FOR IMMEDIATE RELEASE
2 November 2018

New WhiteHawk 360 Cyber Risk Framework Contract with U.S. Government
For Real-Time Vendor Cyber Risk Management

Highlights

- **This tailored version of the 360 Cyber Risk Framework provides BitSight cyber risk ratings, continuous monitoring, cyber risk alerts and WhiteHawk risk mitigation analytics, AI Risk Profile, and matching to vendor options in real-time to U.S. Government to provide continuous insight across hundreds of vendors at once.**
- **Recent U.S. Government focus on the systemic risks posed by their IT and software supply chain vendors has been growing both at Department of Defense and Department of Homeland Security.**
- **This U.S. Government implementation has a deep focus on supply chain cyber risk analytics (WhiteHawk Scorecard), which can warn of and prevent the type of breach recently suffered by British Airways.**

Perth, WA and Alexandria, VA – WhiteHawk Limited (ASX:WHK) ("WhiteHawk or "the Company"), the first global online cyber security exchange enabling small-to-medium businesses to take smart action against cyber-crime, is pleased to announce that it has entered into a new contract to provide a tailored version of its 360 Cyber Risk Framework to departments within the U.S. Government to protect against supply chain intrusions.

Under the contract, the Company will be providing sensitive risk analytics and mitigation, providing needed added protections to a breadth of office and mission functions. The initial phase of the contract is commencing immediately, followed by customer evaluation and option for expansion. The quantum of this first phase of the direct contract is minimal (sub-US$100,000), Phase 2 expands the scope of the risk framework across the U.S. Government department, to include all vendors being monitored and serviced by the Company's Cybersecurity Exchange, where the Company can derive additional revenues from the sale of vendor's products purchased across the Exchange.

Supply chain cyber risks

Initial reporting of the September 6th British Airways breach of all customer personal and financial data inputted from 21 August to 5 September 2018 affecting over 380,000 customers credit and debit cards, appears to be the result of supply chain risk. As stated in the September 7th BBC article, "Prof Woodward points out that this is an increasing problem for websites that embed code from third-party suppliers - it's known as a supply chain attack. Third parties may supply code to run payment authorization, present ads or allow users to log into external services." It is the vetting of such software vendors and service providers, that the 360 Risk Framework is designed to address, in advance of a breach. British Airways could be fined up to Euro One Billion under new European Commission regulations where penalties for data breaches can be levied up to 4% of the company's

turnover. In addition, there is potential significant damage to customer relations and brand reputation.

WhiteHawk continues to promote tailored versions of this Framework to U.S. based Financial Institutions, Manufacturers (commercial & federal), U.S. Utilities, and Government and has a current pipeline of potential contracts at varying stages of negotiation to supply the 360 Cyber Risk Review and Mitigation automated approach.

This has positioned the Company to potentially close an additional four sales of the 360 Cyber Risk Framework in 2018 and first quarter 2019. The latest customer channel focus is on the 3,200+ power and water utilities across the United States (regional power associations, regulators, and larger private utilities) who are all searching for how to gain continuous insight into and to address their cyber related risks.

Importantly, this process drives companies that are in a Prime Company's supply chain to WhiteHawk's Cybersecurity Exchange, to mitigate key cyber risks in real-time. Some of the current pipeline companies have supply chains exceeding 5,000 companies.

Terry Roberts, Executive Chair of WhiteHawk, commented, "With this contract we continue to demonstrate that our Cyber Risk Frameworks are equally of impact and value across sectors. And now we are having these conversations and demonstrations with key U.S. government departments (Dept of Defence, Department of Homeland Security, the Intelligence Community) and Government Owned Utilities, who are highly targeted and in great need of an effective, affordable, and scalable cyber risk framework. Traditionally Supply Chain Company or Vendor Risk Management programs are focused primarily on financial and product/service risk checks by a large staff of personnel and business processes. I wanted an end to end approach that leverages best of breed open data sets and premier risk tradecraft, baked into AI driven algorithms and analytics – all displayed in an integrated dashboard. This way we can scale our risk insights across hundreds and even thousands of vendors and supply chain companies. In addition, we have integrated our WhiteHawk Cybersecurity Exchanges' ability to identify and mitigate all critical cyber related risks."

-ENDS-

For more information:

WhiteHawk media inquiries (USA)
LeighAnne Baxter
publicrelations@whitehawk.com
+1 833 942-9237

WhiteHawk investor inquiries
(AUS)
Kevin Kye
investors@whitehawk.com

About WhiteHawk

Launched in 2016, WhiteHawk began as a cyber risk advisory service with a vision to develop the first online self-service, cyber security exchange, simplifying how companies and organizations discover, decide, and purchase cyber security solutions that directly mitigate their key cyber business risks. Today, we help US companies to connect to content, solutions, and service providers through evolving our rich data and user experience. WhiteHawk is a cloud-based cyber security exchange platform that delivers virtual consultations, Artificial Intelligence Cyber Risk Profile's that immediately match SME customers to tailored 'solutions on demand. The platform enables customers to leverage their tailored Security Story to find affordable and impactful cyber tools, content, and relevant services through our algorithms and expertise, to better understand how to improve and stay ahead of today's cyber threats. The Platform enables companies to fill their needs on an ongoing basis with demonstrated cost and time savings. For more information, visit www.whitehawk.com.

Level 28 140 St George Tce Perth WA 6000
Tel : +61 8 6311 4636, Fax : +61 8 6311 4661
ABN: 97 620 459 823
www.whitehawk.com