



WHITEHAWK®

# Quarterly Activities Report

## September 2025

WhiteHawk Limited (ASX:WHK)

Quarterly Activities Report for the Period Ended:  
30 September 2025

For personal use only

## HIGHLIGHTS

**WHITEHAWK LIMITED (ASX: WHK OR “WHITEHAWK” OR “THE COMPANY”), THE FIRST GLOBAL ONLINE CYBER SECURITY EXCHANGE ENABLING BUSINESSES AND ORGANIZATIONS OF ALL SIZES TO TAKE SMART ACTION AGAINST CYBERCRIME VIA RISK, MATURITY, COMPLIANCE AND THREAT SOFTWARE AS A SERVICE ANNUAL SUBSCRIPTIONS AND VIRTUAL CONSULTS, IS PLEASED TO PROVIDE AN UPDATE ON ITS PROGRESS FOR THE FIRST QUARTER.**

- Invoiced US\$258K in the third quarter.
- US\$85K in receivables as of 30 September 2025.
- New U.S. University Cyber Research Program Contract.
- Australian University contract in process for an annual subscription for Cyber Analyst Platform as a Service in order to scale Cyber Experiential Internships, online graduate and under-graduate programs and research.
- Provided a sole source 90-day proposal to U.S. Office of the Secretary of Defense (“OSD”) across 600 Critical Infrastructure Entities for \$280K USD.
- After 5 years of being in process, the final U.S. Defense Federal Acquisition Regulation Supplement (DFARS) rule to implement the Cybersecurity Maturity Model Certification (CMMC) Program contractual requirements for all U.S. Defense Contractors goes into effect on Nov 10<sup>th</sup>, 2025. WhiteHawk can now sell directly and in partnership with Dun & Bradstreet our automated Path to CMMC Offering.
- Two current WHK clients require CMMC Compliance, and a new CMMC Client contract is being scoped.
- Responding to State of Maryland Department of Labor Cyber Clinics RFP for a 3-year contract not to exceed \$1M USD, to provide Higher Education Students with Experiential Learning, while providing services to State and Local Critical Infrastructure. Contract award January 2026 for a February 2026 contract commencement.
- Requested by State of Florida to partner on a State-Wide Cyber Resilience Program in two Phases. Phase 1 in 2025, to include 3 to 5 Florida Universities with annual subscriptions for WHK Cyber Analyst Platform as a Service. Phase 2 now being written into 2026 Bill to include all 29 Florida Cyber Academic Centers of Excellence to have annual subscriptions for 3 years starting in 2026, for WHK Cyber Analyst PaaS. Contract portion for WHK is \$2.2M USD a year.
- While this 10 Year Contract Vehicle remains active, GSA SCRIPTS BAA Contract Vehicle has released two Task Orders to date one was a Sole Source requirement and the second was out of scope for the Knexus Research - WHK Team.

For personal use only

Additional Task Orders at this time, remain delayed due to U.S. Fiscal Year Budget delays and Government Shutdown. Responded to quick turn Department of Navy Cyber-Supply Chain Risk Management Sources Sought on 24OCT25. Prior to the Government Shutdown, Team Knexus/WHK have been engaging with Federal Clients to scope and generate Supply Chain Risk Management Task Orders that can be released on GSA SCRIPTS BAA that have been shaped by our Team.

- Reviewing and responding to three current AU Government Cyber Services and Solution RFQ's for October and November 2025 with DoxAi and their AU Government Services Partner.

New AU Channel Partnerships responding to Australian Government RFP's and engaging with regional commercial clients.

- WHK Cyber Resilience Moonshot Update – By Region, Sector, City or University:
  - Channel Partners - with focus on State of Maryland, Ohio, Florida, Pennsylvania - both State Governments and Universities.
  - Channel Partner - with focus on U.S. Department of Defense Critical Infrastructure.
  - Channel Partners - with focus on 30 Australian Universities and Government Agencies with meetings in October in Canberra.

For personal use only

# UPDATES FOR THE QUARTER

## **Prime Cyber Services Contract with a Global Social Media Platform Company**

### **Contract Summary**

- Two-year contract 01/01/2025 – 31/12/2026 to provide Third Party Risk Management Services for Risk Monitoring, Cyber and Architecture SME services, and Platform integration services.

### **Progress for the Quarter**

- Provide services to process third-party onboarding onto monitoring platform.
- Perform monthly analytics across three third-party portfolios to identify and capture trends and performance

## **Cyber Risk Program contract with Cailabs U.S. Subsidiary**

### **Contract Summary**

- Cyber Risk Program renewed for second year. New subscription period 01/02/2025 – 31/01/2026.
- Provide continuous cyber risk monitoring with quarterly analysis, assessment, reporting, and review vulnerability findings and recommendations.
- New CMMC Level 1 Requirements.

