Industry Recommended Framework and Implementation Roadmap for Delivering Cyber-Ready Ships

Harshal Patil | August 22, 2024

Agenda

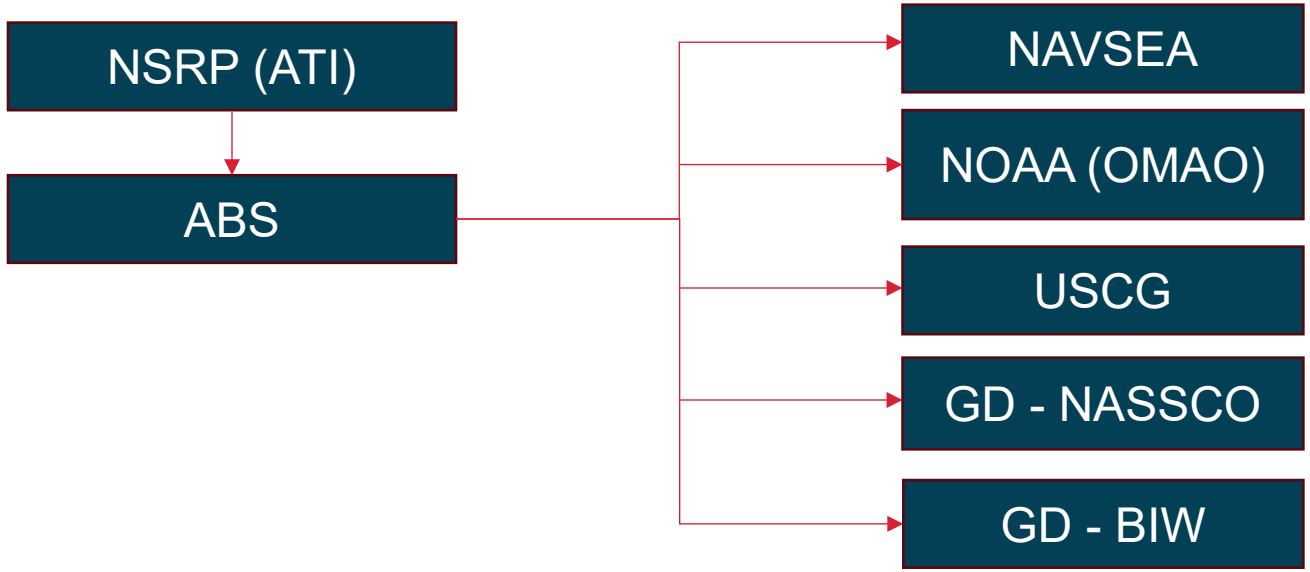
1.	Introduction
2.	Project Stakeholders
3.	Project Overview
4.	Activities Performed
5.	Next Steps
6.	Industry Workshop
7.	Questions

Meet the Speaker

Harshal Patil
Principal Cybersecurity Engineer

Project Stakeholders

Project Stakeholders



- NSRP (ATI) – National Ship Research Program Advanced Technology International
- ABS – American Bureau of Shipping
- NAVSEA – Naval Sea Systems Command
- NOAA - OMAO – National Oceanic and Atmospheric Administration Office of Maritime and Aviation Operations
- GD - NASSCO – General Dynamics National Steel and Shipbuilding Company
- GD - BIW – General Dynamics Bath Iron Works
- USCG – United States Coast Guard

Project Overview

Problem Statement

- Starting 1 July 2024, all new construction vessels (over 500GT) seeking class approval will be required to meet the cyber resilience requirements included in IACS UR E26 and E27
  - ABS Requirements UR E26 (eagle.org)
  - ABS Requirements UR E27 (eagle.org)
- U.S shipbuilders must meet various cyber requirements like Navy Risk Management Framework (RMF), NIST Cyber Framework, Class Society requirements in delivering ships for U.S Government Agencies
  - NAVY/MSC, USCG, NOAA, MARAD, USACE, and other law enforcement and research entities
- These new cyber resilience requirements not only impact shipbuilders, but the entire critical equipment/ systems supply chain
- Road map to focus on major activities to be completed by shipyards before delivering a vessel

