST to develop a "NIST Cybersecurity Framework Profile" for the offshore oil and natural gas operating environment. The SC believes that this Profile will provide a baseline for risk and vulnerability assessments within the maritime/oil and gas industry.

In order to answer Question #1 and to provide input to USCG and NIST in developing the Profile for offshore oil and gas, the SC has categorized cyber-dependent systems in the maritime industry as follows (The systems listed herein are not an all-inclusive list, but rather an example of the cyber-dependent systems found in the U.S. OCS. The systems are listed in alphabetical order:

- Marine / Navigation Systems
  - Accommodations
  - Anchor Handling
  - CCTV
  - Communication
  - Cranes
  - Fire and Gas
  - Load and Stability
  - Maintenance Management Systems
  - Power Management (PMS)
  - Station Keeping and Propulsion
  - Vessel Management System (VMS)
- Process Systems
  - Dive Support Systems
  - Drilling Systems
  - Fluid Storage and Transfer Systems
  - Heavy Lift Vessels

- Pipe / Cable Lay, and Construction Vessels
- Production Systems

The SC presents Table 1: Potential Impact Levels from the Federal Information Processing Standards Publication 199 (FIPS 199) as an example of one of the methods to categorize system risk/impact. We recommend that each category be extended to include the effect on the environment and loss of organization reputation, which the SC notes are missing from FIPS 199.

Risk Impact	Definitions
<p style="text-align: center;"><b>Low</b></p>	<p>The potential impact is low if-The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p> <p>A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals</p>
<p style="text-align: center;"><b>Moderate</b></p>	<p>The potential impact is moderate if-The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p> <p>A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.</p>
<p style="text-align: center;"><b>High</b></p>	<p>The potential impact is high if-The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p> <p>A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or</p> <p>(iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.</p>

**Table 1: Potential Impact Levels** (Also, the SC recommends that each category include the effect on the environment and loss of organization reputation, which the SC notes is missing from this chart.)



The potential impact and residual risk of these systems is dependent on individual company, facility, vessel, geographical region, level of automation of vessels and other parameters affecting cybersecurity risk impact evaluation (as shown in Table 2).

Potential Impact to Industry	Systems	Residual Risk of System / Network Design*
<p>* Based on individual company, facility, vessel, geographical region, level of automation of vessels and other parameters affecting cybersecurity risk impact evaluation.</p>	<p><b>Marine / Navigation Systems</b></p>	<p>*Based on individual company, facility or vessel mitigation risk assessment *See note regarding third party equipment</p>
	<ul style="list-style-type: none"> <li>● Accommodations</li> </ul>	
	<ul style="list-style-type: none"> <li>● Anchor Handling Systems</li> </ul>	
	<ul style="list-style-type: none"> <li>● CCTV</li> </ul>	
	<ul style="list-style-type: none"> <li>● Communications</li> </ul>	
	<ul style="list-style-type: none"> <li>● Cranes</li> </ul>	
	<ul style="list-style-type: none"> <li>● Fire and Gas</li> </ul>	
	<ul style="list-style-type: none"> <li>● Load and Stability</li> </ul>	
	<ul style="list-style-type: none"> <li>● Maintenance Management Systems</li> </ul>	
	<ul style="list-style-type: none"> <li>● Power Management (PMS)</li> </ul>	
	<ul style="list-style-type: none"> <li>● Station Keeping and Propulsion</li> </ul>	
	<ul style="list-style-type: none"> <li>● Vessel Management System (VMS)</li> </ul>	
	<p><b>Process Systems</b></p>	
	<ul style="list-style-type: none"> <li>● Dive Support Systems</li> </ul>	
	<ul style="list-style-type: none"> <li>● Drilling Systems</li> </ul>	
	<ul style="list-style-type: none"> <li>● Fluid Storage and Transfer Systems</li> </ul>	
	<ul style="list-style-type: none"> <li>● Heavy Lift Vessels</li> </ul>	
	<ul style="list-style-type: none"> <li>● Pipe / Cable Lay and Construction Vessels</li> </ul>	
<ul style="list-style-type: none"> <li>● Production Systems</li> </ul>		

**Table 2: Potential Impact Levels Vessel Systems** (\*All third party equipment should have strict access, authentication, and authorization controls. Third party gear should mimic or be more stringent than facility owner/operator gear.) Note: The systems listed above are small examples of systems found on vessels and or platforms operating in the U.S. OCS.

**2. What procedure or standards do the MOU and facility operators now employ to identify potential cybersecurity vulnerabilities to their operations?**

Procedures and standards in the U.S. maritime and oil and gas industry are currently company-dependent.

Vulnerability identification processes that have been identified within the industry include:

- **Vulnerability Assessments:** The analysis of system, application and configuration vulnerabilities to compare current versions, patches, hotfixes and configurations against known vulnerabilities on systems within the scope of an assessment.
- **Risk Assessments:** An assessment process to identify risk in policies, procedures, personnel, and systems that calculate and describe the risk based upon identified vulnerabilities and/or threats and a solution to mitigate that risk. Risk assessment processes occur for many maritime/oil and gas industry companies and involve analysis of risks (impact vs. likelihood) and identification of mitigating controls.
- **Network and system monitoring:** Network and system monitoring has the potential of providing identification of anomalous behavior, configuration changes, and connections. This can be managed and monitored through a centralized or decentralized system. This can provide identification of unauthorized connections and configuration changes which could potentially introduce a vulnerability.

Regarding maritime environmental controls, companies operating in the maritime environment have always spent a significant portion of their effort selecting or designing equipment and associated control systems that are reliable, redundant, and safe. Doing anything less would potentially expose inherent risk of inoperable or ill-suited functionality resulting in diminished reliability and increased cost. The advent of automation of control systems has not changed this requirement; it has only added another aspect to the analysis and design processes that have always been used.

