# USS Ship Security Awareness Program

## Table of Contents

Executive Summary ......................................................................................... 3

Engagement and Training Strategies …............................................................ 4

Overall Engagement Strategy …........................................................... 4

Primary Training Strategy …................................................................ 6

Sustainment Training Strategy …......................................................... 6

Metrics ….......................................................................................................... 8

Training Specification Sheets …....................................................................... 10

## Executive Summary

As a multi-billion-dollar national asset, USS Ship and her crew are a unique and invaluable part of a national critical infrastructure relied upon to deliver intelligence and data for national decision-makers. As a warship and her crew, we must maintain the highest levels of readiness to enforce free navigation of international waters, interdict illicit trade, protect US coastlines, and defend US interests abroad. Finally, should the call arise, we must be ready to shoot at a moment’s notice.

The technologies on our warship are a vast network of interconnected information systems. Long gone is the era of mostly mechanical systems operated solely by human grit and ingenuity. Today, our modern warship is akin to an interconnected nerve center of sensors, communication circuits, computers, control systems, and user interfaces. While unique compared to other information systems, being air-gapped and independent of civilian internet technologies, there is one risk that is ever-present and persistent:

Our human risk.

Security Awareness Programs formalize and strategically plan an organization’s process for educating its people on security risks and best practices. This document outlines our command’s implementation of a Security Awareness Program (SAP) to mitigate our human risk in the cybersecurity realm and train our sailors to understand, recognize, and successfully manage the risks they may experience on and off duty. Ultimately, this program exists to ensure our ship is ready and able to successfully execute missions directed by our commanders for the good of our country and the American people.

This program shall be administered by the Information Warfare Officer (IWO), who reports to the Ship’s Navigator. The ship’s Captain, Squadron Intelligence Officer, and Squadron Communications Officer will serve as an advisory board for this program.

## 1. Engagement and Training Strategies

A Ship’s crew is a unique melting pot. Men, and increasingly women, from all walks of life, socioeconomic backgrounds, professional training pipelines, and a broad generational spectrum are expected to coalesce into a tightly knit team who live together in a sealed steel tube, and perform high consequence missions contributing to national security with little outside support or oversight. Militarization training during entrance into the military and initial professional training pipelines aids this necessary team building. Nonetheless, this melting pot of personalities and backgrounds presents a significant challenge to a comprehensive and effective training program on a highly technical and transparent topic like security awareness.

Recognizing these challenges, this next section of USS Ship’s SAP will name the specific difficulties we anticipate, discuss strategies to address them, and layout a program for accomplishment and sustainment.

### a. Overall Engagement Strategy

*Analysis of Ship Culture*

While each Ship has its own unique culture, there is a fluidity to that culture thanks to the regularly scheduled shift the crew experiences with each new Captain. To account for these rolling cultural shifts at a specific Ship command, this analysis will focus on the overall US Navy Ship culture as it will be the most representative of what the newest crew member arriving from initial accession training will come to know or what the saltiest Chief Petty Officer arriving for his last tour before retirement will expect.

A critical demarcation to be addressed is the major shift in Navy culture underway right now. Around the early 2000s, the Navy committed to initiatives modeled after corporate culture to move away from the historical perception of rough seafarers and toward the image of a professional fighting force. As sailors from both eras continue to serve, this program must account for the older generation of sailors with respect for authoritarian leadership based on orders and command presence contrasted against the newer generation with motivation based on understanding the “why” behind carrying out their duties. To address this aspect of our culture, we will seek a happy medium between providing clear, concise directives from a figure of authority while offering to expound on the “why” for those who need more understanding to buy-in.

Ship culture is summarized by a strong sense of patriotism, respect for duty, grit, ingenuity, and the use of procedures; combined with a healthy dose of sarcasm, edgy humor, and competition. These will all be leveraged in our awareness program to ensure our message is not lost on those who might otherwise chalk up security awareness to the realm of the nerds.

Like any bureaucratic system, there is a need to address the fact that any new program is quickly relegated to the ranks of an additional administrative burden if it is not framed correctly from the start. When introducing our program to the crew, and newly reporting crew members, comprehensive initial training with command leadership involvement will be required to raise the program’s importance out of bureaucratic noise to one critical for our mission success. Persistent command leadership involvement will also be necessary to ensure continued respect for, and attention to, the program’s message.

