|  |  |
| --- | --- |
| From: e-NAV Committee, vice chair | PAP26-8.1.3 |
| To: PAP | 22 October 2013 |
|  |  |

Draft IALA Briefing Note

**AIS Vulnerability**

# Summary

## Purpose

The accompanying draft briefing note is intended for discussion at PAP and possible distribution to IALA Members. It draws attention to recent publicity concerning the vulnerability of AIS to spoofing and other interference and sets out the risks and the precautions that should be taken by those administrations using AIS information and providing AIS services.

## Background

Research results have been published recently showing that AIS information can be spoofed, that is false information can be presented, including the names and other details of vessels, their position and status:

<http://blog.trendmicro.com/trendlabs-security-intelligence/vulnerabiliesties-discovered-in-global-vessel-tracking-systems/>

Further discussion, including an IMO response, can be found on:

<http://www.technologyreview.com/news/520421/ship-tracking-hack-makes-t>ankers-vanish-from-view/

These vulnerabilities have, in fact, been well-known since the early days of AIS, but this publicity may result in IALA Members facing questions. The attached briefing note is intended to assist in answering these questions.

# 2 ACTION REQUESTED

The Policy Advisory Panel is invited to consider this draft briefing note for distribution to IALA Members.

**Draft IALA Briefing Note – AIS Vulnerability**

**Introduction**

Research results have been published recently showing that AIS information can be spoofed, that is false information can be presented, including the names and other details of vessels, their position and status:

<http://blog.trendmicro.com/trendlabs-security-intelligence/vulnerabiliesties-discovered-in-global-vessel-tracking-systems/>

Further discussion, including an IMO response, can be found on:

<http://www.technologyreview.com/news/520421/ship-tracking-hack-makes-t>ankers-vanish-from-view/

These vulnerabilities have, in fact, been well-known since the early days of AIS, but this publicity may result in IALA Members facing questions. The attached briefing note is intended to assist in answering those questions.

**About AIS**

The Automatic Identification System (AIS) is an internationally standardised, VHF Broadcast system providing identity, position and status of ships. Carriage of Class A AIS units is required for SOLAS Convention vessels. Class B equipment is now carried voluntarily on many non-SOLAS vessels, including leisure and fishing craft and service vessels. AIS is also used to provided Aids to Navigation (AtoN) on fixed and floating platforms. The position of vessels and floating AtoN is generally provided by GPS, although other electronic position fixing systems (EPFS) can be used.

**Nature of Vulnerabilities**

It should be noted that AIS was originally provided for safety reasons, not for security purposes, so it was never designed to be resistant to malicious interference.

Previous studies have identified the following potential causes of failure:

* Incorrect data input to AIS unit
* Disruption to GNSS (GPS)
* Failure of AIS unit
* Degradation of VHF propagation
* Loss of VHF reception
* Control system malfunction

The first two of these causes can be brought about by deliberate broadcast of false information, including manipulation of GPS, so-called spoofing, for example a false position or identity can be broadcast. In common with other navigation and communications systems, AIS should not be relied upon as the sole source of information.

**Precautions**

Administrations providing services via AIS, such as AIS AtoN, or using AIS data for analysis purposes should be aware of these vulnerabilities and should consider taking the following precautions:

* All AIS information should be verified by some other means, for example radar or VHF DF
* Any apparently false or anomalous signals should be investigated by cross-checking with other AIS receiving stations and displays
* The integrity of broadcast information, especially AIS AtoN, should be monitored to ensure that identity, position and status are correct
* The integrity of GPS (or other EPFS) should be monitored, for example by Differential GPS
* Equipment used to broadcast AIS signals, such as base stations, should be located in secure premises and unauthorised access should not be possible
* AIS monitoring provided via the internet should only be used if access is provided by secure systems (e.g. firewall protected)
* Local Navigation Warnings should be broadcast if false AIS signals are being broadcast

**Conclusions**

* AIS does not have inherent integrity or authentication
* It is possible to broadcast false information via AIS
* AIS should not be used as a sole source of information
* Other means should be used to verify AIS information
* Integrity of AIS information should be monitored.