Processes for identifying vulnerabilities of system design usually starts during the pre-construction design phase. All aspects of vessels/platforms must work effectively together and allow for the control of processes with automated control systems and with backup/safety systems that handle situations in which the primary system(s) could fail. Part of the design work includes assessment of the risks in each component or sub-system to be integrated into a common Operational Technology (OT) or Information Technology (IT) system. These risks include equipment failures, operator failure, physical attack and cyber-attack. For each identified risk, appropriate mitigating controls must be designed to ensure that the residual risks are at an acceptable level. -



**3. Are there existing cybersecurity assurance programs in use by the industry that the Coast Guard could recognize? If so, to what extent do these programs address MOU or facility systems that could lead to a Transport Security Incident?**

The SC is aware that the industry uses several cybersecurity standards and guidance to assist them in establishing their cybersecurity/cyber risk policies and procedures. Following is a non-exclusive listing of those cybersecurity standards and guidance:

- NIST Framework for Improving Critical Infrastructure Cybersecurity
- NIST 800-53 Rev 4 - Security and Privacy Controls for Federal Information Systems and Organizations
- SANS 20: Critical Security Controls for Effective Cyber Defense
- SANS ICS Cyber Kill Chain
- ISO 28001:2007 - Security management systems for the supply chain; Best practices for implementing supply chain security, assessments and plans - Requirements and guidance.
- ISO/IEC 27001:2013 - Information Technology - Security techniques - Information security management systems – Requirements
- ISO/IEC 27002:2013 - Information Technology - Security techniques - Code of practice for information security controls
- ISO 27032 (Guidelines to Cybersecurity)
- ISA/IEC 62443 (Industrial Automation and Control Systems Security) Standard of Good Practice for Information Security (Published by the Information Security Forum (ISF))
- IEC 62351 (Power systems management and associated information exchange - Data and communications security)
- NERC CIP Standards (North American Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP)) - Targeted at the energy sector
- ANSI/ISA 99 Security for Industrial Automation and Control Systems
- International Ship and Port Facility Security Code (ISPS) framework
- API –STD-780 Security Risk Assessment Methodology
- IMO Publication 39/7 dated 10 July 2014, Ensuring Security in and Facilitating International Trade, Measures Toward Enhancing Maritime Cybersecurity (as submitted by Canada)
- Maritime Cybersecurity Standards, 78883 [2014---30613]
- United States Coast Guard (USCG) and Code of Federal Regulations (CFR) (33---CFR) requirements.

Many maritime-related companies working on the OCS develop their cyber risk programs based on information and guidance found in the above listed cyber standards and guidance. Their program is then self-assessed or self-tested using various audit protocols. There are currently no external certifications for OT Cybersecurity specific to Oil and Gas operations.

The SC is aware that two (2) classification societies have guidance documents in place and provide external audit services for their clients.

**4. To what extent do current security training programs for MOU and facility personnel address cybersecurity risks and best practices?**

The SC found that cybersecurity/cyber risk training is again company-dependent. Many companies provide “broad brush” cybersecurity training such as the handling of phishing emails.

Security awareness training should target all facility personnel. Applicability to personnel on MOUs should be in accordance with Section 5 of IMO Resolution A.1079 (28) which identifies categories of personnel who should receive various levels of training, but could apply to other sectors. Any system users and their supervisors should also be trained to recognize suspicious operations of equipment, as well as to judge suspicious human actions. It was mentioned that a Cyber Behavior Program could be a part of an effective cybersecurity program, where behavior is challenged – making “if you see something, say something” apply to cyber-related operations. System maintenance personnel who identify problems and failures first hand should receive training that requires immediately mitigating/resolving and communicating the findings identified. More in-depth training in cyber awareness is important for senior management. The SC also noted the importance of any subcontractors using company systems should be required to attend a company approved cybersecurity/cyber risk program(s) prior to accessing any company systems.

In addition, both the Coast Guard and companies using cyber-dependent systems in the maritime industry should encourage vendors of these products to include information on the cyber risks of their technologies through training classes they provide on their technologies, and updates to customers as more data is obtained on these systems.

**5. What factors should determine when manual backups or other non-technical approaches are sufficient to address cybersecurity vulnerabilities?**

System redundancy, network architecture, and ability to recover are critical to an adequate risk management program. Businesses must ensure that the boundary of enterprise networks IT and, operational networks OT are clearly defined. Company policies and procedures should be defined for each and ensure integrity within the separate IT and OT systems.

The SC recommends that companies in the maritime/oil and gas industry utilize Response and Recovery Plan(s), understood by all users, that allows for securing operations, fully assessing the type and severity of the incident, take action in accordance with each plan and then make a decision concerning system recovery. Roles, including naming responsible personnel, must be defined.

Once a Response and Recovery Plan is in place, it is essential that drills with various scenarios are implemented. This will increase user understanding and situational awareness of systems and potential problems that can occur within the systems as response and recovery actions are carried out. SC participants stressed that certain failures cannot be replicated in an actual drill and plans must include the proper training to ensure personnel are aware of these possibilities when exact drills are not possible.

The SC also expressed concern regarding the suppliers of systems and ensuring they use proper design standards. (Access limitations to vendor systems provide a barrier when identifying vulnerabilities that can or cannot be mitigated through the use of manual controls).

**6. How can the Coast Guard leverage Alternative Security Programs to MOU and facility operators address cybersecurity risks?**

The membership of the SC are not involved with Alternative Security Programs (ASP), which are usually designed for smaller vessel fleets and do not have a formal comment for this question. However, Alternative Security Programs (ASP) give groups of similar vessels and/or facilities an alternative way to comply with the Maritime Transportation Security Act (MTSA) and that model could be utilized by the Coast Guard broadly in the cybersecurity arena. Groups of vessels or facilities operated in the same way could document their plans and audit themselves against their plans as a group rather than being seen as individual entities.

**7. How can MOU and facility operators reliably demonstrate to the Coast Guard that critical cyber-systems meet appropriate technical or procedural standards?**

The consensus of the SC is that companies should use a risk based management process to determine the threat to their individual companies IT and OT systems. Each company's processes will differ based on the



type and location of the work conducted and systems used. The defined processes demonstrate and document task completion. Some tasks might include:

- Identifying the cyber risk
- Providing action to mitigate the risk
- Implementing preventive actions
- Training of employees
- Ensuring business practices are in place by implementing an audit system.
- Developing a response and recovery plan and periodically testing the plan via drills.

The SC consensus is that we do not wish to see prescriptive new rules and regulations. It was agreed that it would be helpful for the Coast Guard to document what cyber-dependent systems, commonly used in the maritime industry, could lead or contribute to a transport security incident (TSI) if they failed, or were exploited by an adversary with notations on the risks and potential impact levels gathered by the Coast Guard during this partnership effort. This information could be used by companies to inform their cyber risk assessment processes.

Under this question, the SC also identified that OT should be assessed for vulnerabilities. The industry should monitor the potential system threats brought to the public domain, understand patch management of the entire system (including software, drivers, etc.), ensure that these upgrades/patches are properly implemented, and also, include a roll-back plan in case something is wrong with the upgrade and/or patches.

Additionally in the cyber risk assessment, human risk factors must be identified and addressed.

The SC discussed the potential use of a Failure Mode, Effects and Criticality Analysis (FMECA), as a tool (but not mandatory) for analyzing each system function and its impact for a single point failure, but a cyber-attack could constitute a multi-point failure. Companies should consider these failure possibilities when constructing the recovery protocols and provide system users with support to understand how to identify the failure mode.

