NVIC 01-20, CG-5P Policy Letter 08-16 & the Facility Inspector – Cyber Security Job Aid

By David E. Majors, V.P., Marsec Corp.

The Coast Guard has become extremely concerned about threats from the cyber world and how they affect your facility or vessel. The bulk of the interest is in regard to facilities, so that is the audience I will primarily address in this article.

The Coast Guard's interest became particularly piqued following the June 2017 NotPetya Ransom-ware attack on A.P. Moller-Maersk, which moves approximately one-fifth of the world's freight. By the time the situation was resolved, the company suffered losses in the range of $350 million. And at that, considered themselves lucky as it turned out that their data had not actually been taken but "only" blocked so that they could not access it. See this ComputerWeekly.com article for details and lessons learned, "NotPetya offers industry-wide lessons, says Maersk's tech chief."

When the Coast Guard gets interested in something, we get new guidance and thus we have received three recent such pieces. The first was CG-5P Policy Letter 08-16. It is entitled "Reporting Suspicious Activity and Breaches of Security." My personal view of this document is that it is extremely useful, even if you have NO cyber-security related equipment on your facility.

Having been in the maritime security consulting business for quite some time, I have been asked, more times than I can count, about some particular event that had occurred at a facility and whether it needed to be reported to either the local Coast Guard Captain of the Port (COTP) or the National Response Center (NRC). PAC 08-16 will help you to answer that question should such an unusual event occur at your facility as it gives guidance not just for cyber-related incidents, but for both Suspicious Activity (SA) and Breaches of Security (BoS) and how the Coast Guard views a variety of such events.

PAC 08-16 also introduces a new office that you should be aware of, the National Cybersecurity and Communications Integration Center (NCCIC). Its function is "as a national nexus of cyber and communications integration for the

Federal Government, intelligence community, and law enforcement. For cyber incidents that do not also involve physical or pollution effects, the Coast Guard allows reporting parties to call and report the incident to the NCCIC in lieu of the NRC, as the NCCIC may be able to provide technical assistance to the reporting party." The PAC goes on to state that, "It is imperative that the reporting party inform the NCCIC that they are a Coast Guard regulated entity in order to satisfy the reporting requirements of 33 CFR 101.305. The NCCIC will forward the report electronically to the NRC, who will notify the appropriate COTP." In my opinion you are best off if you continue to make such reports directly to the NRC, so you do not have to worry about whether such notification has occurred. If you do it yourself, then you are CERTAIN. Then, if you believe that NCCIC may be of assistance, contact them at (888) 282-0870.

You should also be aware of their sub-unit, ICS-CERT, which is apparently at least partially staffed with USCG members, and who may be able to offer assistance, particularly in any case you may experience that involves hacking of industrial control systems.

If you have a Marsec® Corporation written Facility Security Plan (FSP) dating from November 29, 2017 or later, your Plan should already have excerpts from PAC 08-16 included within Section 15 Security Incident Procedures. Again, these are mostly concerned with reporting procedures and as such do not impose any significant additional burden on facilities.

On February 26, 2020, NVIC 01-20 Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities was released. While the NVIC is described as not changing any legal requirements, and not imposing any new requirements on the public, it will most certainly require considerable additional work on your part. Essentially, this NVIC requires facilities to assess their level of cyber-security, identify any vulnerabilities and identify measures to mitigate those vulnerabilities. Regulations require that any cybersecurity vulnerabilities identified in the Facility Security Assessment (FSA) must be addressed in the Facility Security Plan (FSP) or Alternative Security Program (ASP).

As is always the case, "mitigate" does NOT necessarily mean "eliminate". In an ideal world that would be the case, but in the real world, with an ever-evolving

cyber threat picture, a threat eliminated on one day is often replaced by another soon thereafter.

Due dates for this assessment are described by this statement in the March 25, 2020 USCG Maritime Commons, "*Beginning 10/01/2021, facilities that need to submit cyber FSA and FSP/ASP amendments or annexes should do so by the facility's annual audit date, which is based on the facility's FSP/ASP approval date. COTPs will still have the flexibility based on resource demands, or based upon request from a facility, to adjust when submissions are received, as long as all facility FSA and FSP (Headquarters for ASPs) submissions are received by the end of the one year period, no later than 10/01/2022*." It goes on to state that whoever conducts the cyber portion of this audit should also be a signatory on the audit letter and list their qualifications. Your IT Department, if you have one, should certainly be made aware of this fact. I HIGHLY recommend that this cyber assessment be completed PRIOR to your usual annual audit as it is otherwise HIGHLY likely to impose significant delays on audit completion.

The NVIC also stipulates that you need not provide the names of products, such as anti-virus programs, that you are using at the time of the cyber assessment. You should however supply enough information that your Plan reviewer can see that the measures you take for mitigation are appropriate for the identified vulnerabilities.

A Frequently Asked Questions (FAQ) page has been developed and is expected to be updated based on questions and feedback received. The FAQ can be accessed at 01-20 FAQ.

The third piece of guidance released is called the Facility Inspector Cyber Job Aid. Like the twenty-six page checklist in NVIC 03-03 CH 2 that has been in use for some time to review your Plan, it contains a fourteen-page checklist for the Coast Guard's Plan reviewers to use when reviewing the cyber aspects of your FSP.

SO WHAT DOES THAT MEAN FOR MY FACILITY?

For a very few small facilities with little computerized equipment, it may not mean much. If you can answer "No" to the following three questions, it may

not be a stretch to describe the vast bulk of the listed items in the checklist as being N/A;

1. Is data stored off-site (or both on and off-site)?

2. Does data have a critical link to safety or security functions?

3. Could a computer or other cyber-system failure result in a Transportation Security Incident?

Please note that *Transportation security incident (TSI)* means "*a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area*".

