energy API
AMERICAN PETROLEUM INSTITUTE

Aaron P. Padilla
Senior Advisor, International Policy

1220 L Street, NW
Washington, DC 20005-4070
Telephone (202) 682-8468
Fax (202) 682-8408
Email padillaa@api.org
www.api.org

Submitted via http://www.regulations.gov,
Docket No. USCG–2016–1084

25 September 2017

Captain R.D. Manning
Chief, Office of Port and Facility Compliance
U.S. Coast Guard

Subject: **API Response to Navigation and Vessel Inspection Circular (NVIC) 05–17; Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities**

Dear Captain Manning:

The American Petroleum Institute (API) welcomes the opportunity to comment upon the Navigation and Vessel Inspection Circular (NVIC) 05–17; Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities (hereafter referred to as the "Cyber Risks NVIC" or "NVIC"). API is the only national trade association that represents all aspects of America's oil and natural gas industry. Our more than 625 corporate members, from the largest major oil company to the smallest of independents, come from all segments of the industry. They are producers, refiners, suppliers, marketers, pipeline operators and marine transporters, as well as service and supply companies that support all segments of the industry.

Cybersecurity is a priority for the oil and natural gas industry. Most, if not all of the largest API member companies manage cybersecurity as an enterprise risk with oversight from Boards of Directors and Senior Executives. As operators of and service providers to energy critical infrastructure in the United States and globally, protecting networks from cyber-attacks is a priority of API's members.

Please see below for overarching comments followed by an attached detailed response.

- **API member companies believe that "Enclosure (2) 05-17" contains too much prescriptive detail, which would inhibit adaptability and innovation to address cyber risks. API believes this NVIC should be significantly streamlined.** ***API recommends that the NVIC reference the NIST Cybersecurity Framework (CSF) Profiles being developed for the Coast Guard by NCCOE/MITRE with industry input.*** Cyberspace threats are constantly changing and require adaptive and innovative cybersecurity operations. Prescriptive regimes force a particular course of action (to meet regulatory responsibilities) and therefore tend to inhibit adaptability and innovation. Historically, the Coast Guard has not maintained a regular review and update of their NVICs and if this continues, then it would be probable that cybersecurity posture would actually decrease as complying with the detailed controls in the NVIC would not afford a suitable defense against newer threats. A better approach would be to refer to the NIST Cybersecurity Framework within the NVIC but direct the reader to NIST 800-82 (which is often quoted in the current text) and the Coast Guard NIST CSF (NCCOE/MITRE) Profiles. These documents include government and industry input, cover specific maritime operations and assets (e.g. bulk liquids transfer, offshore oil and natural gas, navigation systems) and can be more easily kept current as compared to a NVIC.

- **API member companies believe that there is an overemphasis within "Enclosure (2) 05-17" on vulnerability mitigation / management rather than risk mitigation / management.** ***Alternatively, API recommends that the NVIC be refocused on risk rather than vulnerability management.*** Vulnerability management is important but it is a component of risk management. Risk is a function of threat, susceptibility to threat, and impact; vulnerability is a component of susceptibility. Not all risks stem from exploited vulnerabilities (insider attacks are a classic example) and not all critical vulnerabilities may be exploitable (because of network segmentation or other controls.) Refocusing on risk management will ensure that the most impactful vulnerabilities are closed but will not rule out addressing other risks that do not rest upon vulnerabilities.