The SC recommends that USCG, working with industry, clearly define objectives for company cybersecurity/cyber risk programs and critical systems to be addressed in those programs. As stated herein, many companies have internally developed their cybersecurity programs using the NIST framework and ISO 27000 guidelines (or alternatives to these standards) and would refine their programs based on

clear guidance from the USCG. These company-generated programs include an audit system and allow for continuous update and improvement of the program based on assessments, events, and recordable incidents.

The SC discussed the potential of the USCG considering a voluntary Questionnaire based on the NIST framework that would serve as the company's confirmation of a cyber risk based system within their companies. Another topic of discussion was that the USCG may want to consider Bureau of Safety and Environmental Enforcement (BSEE) / Safety and Environmental Management Systems (SEMS) and 33 CFR (MTSA), systems already in place that could be enhanced to cover cybersecurity guidelines.

**8. Do classification societies, protection and indemnity clubs, or insurers recognize cybersecurity best practices that could help the maritime industry and the Coast Guard address cybersecurity risk?**

Classification societies have been working on this and have guidance/measures to address their and their clients' cyber threats. They are advocating a risk based approach as is this SC. They are also conducting some software certifications.

Protection and indemnity clubs (P&I Clubs) and insurers are requesting questionnaires from the clients on their cybersecurity and risk programs. It is the opinion of the SC that these groups are collecting information and are still attempting to figure out how to address and mitigate cybersecurity risk. It is suggested that there is not enough data (actuary information) for these insurers to determine the cost vs. risk in the industry.

## Phase II

**Question 9 - Provide comments on any related cybersecurity issues not addressed in the above questions.**

### Centralized information and data sharing

The SC recommends that the USCG select or designate a method for the USCG to report and share cyber data in order to keep the industry aware and informed of the types of incidents that can happen and allow them to

prepare for similar events/situations in their organizations. The SC is aware of the USCG's recent distribution of Maritime Cyber Bulletins and views them as informative for our specific industry. We are additionally aware of the US-CERT (Department of Homeland Security (DHS) – United States Computer Emergency Readiness Team) daily emails and weekly vulnerability summaries which do provide good information, but are not filtered by industry. Industry use of these available communication avenues should be encouraged.

The consensus of our SC is that the reporting by companies to the USCG should be voluntary, with a mechanism to report anonymously. The method of reporting must be easy for the oil and gas/maritime industry requiring a minimum of additional labor to report. An automated, computerized system is suggested. Web based reporting, free for all to access, is the recommended format to utilize. Voluntary reporting of many kinds of indicators may be helpful, given that knowledge of the lower level threats and the near miss-type of incidents may be just as relevant as the larger breaches and threats. This wealth of knowledge would be very beneficial to the industry by assisting them in continuously improving cybersecurity posture.

A big question heard from the SC participants is “what would happen with the data reported”? While it is expected that a major cyber incident resulting in severe or catastrophic adverse effect on organizational assets, operations or personnel would become public knowledge very quickly, the USCG and industry can benefit from sharing of information about threats below this catastrophic level. For example, cybersecurity risks can often also be physical in nature – occurring by direct contact by personnel with unauthorized access to IT equipment. The communications of these types of cybersecurity risks could benefit the industry the most as cybersecurity programs mature. Also, if cybersecurity reporting would cause hours of follow up labor, (beyond the labor already required in the organization's cybersecurity program), then the chances of sufficient reporting would be slim. Therefore, any reporting system implemented should be clearly communicated to the industry and include how it will be used by USCG/DHS. In addition, it should include a prompt feedback system. Real time automatic distribution of the cybersecurity indicators and risks to all organizations and vessels must be as specific as possible, while maintaining confidentiality. This would alert all concerned and generate an ongoing timeline which could trend possible attacks. The trending could be a dedicated task within DHS or USCG, or it could be done by a voluntary industry group.

The SC looked at two reporting methods currently being utilized by industry: US-CERT and DHS-USCG Form CG-2692.



The SC consensus is that the CG-2692 is less suitable for the reporting and feedback we would like to see occur in the industry. The threshold for reporting is higher which would not allow the lower level cyber risks to be reported. Additionally, there is no feedback mechanism or trend analysis distribution currently built into the USCG use of the form. The SC did discuss the possibility of a check/tick box on the CG-2692 form indicating cyber-related circumstances involved that would link to an additional supplemental cyber report that would move the cyber indicator/threat to the DHS/ National Cybersecurity and Communication Integration Center (NCCIC) system.

The US-CERT form is part of the US-CERT Incident Reporting System and is more compatible with what the industry would like to see in place for cyber reporting and data sharing. This form allows for reporting of all cyber indicators, and if kept confidential, would encourage reporting of indicators classified as lower level. It is the SC's understanding that the US-CERT form goes to the NCCIC data base, where it is given a tracking/receipt number, in order to track the number of reports and provide historical reference. It is then used for trend analysis, which can be accessed by all industries. We additionally understand that NCCIC prioritizes confidentiality with regard to distribution of the trend analysis, labeling it as Protected Critical Infrastructure Information (PCI) and in many cases working with the submitter prior to sending out feedback and analysis.

For this reporting and information sharing program to be successful, a firm agreement between industry and DHS-USCG must be reached to guarantee anonymous reporting and feedback distribution. The SC has been advised that the current method for anonymous reporting to US-CERT is by a telephone call if there are sensitivities to using the form. This anonymous reporting would be acceptable to the SC, but we believe that alternate avenues of anonymization or pseudonymization, appropriate to privacy standards applicable to U.S. law should be explored by the DHS/USCG *(The SC noted the importance in anonymization is that the personal identifiable data is completely removed from the reported data and then deleted. The deletion should be formally verified using an electronic procedure. Furthermore, -it should not be possible to regenerate the coupling between the reported data and the personal identifiable data. The SC recognizes that this means that it might not be possible for the entity receiving the reported data to contact the entity reporting the data. The SC noted that the importance in pseudonymization is to decouple the personal identifiable information from the reported data (information reported). This can, for example be done by storing the personal identifiable data in a non-linkable format and completely separate from the reported data, such as with the use two separate databases. In this case, the identifiable personal information is first linked to a non-identifiable representation such as a number and stored in a dedicated database. Then the non-identifiable representation is stored in another dedicated database, together with the reported data. In addition, the original data, including the web-form and the IP-address would need to be deleted. This*

process should preferably be electronic, with a formal verification of the deletion of the original data and any personal identifiable data linked to the original data. The SC noted encryption of the reported data is a separate matter, not directly linked to anonymization or pseudonymization).