It will be more complicated if you do not fall into this category. In the comments within the Federal Register discussing NVIC 01-20, several questions were raised (some of them by Marsec Corporation) and answered by the Coast Guard. Below are a selection of those most critical along with other issues of which you should be aware;

1. Doubt was expressed about the Coast Guard's capability to perform Plan Review of cyber assessments at the unit level. The downside being that if this is too complex to task to the usual Plan Reviewers, then all FSPs would have to be funneled through a higher echelon office, slowing the process to a near grinding halt. In response, the Coast Guard replies that among other things, the time preceding 10-01-21 will be used to familiarize their reviewers with these processes. The Facility Inspector Cyber Job Aid is designed to resolve this issue.

2. While the Coast Guard encourages the use of the Institute of Standards and Technology's Cyber Security Framework (NIST CSF) to improve the facility's cyber posture above what is outlined in the (sample procedures) outlined in the NVIC, and provides links on the FAQ page, to the Framework, guidance is flexible allowing each facility to create solutions that fit its specific needs and changing risks. The NVIC therefore should not be viewed as a checklist of prescribed cyber-security solutions. (Author's note): The "Framework" itself as well as an

additional link with a short PowerPoint (described as Framework V1.1 Downloadable Presentation) is available at https://www.nist.gov/cyberframework/framework

3. The comments stress that this is not "new" regulation, but instead is an integral part of a Facility Security Assessment (FSA). The reasoning was the following wording from 33 CFR 105.300(d) which states that "*Those involved in a FSA must be able to draw upon expert assistance in the following areas, as appropriate: (long list of qualifications follows, but included among them are:) (11) Radio and telecommunications systems, including computer systems and networks*". "*The Coast Guard believes this includes the expertise needed to self-assess risk and establish security measures to counter the risks involved with a MTSA-regulated facility's computer systems and networks.*" (Author's Note: QUITE the reinterpretation in my humble opinion).

4. Recommends viewing an American Bureau of Shipping webinar entitled "Marine Transportation System Cyber Awareness". The focus is on identifying cyber systems that are related to MTSA regulatory functions or that could cause or contribute to a Transportation Security Incident (TSI). (Author's note: I also recommend viewing this as it covers the differences and interfaces between Information Technology (IT), (often handled at corporate level) and Operational Technology (OT), (often handled locally) and how they are being more frequently linked. It certainly helps clarify what equipment should be considered when performing this assessment.

5. The Federal Register comments stress that this applies to MTSA-regulated facilities but not to Ports, except those Ports that are MTSA-regulated.

6. While the due dates are not included in the Federal Register, (see the linked Maritime Commons article above for those), the comments state that the assessment must be completed, and that Plans must be amended by either revising current FSPs or attaching a cyber-annex to the FSP. In either case, those would be the only portions of the FSP to be reviewed and re-approved.

I anticipate that in Marsec® Corporation drafted Plans, this will actually result in a blend of the two with short inputs into several Sections of our Plans to deal with Section-specific suggested items listed in the NVIC plus a new Appendix composed of a report supplied by the client's IT Department showing the vulnerabilities noted and security measures in place to deal with them. It is our intention to scan these reports into this Appendix in their entirety.

FSOs should ensure that the company's IT department is provided access to all of the guidance linked within this article so they are fully aware of both the guidelines and the tools that the Coast Guard will be using to assess their reports (i.e. the Facility Inspector Cyber Job Aid). "Writing to the Job Aid", is highly encouraged. Especially in terms of aligning the report to the checklist in the Job Aid so that the things that the CG's reviewers are looking for fall in the same order as shown in that Aid. The cyber-Amendments included within your Plan are MUCH more likely to be approved on the first try if the reviewers can easily relate the line items in the job aid with the information in your report. Remember, these reviewers are UNLIKELY to be full-time IT professionals. On the contrary, they will likely be the same Coast Guard Petty Officers who have reviewed the rest of the Plan dealing with the usual physical concerns. So PLEASE make it easy for them to find what they are looking for in the order they expect to find it.

7. Procedures for managing software updates and patch installations should be described in the FSP.

8. The burden for conducting cyber-security assessment falls on the facility. The good news is that how it is achieved is not limited unlike those for physical security audits. In short you may use your own IT department staff to conduct the assessment, should you wish. In most cases, this is likely to be the desired approach due to the fact that there is probably no one more familiar with your systems than your own staff-members managing them.

Within NVIC 01-20 itself, descriptive recommendations of wording to include within the FSP, applying to particular Sections within your Plan are shown in italics

following citations describing that Section. Below is one for Section 3, Drills & Exercises;

"Drills and Exercises"
33 CFR 105.220
33 CFR 106.225

Describe how drills and exercises will test cyber security vulnerabilities of the FSP. Facility owners and operators may wish to meet this requirement by employing combined cyber-physical scenarios. In general, drills and exercises must test the proficiency of personnel assigned to security duties and enable the Facility Security Officer (FSO) to identify any related security deficiencies that need to be addressed."

As noted in paragraph 6 above, Marsec Corporation has drafted language to cover all of these within our sample FSP (and which we intend to use within our client's Plans, with their approval).

Our foremost concerns in doing so, were that the procedures be;

(1). Reasonably easy to understand and achieve
(2). Minimally consuming of the security department's time and resources
(3). Meet the Coast Guard's concerns

In this particular case, the wording we used stipulated that at least one of the facility's four required drills each year would involve a cyber-security aspect.

It has also come to our notice that certain Captains of the Port are requiring that this be performed on all "new" or "renewed" Plans being submitted as of now.

And that is all we have for you at this time. There is a fair chance that additional guidance will appear prior to October 1, 2021. If so, it is our intention to add it to this page.