- **API member companies believe that tying cybersecurity activities to MARSEC levels is not suitable for cybersecurity.** ***API member companies recommend that the NVIC does not link cybersecurity to MARSEC levels and instead that the U.S. Coast Guard (USCG) communicate the level of security and response that the USCG will provide to industry on cybersecurity, as it does for physical security and in the event of a change to the MARSEC levels.*** "Enclosure (1) 05-17" mentions multiple times tying certain cybersecurity activities to MARSEC levels. The U.S. Coast Guard (https://www.uscg.mil/safetylevels/whatismarsec.asp) defines three Maritime Security levels: (1) MARSEC Level 1 means the level for which minimum appropriate security measures shall be maintained at all times; (2) MARSEC Level 2 means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a transportation security incident; and (3) MARSEC Level 3 means the level for which further specific protective security measures shall be maintained for a limited period of time when a transportation security incident is probable, imminent, or has occurred, although it may not be possible to identify the specific target

  "Additional protective security measures" are appropriate and more easily implemented for physical security; an example may be hiring more security guards to patrol a physical plant during a heightened emergency. Adding additional controls is less appropriate for cybersecurity. Generally, one will implement any and all controls that one can implement. That is, if one has whitelisting software to allow only known (good) programs to run, one is not going to hold that technology in reserve until a higher MARSEC level is proclaimed (as one is paying for the software one way or another). Adding personnel or other capabilities also takes significant time and effort. As one is likely to use all available cybersecurity controls, an increased MARSEC level would have little effect. Alternatively, one can consider cyber systems to be under constant attack and therefore must have all cybersecurity controls "on deck" at all times.

  In addition, this NVIC does not address the level of security and response the U.S. Coast Guard will provide industry in the event of a change to Maritime Security Level. An understanding of the level of USCG security and response is necessary as it factors into our risk based decisions on how to operate our facilities as maritime security levels change in the port or offshore environment. Historically, when the USCG engages with the maritime industry with regard to vessel navigation, safety and security, as well as environmental protection, USCG often provides training and exercises in order to facilitate industry understanding of new standards and technology.

- **The NVIC does not reference oil and natural gas industry standards for completing Facility Security Plans (FSPs).** ***API member companies recommend that the NVIC reference API Recommended Practice 781 “Facility Security Plan Methodology for the Oil and Natural Gas Industries,” which incorporates cybersecurity into facility security plans, as a possible means to meet the NVIC’s cybersecurity requirements.*** Much of the NVIC talks of incorporating cybersecurity into Facility Security Plans. API revised its Recommended Practice 781 “Facility Security Plan Methodology for the Oil and Natural Gas Industries” to do this within the past couple of years. This document may serve as a good industry reference for meeting the goals of the NVIC.

- **API member companies are concerned about how the Coast Guard intends to enforce the NVIC.** ***API member companies recommend that the Coast Guard clarify its resourcing for enforcing the NVIC and for working collaboratively with industry on cybersecurity.*** Coast Guard inspectors may likely lack the cybersecurity knowledge to assess the preparedness of a site. Cybersecurity, unlike physical security, will likely extend outside of the physical location; while location personnel are responsible for protection of the facility, cybersecurity will be a shared operation with some of the personnel responsible located miles away at corporate headquarters if not at cloud or other public sites.

  With the release of NVIC 05-17 it is still unclear what capacity USCG maritime inspectors and security specialists will have to engage and approve cybersecurity vulnerability assessments, and security plans as well as the appropriate level of understanding by facility security officers. Without clear engagement and basic understanding, industry will have a hard time providing the USCG with a consistent security posture across either local or national maritime security environments.

- **Outside of the publication of this NVIC, API member companies seek greater collaboration with the Coast Guard to address emerging potential cybersecurity threats.** For example, API member companies remain committed to maintaining the security and reliability of onboard safety mechanisms that would automate quick response in the event of casualty, which are connected with increasingly more sophisticated digital systems. The USCG already regulates safety devices on vessels and platforms with regard to physical capabilities of devices, such as currency of flares and life rafts, feasibility of fire suppression systems, etc. API member companies believe there is the potential for continued collaboration between industry and the Coast Guard to address the potential cyber risks to marine safety systems in order to continue to reduce the risk of injury, environmental damage or loss due to system loss, compromise or damage due to a cyber security breach.

We thank the U.S. Coast Guard for the opportunity to comment on the NVIC.