During one of our Phase II SC meetings, the ONG-ISAC provided some information on their organization. We learned that the finance industry has made tremendous progress with their cybersecurity risk assessment systems and does a very good job with communicating indicator feedback through the Financial Sector- ISAC (FS-ISAC). The ONG-ISAC maintains an interface with the FS-ISAC and is shaping their organization on the FS-ISAC's information gathering and sharing systems. The FS-ISAC has a representative working with NCCIC that additionally assures feedback. While many operator and large vessel owner organizations participate in the ONG-ISAC, many smaller industry companies do not and many were unaware of its existence. Also some, but not all, oil and gas/maritime industry associations, participate in the ONG-ISAC and do make some cyber indicator feedback available to their members. While the SC is not recommending the ONG-ISAC, we do believe it is an avenue that industry should be aware of for obtaining information on cybersecurity and cyber risk. The industry should maintain awareness as similar avenues of communication of cyber threats may be available or may become available in the future.

To facilitate the SC's recommendation on Centralized Information and Data Sharing, we have put together a form with the fields that we recommend for oil and gas/maritime industry reporting of cyber indicators (See Exhibit B).

Many of the fields are already on the US-CERT form. In view of this, we recommend that the US-CERT system be utilized for reporting and dissemination of feedback for the industry.

In our recommended form, you will note that we added a field for indicating the type of industry the reporting organization is involved. We suggest that the best feedback would be our own industry feedback and not the unfiltered information that is now produced by US-CERT. We also recommend some additional drop down boxes to make categorizing easier and strengthen consistency. Enough drop-down boxes, with enough actual usable information, so a person inputting incident data would not have to choose a "close enough" option, and the incident would go without the proper information and the cause would elude the database reviewer. The information gathered will provide our industry organizations with sufficient information that vessels, dock



facilities and corporate facilities, main and remote, face cybersecurity risks and that their own systems should be evaluated for vulnerabilities and training of personnel.

In summary, a cyber event can have both positive and negative impacts. All companies do have vulnerabilities and are susceptible to cyber threats. This is why such things as fire-walls, secure switches, air-gaps, secure web browsers, anti-virus and anti-malware software are utilized. On the positive side, more information about cybersecurity threats can improve a cyber system and shared information on indicators can help the industry improve from the awareness of the event. However, companies fear that industry and media knowledge of a cyber event/incident could impact their reputation. Therefore, we stress that information sharing must be carefully orchestrated between government and industry as releasing information which has (or potentially could) harm operations, poses a significant impact on a company, should the media gain access. The element of anonymity is essential. The reporting system will be successful if the implementation is fully publicized, allows anonymity, and contains a feedback loop distributing information to the end users capturing industry sectors and exposing types of threats and vulnerabilities. If DHS / USCG further improves reporting and information sharing as suggested herein, both the reporters of the indicator and the end users receiving the feedback can continue to improve their systems, assisting them in remaining productive and safe.

Identify the steps and processes required in developing a Cybersecurity / Cyber Risk Program, Benchmarks, and Best Practices.

*NIST Cybersecurity Framework in Context of Offshore Oil and Natural Gas (ONG) Industry*

The NIST *Framework for Improving Critical Infrastructure Cybersecurity* (hereafter "Framework") is the single-best comprehensive reference for the US Coast Guard as it seeks to encourage cybersecurity in the offshore maritime environment. The Framework, "a voluntary and risk-based set of industry standards and best practices to help organizations manage cybersecurity risks,"<sup>1</sup> accords with a systems-oriented and risk-based approach that has been proven as the most effective way for companies to manage significant risks, which include cybersecurity. The Framework embodies a management systems approach, prompts companies to tailor a cybersecurity program to each individual company's assets and potential threats and calls for companies to calibrate cybersecurity programs through risk assessment. This NOSAC SC endorses the Coast Guard's referencing of the Framework. This NOSAC SC also continues to recommend to the Coast Guard a voluntary and risk-based approach to managing cybersecurity.

---

<sup>1</sup> NIST, "Framework for Improving Critical Infrastructure Cybersecurity," 12 February 2014, p. 1.

An oil and gas industry recent survey conducted by API and other oil and natural gas industry trade associations, covering all aspects of the industry (including, but not just, offshore) that was fielded in the third quarter of 2015 found that about two-thirds of the 53 oil and natural gas companies surveyed are using the Framework in some manner. The survey found that half of those using the Framework have integrated it into their corporate cybersecurity program while the other half uses the Framework for specific purposes. Other uses of the Framework included:

- 77% of respondents use the Framework to evaluate cybersecurity capabilities and programs.
- 69% use the Framework to prioritize cybersecurity programs.
- 48% use the Framework to facilitate cybersecurity communications (via common language/taxonomy).
- 32% use the Framework to benchmark cybersecurity performance versus external peers.
- 25% use the Framework to evaluate external suppliers / contractors.

#### *Recommendations:*

This NOSAC SC recommends that all offshore industry companies have a Cybersecurity / Cyber Risk Management program which is based specifically on their offshore (and other) assets. This program should include all cyber capable assets (Marine / Navigation Systems – Accommodations, Anchor Handling, CCTV, Communication, Cranes, Fire and Gas, Load and Stability, Maintenance Management System, Power Management System, Station Keeping and Propulsion, Vessel Management Systems (VMS), Process Systems – Dive Support System, Drilling System, Fluid Storage and Transfer Systems, Heavy Lift Vessels, Pipe / Cable Lay, Construction Vessels, Production System, and Process Control Network, and the IT Business).

#### *Steps for Developing a Cybersecurity Program Consistent with the NIST Cybersecurity Framework*

The critical step for developing an effective cybersecurity program for offshore oil and gas operations is to implement a systems approach to cybersecurity, i.e., not a static program or a simply a defined set of practices, but rather a dynamic, holistic and continuously improving program. The five Functions of the Framework (Identify, Protect, Detect, Respond, and Recover) represent the key components to a systems approach. Companies that manage cybersecurity effectively in any industry sector or any segment of the oil and natural gas industry, including offshore, take this approach.

##### a. Key Cybersecurity Aspects of the Offshore Oil and Natural Gas Industry

A Framework-conforming cybersecurity program for a company in the oil and gas industry should be comprised of a set of elements that cover all five Framework Functions, but are tailored to the specific set



of assets and potential threats that a given company faces. In addition, many of these elements are the same for any company, including those operating in the offshore oil and natural gas industry. Common cybersecurity controls for any company, including those operating in the offshore oil and natural gas industry include such illustrative measures as taking inventory of all assets through a cybersecurity lens, conducting patching and anti-virus protection for software, deploying a cybersecurity response plan and numerous others. Here we do not identify or highlight any of these general elements or controls, since they apply to any industry sector and company and because they are numerous.