Project Strategy and Key Deliverables

Project Strategy to Deliver

ABS will lead this strategic effort in collaboration with GD-BIW, GD-NASSCO and the support of the shipbuilding community to develop a recommended roadmap and overall implementation framework

Key Deliverables

- A Cyber-Ready guidance framework and implementation roadmap that is agnostic to specific technology and vendors/tools for Government fleet owners/ operators to complete their cybersecurity certification process and gain the appropriate authority to operate

- As part of the technology transfer process, a webinar will be provided to government and industry agencies

- Publications and participation in various industry and government channels

Project Objectives

PROJECT GOAL

To produce a document that Government fleet owners/operators can reference in their specifications for future ships so that shipbuilders have clarity in requirements for delivering Cyber-Ready ships

- Reduce the shipbuilding cost of meeting currently uncertain and changing cybersecurity requirements for ship deliveries
- Better prepare Government fleet owner/operators to complete cybersecurity certifications and gain Atos using information delivered with ships
- Help improve cybersecurity posture for ships within a framework that considers the full supply chain associated with ship delivery (shipbuilders, OEMs, system integrators, etc.)

Project Benefit Metrics

Project Benefit

Shipyards will benefit from more standardized expectations across the industry on how to meet the various Government requirements for cybersecurity at ship delivery