Sincerely,

Aaron Padilla

Aaron Padilla
Senior Advisor, International Policy

Specific API Comments on Text Within NVIC

Enclosure (1) 05-17

Section	Page	NVIC Text	Comment
Cyber Security and MTSA: 33 CFR Parts 105 and 106	1	This enclosure discusses the specific regulatory provisions that instruct owners/operators of a Maritime Transportation Security Act (MTSA) regulated facility to address cyber/computer system security in the Facility Security Assessment (FSA) and, if applicable, provide guidance within their FSPs to address any vulnerabilities identified in the Facility Security Assessment (FSA). …. If there are electronic or cybersecurity-related vulnerabilities identified in an FSA, an owner/operator may choose to provide this information in a variety of formats, such as a stand-alone cyber annex to their FSP, or by incorporating cybersecurity procedures alongside the physical security measures of their FSP	This section focuses on vulnerability rather than risk management. Vulnerabilities are part of risk management but absent a threat (either an actor or ability to exploit) and/or impact, a vulnerability is not a risk. Vulnerabilities need to be evaluated in the context of threat and impact and the computed risk used to determine which items to mitigate.
	1	If there are electronic or cybersecurity-related vulnerabilities identified in an FSA, an owner/operator may choose to provide this information in a variety of formats, such as a stand-alone cyber annex to their FSP, or by incorporating cybersecurity procedures alongside the physical security measures of their FSP.	It is unclear as to whether there will be multiple formats in which to report incidents and/or whether incident reporting will be required.
	1	Alternative Security Program. “Owners/operators that already employ a comprehensive cybersecurity plan for their organization, or who wish to apply a standard security program that incorporates cybersecurity to multiple facilities, may wish to submit a	The Coast Guard is inviting owners/operators to utilize the ASP protocol to address one portion of their overall security program. Currently ASPs are developed by industry groups and employed by members in good standing of these groups. ASPs address regulatory compliance holistically, without the

Section	Page	NVIC Text	Comment
		security plan under the Alternative Security Program, 33 CFR 101.120.”	one-to-one regulatory alignment demonstrated between the FSP and the checklist in Enc. 3 of NVIC 03.03 ch. 2. Requiring a focused cybersecurity plan to go through the ASP program would require facilities to draw up individual access control, restricted area, and cargo handling sections, among others, that have little to do with cybersecurity.
	1	Mandatory FSA Renewal. The NVIC states “Once this guidance is finalized, an owner/operator may demonstrate compliance with the regulations by including cyber risks in their FSA and including a general description of the cybersecurity measures taken in the FSP, if appropriate.”	According to the regulations, an FSA is performed as a precursor to the initial FSP. The FSA must be reviewed and validated, and the FSA report must be updated each time the FSP is submitted for re-approval or revisions (105.310(c)). The assessment is reviewed during the annual audit of the FSP (Enc. 8, NVIC 03-03, ch.2). Realistically, the original FSA may not receive much maintenance between five-year re-approval cycles. Under this direction, all facilities would be encouraged to perform a new FSA and re-write their FSPs to include a general description of the cybersecurity measures taken to mitigate vulnerabilities. This course of action would delay the inspection and approval cycle as well as place a burden on smaller port and maritime facilities.
	1	Owners/operators do not need to indicate specific or technical controls, but should provide general documentation on how they are addressing their cyber risks.	Assumption is that high level policies and procedures are expected but the document does not explicitly defined “general documentation”
Recommended Cyber Analysis as part of the FSA	2-5	The italicized text provides general guidance on how to potentially incorporate cyber aspects into those requirements	This would imply the NVIC is more guidance than requirement. There is a lack of clarity concerning the purpose of the regulatory sections and the italicized text below each section. The explanation in the NVIC: “Depending on the results of the