We identify ten key high-level controls or practices that are more unique to the offshore oil and natural gas industry and that address the key and more unique aspects for cybersecurity of the offshore oil and natural gas industry from the section above.

The following key high-level cybersecurity controls are typical ones that, if they apply to that company's assets and potential threats, are common to effective cybersecurity programs for offshore oil and natural gas industry companies:

- 1. Digital Controls for Critical Systems.** In order to assess the potential vulnerabilities or and threats to digital controls of critical systems reference in Table 3.
- 2. Assessment of Vulnerability Management in Software Development.** In order to take confidence in software security and reliability "off the shelf," companies assess software developers' management of potential vulnerabilities in the software development lifecycle, either seeking that developers achieve certification or conducting other means of due diligence.
- 3. Patching and Anti-Virus Protection for Process Control Networks (PCN).** Because of the prevalence of digital controls for critical systems, companies conduct patching and anti-virus protection of these digital controls with restrictions in access to these process control environments, such as requiring that vendors conducting patching and anti-virus installation/updates validate patches prior to installation in order to ensure continuity of operations for achieve business resiliency and safe operations. Automated, real-time anti-virus scanning is generally not done for such systems in order to avoid disrupting real time operations.

4. **Segmentation of Process Control Networks.** In order to protect a PCN, companies segregate them from the business IT network, and by extension, the Internet. Typically, an extranet (DMZ) architecture is put into place between the process control and business network to filter communications so they only flow only out of the process control network to the business network.
5. **Set-up of a Specialized Process Control Network (PCN).** As additional protection for a PCN, companies set-up the PCN as a specialized network, allowing for controls to eliminate unneeded protocols (like SMTP Email) and to allow for white-listing to preclude unwanted code from running on the PCN.
6. **Restricted Access to Programmable Logic Controller (PLC).** In order to safeguard physical and digital access to digital controls of critical systems – often a PLC – companies restrict access to personnel, such as by making the PLC certain authorized personnel or vendors. Examples of restricted access include making the PLC accessible only in a rack available to authorized personnel, implementing single point of authority on vessel controls access, securing entire rooms with limited access, such as control rooms or power equipment.
7. **Restrictions and Monitoring for Vendor Access to Original Equipment Manufacturer (OEM) Systems.** Because OEMs require access by third party vendors, companies maintain restrictions and monitoring for access by these vendors. Examples of such restrictions and monitoring include:
  - a. Control by single point of accountability in company personnel;
  - b. Proper change management and permit to work required for vendors to begin work;
  - c. Restricted access to port that is made available only to that vendor when access is needed;
  - d. Scanning of USB devices off network prior to installing them within the process control network (PCN) by a vendor;
  - e. Monitoring of network traffic once a connection is established by a vendor for authorized work.
8. **Redundancy of Systems, based on Criticality of Systems and Risk Assessment.** As another safeguard against the potential compromise of the functioning of digital controls for critical systems, companies put into place redundancy of systems for the most critical and potentially at-risk systems, factoring in the implementation of controls to mitigate risks. There is a not necessarily a standard definition neither of the most critical systems across companies nor of the most residually at-risk systems across

companies. There also is not necessarily a standard type of appropriate systems redundancy to implement, including whether such a redundant system be manual control instead of digital control. The critical control is for companies to implement an appropriate and reliable redundancy of systems for its most critical and residually-at risk systems that are controlled digitally.

9. **Intrusion Detection on Process Control Network (PCN).** In order to prevent and respond to potential PCN intrusions, companies implement capabilities to monitor and detect intrusions to the PCN, given its criticality as the control for critical systems in offshore oil and natural gas. Often such capabilities are pre-installed in the PCN. Intrusion detection can take different forms, but the key control is to have an appropriate mechanism in place to detect potential intrusions to the PCN.
10. **Periodic Onsite Cybersecurity-related Drills.** As in responding to other risks, drills improve companies' abilities to respond and recover from cybersecurity incidents, especially for collaborating with other companies and the government given the physical isolation of maritime operations.

Typically, companies map specific controls or practices that they put into place against the Framework, in order to show where within the systems-approach for managing cybersecurity the controls fit. Table 5 maps the key cybersecurity controls described above to the corresponding Framework Functions.

#### b. Key Cybersecurity Controls for the Offshore Oil and Natural Gas Industry

A Framework-conforming cybersecurity program for a company in the offshore oil and natural gas industry will be comprised of a set of elements that cover all five Framework Functions, but tailored to the specific set of assets and potential threats that a given company faces. In addition, many of these elements are the same for companies in any industry sector or any segment of the oil and natural gas industry. Common cybersecurity controls for any company, including those operating in the offshore oil and natural gas industry include such illustrative measures as taking inventory of all assets through a cybersecurity lens, conducting patching and anti-virus protection for software, deploying a cybersecurity response plan and numerous others. We do not identify or highlight any of these general elements or controls, since they apply to any industry sector and company and because they are numerous.



Instead, we identify ten key high-level controls or practices that are more unique to the offshore oil and natural gas industry and that address the key and more unique aspects for cybersecurity of the offshore oil and natural gas industry from the section above.

The following key high-level cybersecurity controls are typical ones that, if they apply to that company’s assets and potential threats, are common to effective cybersecurity programs for offshore oil and natural gas industry companies:

- i. **Inventory of Digital Controls of Critical Systems.** In order to assess the potential vulnerabilities or and threats to digital controls of critical systems, companies start by inventorying such systems and controls such as those for vessels depicted as a reference in Figure 1 and Table 3. Another approach to inventory controls is by cybersecurity processes, as depicted in Figure 2 and Table 4.

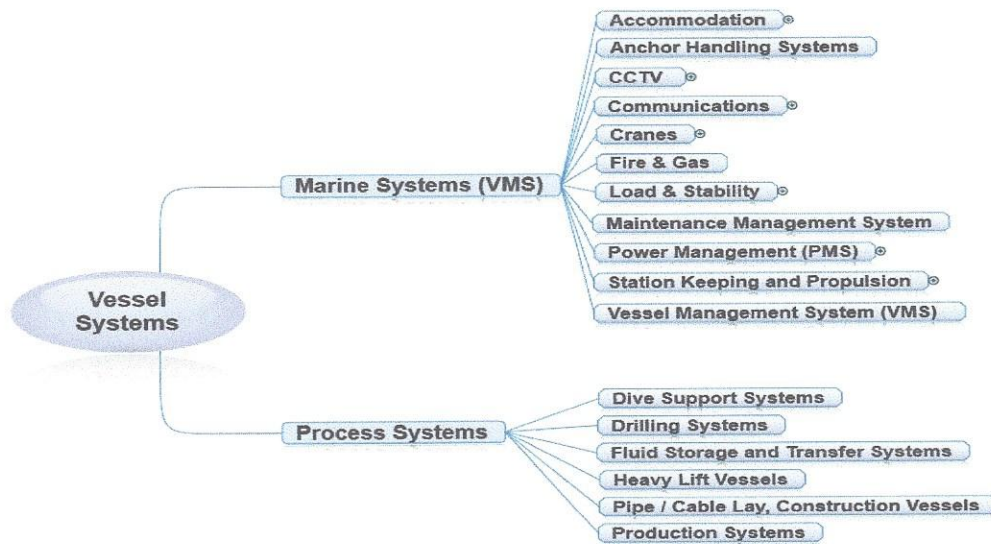


Fig 1: Vessel System

Systems	Documented Controls in Place (Yes, No, NA)	Date of Latest Revision (dd/mmm/yyyy)	Comment
<b>Marine Systems (VMS)</b>			
Accommodations			
Anchor Handling System			
CCTV			
Communications			
Cranes			

