SHIPS NAME: ..
IMO No: ..

Date on-scene survey: ..
Place on-scene survey: ..

CYBER SECURITY THREAT/VULNERABILITY ASSESSMENT

HUMAN THREATS	Relevant		Consequence	Likelihood	Score	Prevention
	Yes	No	1-6	1-6		
Human Error						
Accidental destruction, modification, disclosure, or incorrect classification of information	☐	☐				
Ignorance: inadequate security awareness, lack of security guidelines, lack of proper documentation, lack of knowledge	☐	☐				
Workload: Too many or too few system administrators, highly pressured users	☐	☐				
Users may inadvertently give information on security weaknesses to attackers	☐	☐				
Incorrect system configuration	☐	☐				

Security policy not adequate	☐	☐				
Security policy not enforced		☐				
Security analysis may have omitted something important or be wrong.	☐	☐				
Dishonesty						
Fraud, theft, embezzlement, selling of confidential agency information	☐	☐				
Social engineering						
Attackers may use telephone to impersonate employees to persuade users/administrators to give user name/passwords/modem numbers, etc.	☐	☐				
Attackers may persuade users to execute Trojan Horse programs	☐	☐				
GENERAL THREATS						
Unauthorized use of “open” computers/Laptops’	☐	☐				
Introduction of unauthorized software or hardware	☐	☐				
Time bombs: Software programmed to damage a system on a certain date	☐	☐				
Operating system design errors: Certain systems were not designed to be highly secure	☐	☐				
Protocol design error: Source routing, DNS spoofing, TCP sequence guessing, unauthorized access	☐	☐				
Protocol design error: Hijacked sessions and authentication session/transaction replay, data is changed or copied during transmission	☐	☐				
Protocol design error: Denial of service, due to ICMP bombing, TCP-SYN flooding, large PING packets, etc.	☐	☐				
Logic bomb: Software programmed to damage a system under certain conditions						
Viruses in programs, documents, e-mail attachments	☐	☐				
IDENTIFICATION AUTHORIZATION THREATS						

Attack programs masquerading as normal programs (Trojan horses).	☐	☐				
Attack hardware masquerading as normal commercial hardware	☐	☐				
External attackers masquerading as valid users or customers	☐	☐				
Internal attackers masquerading as valid users or customers	☐	☐				
Attackers masquerading as helpdesk/support personnel	☐	☐				
PRIVACY THREATS						
Electromagnetic eavesdropping / Ban Eck radiation	☐	☐				
Telephone/fax eavesdropping (via “clip-on” telephone bugs, inductive sensors, or hacking the public telephone exchanges	☐	☐				
Network eavesdropping. Unauthorized monitoring of sensitive data crossing the internal network, unknown to the data owner	☐	☐				
Subversion of ONS to redirect email or other traffic	☐	☐				
Subversion of routing protocols to redirect email or other traffic						
Radio signal eavesdropping,	☐	☐				
Rubbish eavesdropping (analyzing waste for confidential documents, etc.)	☐	☐				
INTEGRITY / ACCURACY THREATS						
Malicious, deliberate damage of information or information processing functions from external sources	☐	☐				
Malicious, deliberate damage of information or information processing functions from internal sources	☐	☐				
Deliberate modification of information	☐	☐				
ACCESS CONTROL THREATS						
Password cracking (access to password files, use of bad, blank, default rarely changed passwords)	☐	☐				
External access to password files, and sniffing of the networks	☐	☐				
Attack programs allowing access to systems (back doors visible to external networks)	☐	☐				
Unsecured maintenance modes, developer backdoors	☐	☐				

Modems easily connected, allowing uncontrollable extension of the internal network	☐	☐				
Bugs in network soft are which can open unknown/unexpected security holes.						
Unauthorized physical access to system	☐	☐				
RELIABILITY OF SERVICE THREATS						
Equipment failure from defective hardware, cabling, or communications system.	☐	☐				
Equipment failure from airborne dust, electromagnetic interference, or static electricity	☐	☐				
Denial of Service						
Email bombing	☐	☐				
Server overloading	☐	☐				
Sabotage						
Physical destruction of network, devices and cables	☐	☐				
Viruses and/or worms. Deletion of critical systems files	☐	☐				

Risk = Consequence x Likelihood

For this assessment, numeric rating scales are used to establish consequence potential (1-6) and likelihood probability (1-6).