Section	Page	NVIC Text	Comment
			FSA, this section contains portions of subchapter H that may be applicable. The italicized text provides general, recommended guidance on how to mitigate cyber vulnerabilities determined during the FSA." Industry requests more clarity on the application of cyber security in these subsequent sections.
	2	Ensure information on cyber/computer systems is provided to person(s) conducting the facility security assessment and is considered in the analysis and recommendations and contained in report	The person conducting the facility assessment needs to have some background in cybersecurity to be able to appropriately use the information. Absent such knowledge, the person may fail to recognize serious risks that require mitigation or may overcompensate and try to fix all.
Recommended Cyber Analysis as part of the FSA: Recommendation to Address Identified Cyber Vulnerabilities (as applicable)	2	Describe the roles and responsibilities of cybersecurity personnel for the facility	Depending upon the size of the corporation and the network in place, some cybersecurity personnel "for the facility" may be at corporate central locations. The work listed in the comment is still valid but coordination may be more complicated.
	3	Describe additional cyber-related measures to be taken during changes in MARSEC levels.	Adding additional controls makes less sense in cybersecurity. Generally, one will implement any and all controls that one can implement and consequently an increased MARSEC level would have little effect. Alternatively, one can consider cyber systems to be under constant attack and therefore must have all cybersecurity controls "on deck" at all times.
	3	Cyber systems used to perform or support functions identified in the FSP should be maintained, tested, calibrated, and in good working order (e.g., conduct regular software updates and install security patches as they become	Security patches on process control systems are installed at regularly scheduled downtime, not "as they become available".

Section	Page	NVIC Text	Comment
		available).	
	4	Facility operators should establish security measures to control access to the facility Describe the security measures for access control at all MARSEC levels.	This seems to be focused only on physical access. Doesn't seem to be any corresponding (explicit) entry for logical (computer) access
	4	Describe security measures to protect cargo handling at all MARSEC levels to include measures that protect cargo manifests and other cargo documentation to deter tampering and prevent cargo that is not meant for carriage from being accepted	Cargo manifests and other documentation should be protected no matter what the MARSEC level. If you had a technology/control to control this information, you wouldn't hold it back because the MARSEC level was not high enough. There could be a cyber element to this section, however, it appears to be taken directly from the existing CFR publication that focus on physical and operational security. In other remediation sections, they added the term "cyber" at a minimum.
	4	Facility owners or operators should ensure the FSO develops and implements an FSP that addresses each cyber vulnerability identified in the Facility Security Assessment	There is an overemphasis on vulnerability identification and remediation vs. risk identification and remediation
	4	Describe cybersecurity measures to protect delivery of vessel stores and bunkers at all MARSEC levels to include procedures, which protect electronic files to deter tampering and ensure integrity of stores.	Likewise, if you have such protective technology available, you deploy it no matter what the MARSEC level is.

Enclosure (2) 05-17

Section	Page	NVIC Text	Comment
Background	1	The NIST CSF	It is good to reference the NIST CSF but the document should use the NIST CSF definitions of the functions rather than redefining them.
A. Identify and Cyber Governance **1. Establishing Cyber Risk Management**	2	Cyber risk management is an ongoing process of identifying and assessing vulnerabilities, responding to cyber events, and adjusting policies, programs, and procedures to minimize potential disruption	This is more a definition of “cybersecurity” than “cyber risk management”. Cyber risk management is assessing risk (threats – vulnerabilities – impact) and putting appropriate mitigations in place to bring risk within tolerance levels
A. Identify and Cyber Governance **1. Establishing Cyber Risk Management** **1.1 Define Cyber Responsibilities and Create a Cyber Risk Management Team**	2	Direct access to communicate with the highest level in the organization and with appropriate intermediate management levels	Should be “appropriate level” of management. Depending upon the definition of “organization”, the highest level of management might be the board of directors and they should not have such “hands on” responsibility
	3	While information technology (IT) specialists should be part of this effort, they may not fully recognize the various operational systems on a waterfront, the potential consequences, should they fail, or have an operator’s perspective on potential non-technical (and lower cost) solutions. In short, a team consisting only of IT professionals will only identify IT related threats and IT related solutions	The paragraph should emphasize, as the risk sentence begins, that the CRMT needs representation from all pertinent disciplines to identify IT, OT, safety, and physical issues that need to be addressed.
		Information technology specialists	One needs to recognize that not all needed information technology specialists may be located at the site.
		Some large organizations with diverse operations may centralize their cyber risk management policies at the corporate level. While this can be useful to ensure consistency across the organization, it is crucial that corporate cyber risk	Rather than trying to get central to manage facility risks, a better plan is to centralize policies which need to be centralized but distribute those which need local control.