Systems	Documented Controls in Place (Yes, No, NA)	Date of Latest Revision (dd/mmm/yyyy)	Comment
Fire & Gas			
Load and Stability			
Maintenance Management System			
Power Management Systems (PMS)			
Station Keeping and Propulsion			
Vessel Management System (VMS)			
<b>Process Systems</b>			
Anchor Handling Systems			
Dive Support Systems			
Drilling Systems			
Fluid Storage and Transfer Systems			
Heavy Lift Vessels			
Pipe / Cable Lay and Construction Vessels			
Production Systems			

Table 3: Example of Vessel Systems Controls Checklist



Fig 2: NIST Cybersecurity Framework Mapping of Key Cybersecurity Controls for Offshore Oil & Natural Gas

Sections	Documented Controls in Place (Yes, No, NA)	Date of Latest Revision (dd/mmm/yyyy)	Comments
Configurations			
Controls / Monitoring			
Cyber Hygiene			
Incident Response and			

Sections	Documented Controls in Place <small>(Yes, No, NA)</small>	Date of Latest Revision <small>(dd/mm/yyyy)</small>	Comments
Management			
Inventories			
Security Testing			
Vulnerabilities			

Table 4: Example of Critical Security Checklist

- ii. **Assessment of Vulnerability Management in Software Development.** In order to take confidence in software security and reliability “off the shelf,” companies should assess software developers’ management of potential vulnerabilities in the software development lifecycle, either seeking that developers achieve certification or conducting other means of due diligence.
- iii. **Patching and Anti-Virus Protection for Process Control Networks (PCN).** Because of the prevalence of digital controls for critical systems, some companies conduct patching and anti-virus protection of these digital controls with restrictions in access to these process control environments, such as requiring that vendors conducting patching and anti-virus installation/updates validate patches prior to installation in order to ensure continuity of operations for achieve business resiliency and safe operations. Automated, real-time anti-virus scanning is generally not done for such systems in order to avoid disrupting real time operations.
- iv. **Segmentation of Process Control Networks.** In order to protect a PCN, companies segregate them from the business IT network, and by extension, the Internet. Typically, an extranet (DMZ) architecture is put into place between the process control and business network to filter communications so they only flow out of the process control network to the business network.
- v. **Set-up of a Specialized Process Control Network (PCN).** As additional protection for a PCN, companies set-up the PCN as a specialized network, allowing for controls to eliminate unneeded protocols (like SMTP Email) and to allow for white-listing to preclude unwanted code from running on the PCN.
- vi. **Restricted Access to Programmable Logic Controller (PLC).** In order to safeguard physical and digital access to digital controls of critical systems – often a PLC – companies restrict access to



personnel, such as by making the PLC only accessible to authorized personnel or vendors. Examples of restricted access include making the PLC accessible only in a rack available to authorized personnel, implementing single point of authority on vessel controls access, securing entire rooms with limited access, such as control rooms or power equipment.

- vii. **Restrictions and Monitoring for Vendor Access to Original Equipment Manufacturer (OEM) Systems.** Because OEMs require access by third party vendors, companies maintain restrictions and monitoring for access by these vendors. Examples of such restrictions and monitoring include:
- a. Control by single point of accountability in company personnel;
  - b. Proper change management and permit to work required for vendors to begin work;
  - c. Restricted access to required ports/access for the work that is made available only to that vendor when access is needed;
  - d. Scanning of USB devices off network prior to installing them within the process control network (PCN) by a vendor;
  - e. Monitoring of network traffic once a connection is established by a vendor for authorized work.
- viii. **Redundancy of Systems, based on Criticality of Systems and Risk Assessment.** As another safeguard against the potential compromise of the functioning of digital controls for critical systems, companies put into place redundancy of systems for the most critical and potentially at-risk systems, factoring in the implementation of controls to mitigate risks. There is a not necessarily a standard definition neither of the most critical systems across companies nor of the most residually at-risk systems across companies. There also is not standard threshold of appropriate systems redundancy to implement, including whether such a redundant system be manual control instead of digital control. The critical control is for companies to implement appropriate and reliable redundancy of systems for its most critical and residually-at risk systems that are controlled digitally.
- ix. **Intrusion Detection on Process Control Network (PCN).** In order to prevent and respond to potential PCN intrusions, companies implement capabilities to monitor and detect intrusions to the PCN, given its criticality as the control for critical systems in offshore oil and natural gas. Often such

capabilities are pre-installed in the PCN. Intrusion detection can take different forms, but the key control is to have an appropriate mechanism in place to detect potential intrusions to the PCN.

- x. **Periodic, Onsite, Cybersecurity-related Drills.** The offshore industry is familiar with mandatory and regular drills. For operations where safety is a major issue, Fire & Boat drills, Process Operations Kick & Pit drills are usually fitted into the work program where suitable. Cybersecurity and Cyber Risk Management similarly can be included with the company regularly scheduled drills as define in the organization policies and procedures. Likewise, desktop and on-site drills are an integral component of any Cyber Risk Management program, to make all key personnel more aware and prepared for any potential attack, which could target either or both, the offshore or onshore assets. Logging the results and lessons of drills help companies to strengthen response.

Typically, companies map specific controls or practices that they put into place against the Framework, in order to show where within the systems-approach for managing cybersecurity the controls fit. Table 5 maps the key cybersecurity controls described above to the corresponding Framework Functions.