*Branding*

Given the limited space and unique constraints of the Ship environment as a daily workplace, branding will have to be creative and fluid. Nonetheless, a consistent branding strategy will tie the program’s success to the defeat of a common enemy. Given USS Ship’s normal operating area, the totalitarian government of Rubek is the most recognizable adversary for the crew, both at sea and in cyberspace. Our program will capitalize on tying mission success and a sailor’s success in cyberspace to the defeat of a common adversary.

Additionally, our program will use a strong tie to patriotism since, in the absence of open conflict, the use of an enemy could seem contrived.

*Messaging Why Security Matters*

Three broad categories are used to focus this section: crew readiness, ship readiness, and mission security.

Crew Readiness: As technicians in an extremely demanding environment aboard what has been called the most complex machine on earth, our sailors must be ready to perform at their very best. Nonetheless, cyber threats continue to proliferate worldwide, affecting our sailors at work and home. By training our sailors in the best cybersecurity practices, we can mitigate one of many vectors that threaten maximal crew performance and resiliency. We aim to maximize their ability to recognize and counter possible cyber-attacks that could affect their home life, financial stability, or sense of security, any of which could lead to a reduced ability to perform their duties at work. The message for our sailors will be promoting the stability and the security of their home life.

Ship Readiness: Our networks are well isolated, tightly secured systems thanks to the Department of Defense (DoD) and multiple civilian contractors. These defenses operate in concert with our embarked team of IT technicians, local monitoring tools, and comprehensive procedures. However, the best technologies and equipment are for naught if our sailors represent an untrained and, therefore, unmitigated threat vector. As demonstrated by the STUXNET virus attack, air-gapped, carefully secured control systems are no match for an opportunistic attack coupled with only one vulnerable user. Similarly, we must protect ship readiness by ensuring our sailors will not serve as the conduit for compromising our systems. The message for our sailors will be one of protecting our ship and our home at sea.

Mission Security: Our sailors, by association with the Ship warfare community, represent a valuable target for foreign state actors. Training our crew to be aware of operational security risks represented by sharing information outside of work is critical to our mission success and readiness. Our sailors must understand the process by which online platforms and communities can be leveraged, through open-source intelligence (OSINT) techniques, to aggregate fragmented, seemingly insignificant pieces of information into a comprehensive and compromising data set. Further, our sailors must identify and report experiencing any attacks to enable our counter-intelligence mechanisms to take effect. Our message to sailors will be to keep our mission and, by association, ourselves safe when at sea. Our ultimate goal is to return home safely to our families and loved ones.

### b. Primary Training Strategy

Two types of primary training are utilized: Annual refresher training as dictated and provided by the DoD and initial training for newly reporting sailors.

USS Ship falls under US Navy General Military Training (GMT) requirements, which, in part, direct computer-based training (CBT) modules with the titles “Cyber Awareness” and “Counter Intelligence Awareness and Reporting.” These training modules are required on an annual basis and are recorded and reported to Squadron and Type Commanders through the Navy’s learning management system. These two training modules are updated yearly and will serve as the basis for our local SAP. While highly informative and well-produced, these training modules are generic to the Navy as a whole and do not address specific threats and considerations unique to the Ship warfare community. This issue of specificity will be discussed in the sustainment training section. The ship’s GMT coordinator will ensure the command complies with the annual requirements to ensure this foundational part of our awareness program is in place.

When a sailor reports aboard USS Ship for the first time, their only exposure to security awareness training is assumed to be the annual GMTs. If they are fresh from the accession and training pipeline, GMTs may be the only exposure to security awareness ever. If they have served on previous ships or at other commands, they may have more experience, but they may also have behaviors or ideas about security awareness to be unlearned or refined. During the check-in process, a new crewmember will participate in one-on-one discussions with the IWO, an IT division representative, and, finally, the Navigator. These discussions will include a PowerPoint presentation to standardize the process and ensure all topics are covered. The focus of this initialization training will be for the IWO to establish the “why” for the program and how even a single individual’s behaviors are critical for our success. The IT division representative will primarily focus on the “how” and “what,” discussing the processes and tools available to the sailor aboard USS Ship to report security issues. The Navigator will establish command leadership involvement in the program and promote the vision for how USS Ship does security awareness to include why we are different than what the sailor has likely experienced at previous commands.