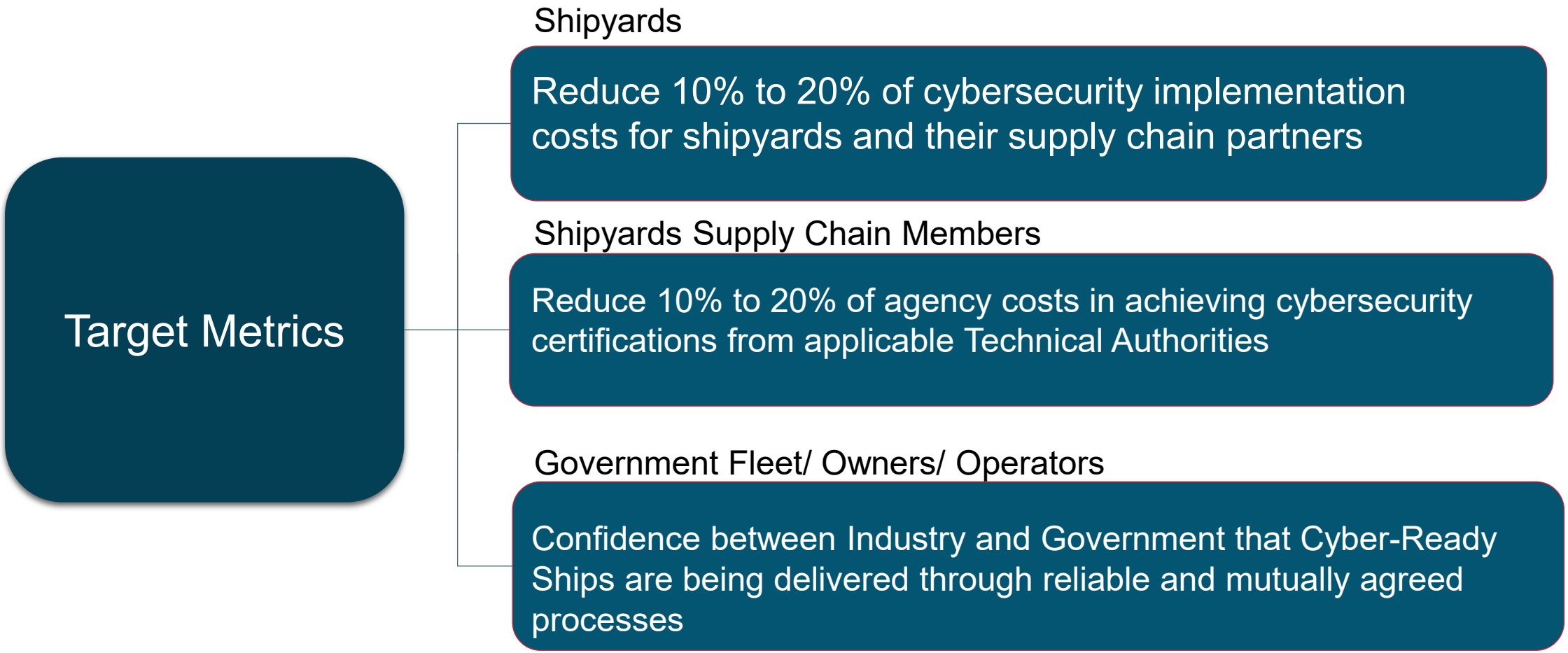
Shipyards Supply Chain Members

Alignment of requirements for delivering Cyber-Ready ships will strongly benefit supply chains supporting yards

Government Fleet/ Owners/ Operators

Agencies will benefit from having ready-made guidance from the industry that supports compliance with agency requirements and can be referenced easily in ship

Project Target Benefit Metrics



Activities Performed

Project Tasks

Task Details		
Task 1 Document the range of cybersecurity compliance requirements and best practices	Task 2 Document compliance procedures/methods followed by Shipyards to meet cyber requirements	Task 3 Industry workshop to review compliance requirements and obtain information on compliance processes followed by industry

Project Tasks

Task Details

Task 4	Task 5	Task 6
Develop a roadmap for delivering Cyber-Ready ships in the most cost-effective and efficient manner	Host a government/industry workshop presenting the Cyber-Ready ship framework	Finalize the roadmap for implementation of Cyber-Ready Ships

Task 1 Activities (1 May 2024 to 12 July 2024)

- Document submission from various stakeholders
  - NAVSEA – Cyber Survivability Endorsement Guide, 8510.01 (Risk Management Framework) and 8500.01
  - USCG Cyber SOW – 10 requirements with references to the Risk Management Framework as per DoDI 8510.0.
  - General Dynamics NASSCO – Internal Cyber requirements
  - General Dynamics Bath Iron Works – Internal Cyber requirements

Task 1 Activities (1 May 2024 to 12 July 2024)

- ABS has compiled the requirements that are being sent by all the stakeholders
- There are requirements that map the cybersecurity requirements to
  - DOD Risk Management Framework (RMF) based on NIST 800-37 (Risk Management Framework for Information Systems and Organizations)
  - NIST 800.53 Rev 5 (Security and Privacy Controls for Information systems and Organizations)
  - NIST 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations)
  - NIST 800-82 (Guide to Operational Technology (OT) Security)
- ABS identified requirements from International Association of Classification Societies (IACS)
  - IACS Unified Requirement E26 “Cyber Resilience of Ships”
  - ABS Cybersafety requirements for CS-System, CS- Ready, CS-1 and CS-G notations

Next Steps

Project Steps In Next 6 months

- Shipyards to document how requirements are currently addressed, including work processes and non-proprietary methods/tools they are using
- ABS to conduct workshop to collect feedback on compliance requirements and how the requirements are met
- Develop a draft roadmap based on the collected inputs from all the stakeholders
- Present draft framework and its key concepts in a webinar
- Revise the draft framework based on the webinar's feedback

Industry Workshop

Industry Workshop Agenda

- To be scheduled in September 2024
- Present the requirements that are currently being submitted by the participating stakeholders of the project
- Gather inputs from the workshop participants on how the cybersecurity requirements are being currently addressed during construction phase including information about the timelines
- Gather other cybersecurity requirements during construction phase from the stakeholders

Questions?

Thank You

www.eagle.org