Consequence	Likelihood
1. Impact is negligible	1. Unlikely to occur
2. Effect is minor, major agency operations are not affected	2. Likely to occur less than once per year
3. Organization operations are unavailable for a certain amount of time, cots are incurred.	3. Likely to occur once per year
4. Significant loss of operation.	4. Likely to occur once per month
5. Effect disastrous, systems are down for an extended period of time	5. Likely to occur once per week
6. Effect is catastrophic, critical systems are offline for extended period of time, data is lost or irreparably corrupted	6. Likely to occur daily

The following table to determine and understand the potential criticality (risk level) of each threat/vulnerability based on the calculated risk value.

Score	**Risk Level**	**Risk occurrence result**
1 - 12	Low risk	Occurrence may result in minimal loss of assets, information or information resources. May affect the vessels operation.
13 - 24	Medium Risk	Occurrence may result in some loss of assets, information or information resources. May disrupt the vessels operation.
25 - 36	High Risk	Occurrence may result in significant loss of assets, information or information resources. May seriously disrupt the vessels operation.

ON-SCENE CYBER SECURITY SURVEY

PERSONELL SECURITY	**Yes**	**No**	**NA**	**Observation**	**Countermeasures**
Do you have a process for effectively cutting off access to facilities and information systems when an employee/contractor terminates employment?	☐	☐	☐		
PHYSICAL SECURITY	**Yes**	**No**	**NA**	**Observation**	**Countermeasures**
Are your PCs inaccessible to unauthorized users (e.g. located away from public areas)?	☐	☐	☐		
Is your computing area and equipment physically secured?	☐	☐	☐		
Are there procedures in place to prevent computers from being left in a logged-on state, however briefly?	☐	☐	☐		
Are screens automatically locked after 10 minutes idle?	☐	☐	☐		
Are modems set to Auto-Answer OFF (not to accept incoming calls)?	☐	☐	☐		
Do you have procedures for protecting data during equipment repairs?	☐	☐	☐		
ACCOUNT AND PASSWORD MANAGEMENT	**Yes**	**No**	**NA**	**Observation**	**Countermeasures**
Do you ensure that only authorized personnel have access to your computers?	☐	☐	☐		
Do you require and enforce appropriate passwords?	☐	☐	☐		
Are your passwords secure (not easy to guess, regularly changed, no use of temporary or default passwords)?	☐	☐	☐		
Are you computers set up so others cannot view staff entering passwords?	☐	☐	☐		
CONFIDENTIALITY OF SENSITIVE DATA	**Yes**	**No**	**NA**	**Observation**	**Countermeasures**
Do you classify your data, identifying sensitive data					

Do you classify your data, identifying sensitive data versus non sensitive?					
Is the most valuable or sensitive data encrypted?	☐	☐	☐		
Do you have procedures in place to deal with credit card information?	☐	☐	☐		
Is there a process for creating retrievable back up and archival copies of critical information?	☐	☐	☐		
Is waste paper binned or shredded?	☐	☐	☐		
Do your policies for disposing of old computer equipment protect against loss of data (e.g.. by reading old disks and hard drives)?	☐	☐	☐		
EMERGENCY PREPAREDNESS	**Yes**	**No**	**NA**	**Observation**	**Countermeasures**
Do you have a current contingency plan?	☐	☐	☐		
Is there a process for creating retrievable back up and archival copies of critical information?	☐	☐	☐		
Do you have an emergency/incident management communications plan?	☐	☐	☐		
Do you have a procedure for notifying authorities in the case of a disaster or security incident?	☐	☐	☐		
Have you identified who will speak to the press/public in the case of an emergency or an incident?	☐	☐	☐		
SECURITY AWARENESS AND TRAINING	**Yes**	**No**	**NA**	**Observation**	**Countermeasures**
Are you providing information about computer security to your staff?	☐	☐	☐		
Do you provide training on a regular recurring basis?	☐	☐	☐		
Are employees taught to be alert to possible security breaches?	☐	☐	☐		
Are your employees taught about keeping their passwords secure?	☐	☐	☐		

Do you review and revise your security documents, such as: policies, standards, procedures, and guidelines, on a regular basis?	☐	☐	☐		
Do you audit your processes and procedures for compliance with established policies and standards?	☐	☐	☐		
Do you test your contingency plans on a regular basis?	☐	☐	☐		