Functions	Key Controls
IDENTIFY	<ol style="list-style-type: none"> <li>1. Assessment of Vulnerability Management in Software Development</li> <li>2. Inventory of Digital Controls of Critical Systems</li> </ol>
PROTECT	<ol style="list-style-type: none"> <li>3. Patching and Anti-Virus Protection for Process Control Networks (PCN)</li> <li>4. Restricted Access to Programmable Logic Controller (PLC)</li> <li>5. Redundancy of Systems, based on Criticality of Systems and Risk Assessment</li> <li>6. Restrictions and Monitoring for Vendor Access to Original Equipment Manufacturer (OEM) Systems</li> <li>7. Segmentation of Process Control Networks</li> <li>8. Set-up of a Specialized Process Control Network (PCN)</li> </ol>
DETECT	<ol style="list-style-type: none"> <li>9. Intrusion Detection on Process Control Network (PCN)</li> </ol>
RESPOND	<ol style="list-style-type: none"> <li>10. Periodic, Onsite, Cybersecurity-related Drills.</li> </ol>
RECOVER	<i>[No unique controls for offshore oil and natural gas that are different from other industry or oil and natural gas industry]</i>

Table 5: NIST Cybersecurity Framework Mapping of Key Cybersecurity Controls for Offshore Oil & Natural Gas

*Best Practices: Cybersecurity and Cyber Risk Management.*

The offshore oil and natural gas industry has implemented several more specific best practices related to the key Cybersecurity controls listed in the section above. While there is no one-size-fits-all set of best practices,

the following is a list of illustrative examples of industry practices as they correspond to the NIST Cybersecurity Framework Categories:

a. Identification

- i. A company should have established Roles and Responsibilities in place to identify steps required in case of a Cybersecurity event.
- ii. Develop an inventory of all onboard industrial control systems. Then identify their direct communication link capabilities (normally used for remote support) and have an understanding on the consequences of a cybersecurity threat on those systems.
- iii. Identify each Industrial Control Network and identify if there is interlink between them.
- iv. Provide all personnel with bulletins, advisories, and/or alerts on the latest Cybersecurity threats and emerging equipment vulnerabilities.
- v. Identify system interface points whereby loss of a system or subsystem directly compromise operation and functionality of a critical system (i.e. GPS coordinates).
- vi. Create a detailed software register identifying the software and version which supports each of the critical system.
- vii. Perform any update, change, maintenance, data transfer (including extracting data) or similar for each individual system using a controlled and approved procedure that are traceable back to the company performing the activity.

b. Protection (*the following process solutions and measures should be in place in order to protect the process controls / vessels systems*)

- i. Implement a Management of Change process on all systems, to include software and configuration changes.
- ii. Institute an access control policy for the relevant control systems on board a vessel.
- iii. Conduct any data transfer to and from a control system using a secure method and in accordance with an authorization process.
- iv. Implement Network Segmentation - Critical control systems should be segmented from business IT systems and all other control systems.
- v. Implement End Point Protection where applicable.
- vi. Install a Perimeter Demarcation Control System.



c. Detection

- i. Establish a means to detect. In the area of industrial control systems there are various means of detecting a cyber threat or vulnerability. These may be hardware, software or processes and can be either proactive or reactive. This can include having regularly updated security solutions in place.
- ii. Communicate event detection information to all relevant and appropriate parties.
- iii. Conduct cybersecurity training for personnel responsible for the industrial control systems, especially training focused on Industrial Control Systems, and incident response training.

d. Response

- i. Develop, implement and test a response plan for all cyber systems.
- ii. Upon detection of Cybersecurity event:
  - a. Follow the company's policy.
  - b. Assesses the risk and notified the appropriate party(ies).
  - c. Evaluate the severity of the event and determine the appropriate response action.
  - d. Execute the agreed upon response action.
  - e. Validate executed action(s).
  - f. Document.
  - g. Review actions and outcomes for possible changes to response plans.

e. Recovery

- i. Implement a configuration management system for all programmable systems; whereby the personnel can restore the configuration to a known good state.
- ii. Implement a software backup method that ensures backups are tested, verified and stored in a manner that they are accessible.
- iii. In full system restoration from a backup image, include scanning of the image and system that indicates image is free from compromise before placing the system back in operations.
- iv. Share Lessons Learned.

*Test and Assessments*

- i. Test and assessment processes exists
  - Demonstrate how changes to the control system are managed and access is controlled.
  - Demonstrate relevant Cybersecurity training of the personnel involved with critical control systems.
- ii. Conduct tests and/or assessments to identify opportunities for improvement

- iii. Capture and report internally test and/or assessments results.

## Industry Definition

The SC was asked to deliberate on three specific definitions for Phase II of this task – **cyber breach of security, cyber suspicious attack and vulnerability(ies)**. The SC noted during deliberations that different government agencies have different cyber-related definitions. Rather than producing an additional set of definitions, we have provided the most acceptable definitions already in use and quoted the source of the definition. In some instances, we explain our choice of definitions and define other terms inside our chosen definition. These definitions, endorsed by the SC, are not intended to set a precedent for policy making, nor are they intended to trigger any reporting to the U.S. Coast Guard unless already defined by statute or regulation. Unless otherwise stated, the definitions offered below come from either existing federal statutes or regulations, with source cited.

For the definition of cyber breach of security, the SC has chosen to use the definition of breach of security:

- *Breach of security* — “An incident that has **not** resulted in a transportation security incident, in which security measures have been circumvented, eluded, or violated.” *Source*: 33 C.F.R. 101.105 (part of existing Coast Guard regulations).
- *Comment from the SC*: Section 101.105’s definition of “breach of security” is modified by the term “transportation security incident.” A “transportation security incident” is defined by regulations to mean a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.” The use of the term “breach of security” as proposed, would thus mean incidents where security measures have been circumvented, eluded, or violated, but have not resulted in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.
  - Additional definitions to assist understanding:
    - To define incident, the SC prefers to use the following definition and notes from (*Source*) The Open Group Risk Taxonomy:  
**definition of event**: Occurrence or change of a particular set of circumstances.
      - Note 1: An event can be one or more occurrences, and can have several causes;


- Note 2: An event can consist of something not happening;
  - Note 3: An event can sometimes be referred to as an “incident” or “accident.”
  
- **definition of security:** A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise’s risk management approach. *Source:* Committee on National Security Systems Instruction (CNSSI) 4009.
  
- For the definition of *cyber suspicious attack*, the SC has chosen the definition of “cybersecurity threat” from the Cybersecurity Information Sharing Act of 2016, Pub. L. No. 114-113, Title I, § 102(5) (We have removed the reference to the 1<sup>st</sup> Amendment to the Constitution of the United States and substituted the words, “has resulted” in place of the words “may result”):
  - *Cyber suspicious attack* – an action on or through an information system that has resulted in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.
  
  - *Additional definitions to assist understanding:*
    - **definition of threat** - Anything that is capable of acting in a manner resulting in harm to an asset and/or organization; for example, acts of God (weather, geological events, etc.), malicious actors, errors, failures. *Source:* *The Open Group Risk Taxonomy*.
  