Section	Page	NVIC Text	Comment
		management policy addresses facility-specific risks. Facility operators should be in communication with the corporate cyber risk management policy office to ensure the policy is aligned with their specific vulnerabilities and operations. (Source: NIST SP800-82-4.2.2)	
A. Identify and Cyber Governance **1. Establishing Cyber Risk Management** **1.3 Create a Cyber Risk Management Program**	4	Based on the evaluation of the severity of vulnerability, operators can prioritize systems for mitigation	Severity of the vulnerability is not a proper basis for prioritization. Risk should be that basis; vulnerability is part of risk as is threat and impact
2. Enterprise-Wide Inventory and Analysis	5	Enterprise-Wide Inventory and Analysis	"Enterprise" for large companies is world-wide and quite large. Likely, Coast Guard is more interested in the inventory of pertinent systems rather than all of those in a multi-national corporation?
3. Consequence Analysis, Vulnerability Analysis, and Mitigation Prioritization **3.1 Identify Critical Systems: Evaluate Consequences of Worst Case Scenarios**	7	Cybersecurity Risks – Potential for intentional disruption, compromise, or exploitation of a computer network or control system by non-authorized personnel.	This definition excludes the possibility of a malicious (authorized) individual
		Cyber Safety Risks – Potential for accidental disruption of a computer network or control system by an owner, operator, other actor, or as an unintended consequence of a mishap within a connected cyber system.	There is no need for a separate definition for "cyber safety" as the only difference between cyber safety and cybersecurity risks is intent.
		MTSA plan holders may examine consequences by reviewing the scenarios used to develop the Facility Security Plans or by examining system by system, asking, "What system failures could cause the worst possible consequences?" and "What is the worst possible consequence of a failure or disruption of this major	Agree with the lead-in clause to objectively consider worst case scenarios but the following (displayed) paragraph exclusively looks at worst cases rather than most likely or expected cases. Worst cases need to be reviewed but they alone do not constitute "risk management". All risks, not just worst cases, should be

Section	Page	NVIC Text	Comment
		system?". This will create a picture of which systems require the most rigorous examination.	considered. It is probably more likely for there to be minor incidents that in accumulation cause more damage than a black swan worst case. Focusing only on worst case will miss these other events.
	8	A Major Event would result in one or more deaths, injuries requiring professional medical treatment beyond first aid, damage to property, damage to or loss of a vessel at a facility, destruction of a facility, or discharge or release of oil or hazardous substance. Major events will generally have significant but acute impacts, or less severe but more sustained effects on the MTS	Corporate ratings systems tend to rate any death as catastrophic while Coast Guard has this at the category below.
		Operators should avoid connecting systems with components performing these functions to systems with lower levels of protection	True "air-gapping" is impossible within a modern process control network. Even if there are no physical network connections, outside (lower levels of protection) data / systems still need access. A better recommendation is that when networks of differing security levels are connected, one must do so through cybersecurity components and monitor the connection for unexpected traffic.
3. Consequence Analysis, Vulnerability Analysis, and Mitigation Prioritization **3.3 Vulnerability Severity Assessment**	9	This will be done by answering the questionnaire for each system with a "NO" answer from the Cyber Infrastructure Vulnerability Assessment (Table 4).	Assessing vulnerability severity is fine but this is not the final word on prioritization which should be based on risk assessment. As an example, a malicious insider will likely use granted privileges rather than exploit a hole in the network. Focusing strictly on vulnerability will miss this potential (and perhaps more likely) attacker This is more fodder as to why risk not vulnerability needs to be considered as the basis for prioritization.