### c. Sustainment Training Strategy

USS Ship’s SAP establishes a training regimen built around a monthly cycle to keep security awareness current in our sailors’ minds. Topics will cycle through a predefined list of key behaviors and knowledge requirements reviewed and approved by the advisory board. Local training modules will reinforce the GMT modules and build on them by discussing unique considerations for the Ship force and threats unique to Ships in our operating areas. Seasonal topics will be incorporated during tax season or holiday seasons when social engineering risk is higher. Incidental topics will also be included based on publicly reported breaches or compromises.

Modalities will be as follows:

Weekly Plan of the Day (POD) Notes – Produced daily and posted throughout the ship, every sailor aboard consults the POD multiple times a day. Short factoids, reminders, or updates will be included on the POD to keep security awareness visible day-to-day. These POD notes will be no more than 3-5 sentences of content due to space constraints.

Posters or Infographics in congregation areas – About the ship are several bulletin boards to disseminate information to the crew. Every two weeks, the security team will place a new informational poster or infographic at these locations. These materials will be sourced from outside our local command.

Monthly Newsletter – A short one-page newsletter will be emailed monthly to the crew with security awareness information and updates. These will tie together the POW notes and posters for that month while expanding on the information presented and providing a look ahead for the next month’s topics.

Quarterly training with the Navigator or Captain – To continue establishing command involvement in the SAP, we will produce an all-hands training session given by command leadership to the crew once every three months. This training will focus on the message of “why security matters” and then provide a refresher on selected behavioral topics aligned with the predefined list of topics previously discussed.

## 2. Metrics

To measure and trend our SAP’s effectiveness, we will select three metrics representing USS Ship’s behavioral goals. These metrics will be evaluated and revised on an annual basis when indications point to a goal having been accomplished or if a metric is not providing actionable data. These metrics are not intended to be compliance-focused. Compliance Objective Quality Evidence (OQE) will be recorded, tracked, and reported through the Ship’s IT audit program. The metrics established in this program will emphasize behavior change and best practices for our crew members.

### a. Metric I – Phishing Recognition and Reporting

Due to the unique nature of our commonly used onboard networks being air-gapped and not connected to the public internet, our phishing program will focus on crew member’s personal email addresses, which are registered with the ship’s office for crew recall and communications when sailors are off duty. Our phishing program will seek to recreate targeted attacks based on association with the military in general or regional location to maximize the program's positive training value on our crew’s personal lives while emphasizing the types of attacks they or their families may encounter in day-to-day life. This metric is mapped to our Crew Readiness Message.

Our Phishing campaigns will include all crew members, including command level leadership. Phishing emails will incorporate elements from past training modules to measure training effectiveness, retention, and provide content reinforcement. Click-through, non-reporting without click-through, and reporting will be the outcomes tracked and trended. Phishing campaigns will be conducted every other month.

### b. Metric II – Unauthorized External Media Use and Reporting

External media, USB media, in particular, represents an especially concerning threat vector to USS Ship’s systems. USB media is generally not allowed aboard except for limited IT Division use in carrying out their work or when the ship is at sea to facilitate personal entertainment during off-watch periods. Our external media program will evaluate crew member response to finding a suspect USB device. This metric is mapped to our Ship Readiness Message.

The IT team will purchase and prepare several different USB storage or media devices specifically for SAP use. These devices will be left in public areas along thoroughfares to/from the ship’s pier or left about the ship. Outcomes measured will be reporting the discovery of a suspect device, non-reporting discovery of a suspect device, and unauthorized connection of a device to the ship’s networks. USB device drops will occur monthly to coincide with external device connection log audits of the same periodicity.

### c. Metric III – Information Sharing Sensitivity

In our age of connectedness, information sharing, and social media, the Ship community represents a bastion of the pre-internet age demanding that our sailors limit information sharing. This can lead to a clash between our sailor’s personal and professional lives. No time is this more the case than when the ship is preparing to get underway. Out of a desire to communicate to friends and family on social media that they may not be available for some time, our sailors could inadvertently generate OSINT, and the cumulative effect of multiple sailors doing the same could lead to compromises in mission security. This metric is tied to the message of the same name.

To evaluate this metric, official command sponsored social media accounts will be used to identify sailors and their family members on social media. During the weeks preceding getting underway, these accounts will be checked for publicly available messages or posts that could allude to mission details and represent publicly available OSINT. Instances of inappropriate information sharing will be tracked and trended. Periodicity for this metric will depend on the ship’s schedule.