    - **definition of information system** – “a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems include industrial control systems, such as supervisory control and data acquisition (SCADA), distributed control systems (DCS) and programmable logic controllers.” *Source:* Cybersecurity Information Sharing Act of 2016, Pub. L. No. 114-113, Title I, § 102 (9).
  
- *Vulnerability* – The probability that threat capability exceeds the ability to resist the threat. *Source:* *The Open Group Risk Taxonomy*.



- *Cyber Hygiene* – processes, procedures, and mechanisms that help protect information systems or devices against cyber security threats, including: (1) unauthorized access; (2) alteration of information or code running or intended to be running on such systems or devices; and (3) unauthorized denials of service to authorized users of these systems or devices. *Source: 114th CONGRESS 1st Session H. R. 3664.*

The SC has received excellent guidance from the U.S. Coast Guard while working through the task statement and we are honored and pleased to present this task response. In closing, the SC acknowledges that cybersecurity and cyber risk assessment are continually evolving in the maritime industry. At this time, we respectfully request that NOSAC be kept updated on the status of the upcoming NVIC regarding cybersecurity and any other cybersecurity guidance issued, such as a Cybersecurity Framework Profile for Offshore Vessels that may be collaborated between NIST and USCG. We ask for the opportunity to reconvene the SC once the drafts of the NVIC, or other guidance, are published in order for this diverse team of subject experts on cybersecurity pulled together for this NOSAC SC task to again provide comment to the USCG before final implementation.

  
Kelly McClelland  
Co-Chair

  
Patrice Delatte  
Co-Chair

## Exhibit A - Acronyms

### Glossary of Acronyms

<b>ANSI</b>	American National Standards Institute
<b>API</b>	American Petroleum Institute
<b>ASP</b>	Alternative Security Program
<b>BSEE SEMS</b>	Bureau of Safety and Environmental Enforcement / Safety and Environmental Management System
<b>CFR</b>	Code of Federal Regulations
<b>CIP</b>	Critical Infrastructure Protection
<b>DCS</b>	Distributed Control System
<b>DHS</b>	Department of Homeland Security
<b>DMZ</b>	Demilitarized Zone
<b>FIPS 199</b>	Federal Information Processing Standards Publication 199
<b>FMECA</b>	Failure Mode, Effects and Criticality Analysis
<b>ICS</b>	Industrial Control Systems
<b>IEC</b>	International Electrotechnical Commission
<b>IMO</b>	International Maritime Organization
<b>ISA</b>	International Society of Automation
<b>ISPS</b>	International Ship and Port Facility Security
<b>ISO</b>	International Organization for Standardization
<b>IT</b>	Information Technology
<b>MOU</b>	Mobile Offshore Unit
<b>MTSA</b>	Maritime Transportation Security Act (U.S.)
<b>NCCIC</b>	National Cybersecurity and Communication Integration Center
<b>NERC</b>	National American Electric Reliability Council
<b>NIST</b>	National Institute of Standards and Technology
<b>NOSAC</b>	National Offshore Safety Advisory Committee
<b>OEM</b>	Original Equipment Manufacturer
<b>OCS</b>	U.S. Outer Continental Shelf
<b>OT</b>	Operational Technology
<b>P &amp; I Clubs</b>	Protection and Indemnity Clubs (Insurance)
<b>PCII</b>	Protected Critical Infrastructure Information
<b>PCS</b>	Process Control System
<b>PLC</b>	Programmable Logic Controllers
<b>SANS</b>	SysAdmin, Audit, Networking and Security (Institute)
<b>SC</b>	Subcommittee
<b>SCADA</b>	Supervisory Control and Data Acquisition
<b>TSI</b>	Transportation Security Incident
<b>USB</b>	Universal Serial Bus
<b>US-CERT</b>	United States Computer Emergency Readiness Team
<b>USCG</b>	United States Coast Guard

# Exhibit B – NOSAC CyberSecurity Risk Sub-Committee Recommended Reporting Format

## NOSAC CYBERSECURITY/CYBER RISK SUBCOMMITTEE RECOMMENDED FORMAT (MODIFIED FROM THE US-CERT REPORTING FORM) (Highlighted fields are in addition to those found on the US-Cert Reporting Form)

### Reporter's Contact Information

Please provide your contact information so that we are able to contact you should we need to follow-up. Your contact information is not required to submit a report.

First Name	M.I.	Last Name
Telephone	Email Address	

I would like to report the impacted user's contact information and have the individual's consent to do so:  Yes  No

### Impacted User's Contact Information:

Please provide the impacted user's contact information in the fields below:

Impacted user's contact information is the same as reporter's contact information above.  Yes  No

Impacted User's Name

First Name	M.I.	Last Name
Telephone	Email Address	
Organization Type	Organization Size	

To what industry is your organization associated?

Are you a critical infrastructure\* owner or operator?  Yes  No

\*Critical Infrastructure Definition: Those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (From Executive Order 13636, Improving Critical Infrastructure.

Are your organization's critical operations affected?  Yes  No

Please enter your organization's internal tracking number (if applicable):

Was the incident triggered locally or remotely?

When, approximately, did the incident start?

<small>Date (DD-MM-YYYY)</small>	<small>Time (hh:mm AM/PM)</small>	<small>Time Zone</small>
--------------------------------------	---------------------------------------	--------------------------

When was the incident detected?

<small>Date (DD-MM-YYYY)</small>	<small>Time (hh:mm AM/PM)</small>	<small>Time Zone</small>
--------------------------------------	---------------------------------------	--------------------------

Was the incident/threat malicious or unintentional?

How was the incident initiated?

Where, specifically, did the incident occur?

### Impact Details

Please provide as much information as you can to answer the following questions to allow understanding of the incident

Did the threat disrupt operations?  Yes  No

Which operations/control systems were disrupted?

Has number of physical, actual possibilities may have occurred, e.g.:  Yes  No

Is the confidentiality, integrity, and/or availability of the organization's information systems affected?  Yes  No

### Threat Vectors

- |                                    |                                |   |   |                                    |
|------------------------------------|--------------------------------|---|---|------------------------------------|
| <input type="checkbox"/> Unknown   | <input type="checkbox"/> Web   | <input type="checkbox"/> External / Removable Media | <input type="checkbox"/> Improper Usage             | <input type="checkbox"/> Other     |
| <input type="checkbox"/> Attrition | <input type="checkbox"/> Email | <input type="checkbox"/> Impersonation / Spoofing   | <input type="checkbox"/> Loss or Theft of Equipment | <input type="checkbox"/> Attrition |

Privacy Act Statement . . .