Section	Page	NVIC Text	Comment
4. Protect, Detect, Respond, Recover: Recommended Guidance	10	Once the CRMT recognizes their cyber risks, the organization can select strategies to reduce that risk. However, adequately protecting digital information and cyber dependent system does not usually entail a straight-forward, sequential implementation of specific mitigation measures. Organizations should implement multiple layers of safeguards across a number of different realms (e.g. contracting, human resource management, education and training, network design, physical security, access control, etc).	The risk-based approach outlined in this Section 4 is welcome, in contrast to the emphasis on vulnerability mitigation / management in Section 3. Again, we believe that assessing vulnerability severity is fine but should not be the determinant of prioritization, which should be based on risk assessment.
		While high-risk systems should have more robust protection strategies, this does not necessarily require sophisticated technical solutions	This could be stated more strongly that technical solutions alone are generally insufficient; one needs to have proper policies, procedures, and people (training) to make the technology work.
4. Protect, Detect, Respond, Recover: Recommended Guidance **4.1.1 Cyber Risk Awareness Program**	10	4.1.1 Cyber Risk Awareness Program. Facilities should maintain, and enforce a cyber risk awareness program for employees and contractors. The awareness program should ensure that new and existing employees, as well as contractors requiring access to the organization's IT/OT networks, receive job-relevant training and direction related to the organization's cyber risk management policy.	Much of this is likely provided in corporate awareness training not specifically by the site.
4. Protect, Detect, Respond, Recover: Recommended Guidance **4.1.3 Access Control**	11	4.1.3 Access Control	This is more "authentication" rather than "access control" which generally tends to focus on data/file access
		SSO can reduce the amount 0T of secret authentication information that users are required to protect and thus can increase the effectiveness of this control (the more authentication-related information users are	This statement is true but a problem with SSO is that a compromised credential provides access to multiple (all) systems SSO should not be applied to both low priority and high priority

Section	Page	NVIC Text	Comment
		asked to remember, the more likely they are to forget it or write it down).	systems.
		In order to protect access to critical systems, a secure password management system should:	The document spends significant time on passwords but none on (better) multifactor authentication
	11-12	The value of password protection should be weighed against the risks associated with time-sensitive operations. In cases where rapid access is vital to operations or safety, risks may be better mitigated with manual backups or other procedures.	Agree with the statement that passwords may get into the way of time-sensitive operations but fail to see how manual backups solve a problem of a refinery going critical because an operator forgot his/her password.
	12	In some instances, operational requirements make effective network segmentation a challenge. In such cases, encryption and/or the use of Virtual Private Networks (VPNs) can help organizations better ensure the protection of their critical information	VPN allows a secure connection from one segmented network to another. As VPN would only be used between segmented networks, it is unclear how VPN Helps with the situations when segmentation is a "challenge". Encryption protects data; process control generally favors availability over confidentiality so not sure how encryption helps here either
4. Protect, Detect, Respond, Recover: Recommended Guidance **4.1.4 Network Segmentation**	13	Figure 1 illustrates an "air gap" between business and control systems networks. … Figure 2 shows all the potential ports and access points in an air-gapped control system compared to systems that are not segregated into separate networks.	Air-gapping is really not realistic. Even if one disconnects a network, there are means (U.S.B, vendor maintenance, etc.) where outside devices are brought in. One person I know called an air-gapped network one with very high latency. The integrated picture is not in accordance with accepted architectures like the Purdue Model (ISA 62243) which place a DMZ and cybersecurity stack that manages/monitors/restricts traffic between the process control and business networks. Therefore, comparing and contrasting air-gapped and non-air-gapped systems is a waste of time.
4. Protect, Detect, Respond, Recover: Recommended	14	Remote maintenance of organizational assets should be approved, logged, and	This is a key control

Section	Page	NVIC Text	Comment
Guidance **4.1.5 Protect Equipment**		performed in a manner that prevents unauthorized access.	
	15	To protect against risks resulting from the use of legacy systems, where adequate security measures cannot be implemented, organizations should consider the following	The document does not define "adequate security measures"? The paragraph says these are not available then suggests two solutions that must be "adequate" or what's the point. Normally, we would say that if standard (rather than "adequate") security measures cannot be deployed, one must accept the risk or deploy compensating controls.
	16	Strong authentication (e.g. password protection, biometric ID)	No one normally considers one factor authentication to be "strong." Even "strong" passwords and/or biometrics are weak when compared to multi-factor authentication.
4.2 Detect **4.2.1 Monitor Traffic**	17	Establish and implement procedures to monitor network traffic, physical security, and the activities of external parties and personnel to ensure integrity and availability of cyber systems	As it is written, this scope includes monitoring of remote connections/activity and local connections/activity which includes direct monitoring of the ICS networks.
4.2 Detect **4.2.2 Reporting Responsibilities**	17	Report breaches of cybersecurity and cyber suspicious activity in accordance with current regulations, policy and guidance	There is no reason for this text to be in italics
4.2 Detect **4.2.3 Keep Logs**	17	To ensure accuracy of event logs and subsequent reports, the clocks of all relevant IT/OT systems within an organization should be synchronized	Some recommendation should be specified on the length of time to keep logs.
4.2 Detect **4.2.4 Run Tests**	18	Penetration tests performed by external experts employ attacks using both cyber and social engineering-based elements.	Should say "can employ attacks using both cyber and social engineering-based elements". It's dependent on the defined scope and assessor.
4.2 Detect **4.2.5 Deploy and Update Intrusion Detection Systems**	18	4.2.5 Deploy and Update Intrusion Detection Systems	This is one of the only sections in this enclosure that doesn't specify the environments they want addressed (e.g. IT/OT). They should include this to level set expectations. This section also duplicates the last bullet from protect although there,

Section	Page	NVIC Text	Comment
			intrusion **prevention** systems were deployed with no mention of intrusion **detection** systems. This paragraph goes (needlessly?) into more detail on how IPS/IDS works which is not particularly germane.
4.3 Respond **4.3.1 Investigate Notifications**	19	If monitoring reveals an anomaly, organizations should be able to quickly determine whether the cause is a security incident, a hardware or software problem, or an increase in client demand	Experience finds that rarely can even a sophisticated Security Operations Center "quickly" determine whether an "anomaly" is a cybersecurity incident or not. This generally requires some amount of research / investigation.
4.3 Respond **4.3.2 Plan Thoroughly**	19	4.3.2 Plan Thoroughly	Planning activity should precede investigation. If you do not have the roles defined, then how does anyone know they have investigation responsibilities. Even if they do know, to whom should they report attacks?
4.3 Respond **4.3.3 Limit Consequences**	20	Consider the use of external experts who are skilled in conducting interviews and retracing the behaviour of people who had access to protected information.	British spelling of "behaviour" is used rather than the American "behavior".
4.4 Recover **4.4.1 Back Up Information**	21	4.4.1 Back Up Information	Backups are technically part of NIST CSF Protect, not Recover
4.4 Recover **4.4.4 Perform Exercises**	22	the critical cyber dependent services to be recovered;	It's not clear if the USCG expects to see recovery plans/procedures down to specific automation and control systems, but if they do, this is where they'll call that to attention.

Appendix A 05-17

Section	Page	NVIC Text	Comment
Table 2: Consequence Score Action	1	Table 2	Focused on vulnerability rather than risk
Table 4: Cyber Infrastructure Vulnerability Assessment	3	Table 4	Focused on vulnerability rather than risk
Table 5: Vulnerability Severity Assessment	4	No user-developed software No user-modified software No OSS	Implies user developed, user modified, and open source software is less secure than vendor software