### **Progress for the Quarter**

- Delivered on 3rd quarter's analysis and associated reports.
- Client reviewing additional CMMC services proposal as add-on to contract.

## **Cyber Risk Program contract with Georgetown University**

### **Contract Summary**

- Cyber Risk Program was renewed for the third year. New subscription period 01/04/2025 – 31/03/2026.
- Provide continuous cyber risk monitoring with quarterly analysis, assessment, reporting, and review vulnerability findings and recommendations for continuous improvement.
- New CMMC requirements under development.

### **Progress for the Quarter**

- Delivered 3rd quarter's analysis and associated reports

For personal use only

- Awaiting new Client Governance Lead to start position in October 2025. Continued conversations for additional Cyber Risk Radar for supply chain risk management expected in 4Q 2025.

### **Cyber Risk Radar with Major City in Southeastern US**

#### **Contract Summary**

- Annual Subscription kicked off in May 2025 to perform cyber and business risk assessments and vulnerability analysis for 40 entities.
- Contract has a Base Year and 2 Option Years.

#### **Progress for the Quarter**

- Delivering monthly cyber and business risk assessments reports for portfolio of 40 entities
- Received new Task Order for \$85K USD which is in process.

### **Cyber Risk Program and Radar with Global US Investment Firm**

#### **Contract Summary**

- Annual Subscription kicked off in June 2025 to perform cyber risk assessments and vulnerability analysis for 18 Company Subsidiaries.

#### **Progress for the Quarter**

- Continuing monthly analysis, delivery of reports, and reviews with client.

### **Cyber Risk Program with AU Technology and Data Sciences Company**

#### **Contract Summary**

- A 60-Day Subscription kicked off in July 2025 to perform cyber risk assessment and vulnerability analysis for one of its clients as part of their Managed Services offering.

#### **Progress for the Quarter**

- Performed monitoring, analysis, delivery of reports, and awaiting to debrief client on findings, recommendations, and next steps.

For personal use only

# OUTLOOK

**New WHK Automated Path to CMMC Sales Opportunity across an estimated market of 300,000+ U.S. Defense Contractors.** Started back in 2018 and then stalled:

*On September 10, 2025, the Department of Defense (DoD) issued the anticipated final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to implement the Cybersecurity Maturity Model Certification (CMMC) Program contractual requirements for U.S. defense contractors. The final rule is effective November 10, 2025.*

*Background: The CMMC Program requires defense prime contractors and subcontractors to (i) implement security safeguards for any contractor information systems that process, store or transmit Federal Contract Information (FCI) and Controlled Unclassified Information (CUI), as well as (ii) maintain such safeguards throughout contract performance. Prime contractors are required to flow down CMMC requirements to all subcontractors and suppliers that will process, store or transmit FCI or CUI on their own information systems in performance of the subcontract. Note further that subcontracts for commercial off-the-shelf items (COTS) remain excluded from the flowdown requirement. Note that, for Level 1, only final status is permitted at the time of award and no conditional status is allowed.*

**WHK established an Automated Path to CMMC Level 1 back in 2019 and has been awaiting the finalization of the Rule. Nothing drives Cyber Risk, Security and Resilience sales like a definitive Regulation, where a Company cannot be awarded a U.S. DOD Contract without Compliance. Within 48 Hours WHK provides a comprehensive CMMC 2.0 Level 1 Baseline and prioritized Action Plan for Compliance**

**WHITEHAWK  
Client Portal**

Action Plan AU-E8 CIS v8 CMMC 2.0 GDPR NIST 800-171 NIST 800-53 R5

### Cybersecurity Maturity Model Certification 2.0

The Cybersecurity Maturity Model Certification (CMMC) is a standard for implementing cybersecurity in the Defense Industrial Base (DIB) aimed at measuring the maturity of an organization's cybersecurity processes toward enhancing the protection of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). The CMMC framework was developed in cooperation between the United States Department of Defense (DOD), DOD stakeholders, University Affiliated Research Centers (UARCs) Federally Funded Research and Development Centers (FFRDCs), and the Defense Industrial Base (DIB) sector.

Area	# Controls (24)	Level	Control Code	Description	Completeness
Access Control	2	L3	ACL3-3.1.2E	Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.	OVERALL: 0%
		L3	ACL3-3.1.3E	Employ secure information transfer solutions to control information flo...	N/A
Awareness and Training	2	L3	AT.L3-3.2.1E	Provide awareness training upon initial hire, following a significant cyb...	OVERALL: 0%
		L3	AT.L3-3.2.2E	Include practical exercises in awareness training for all users, tailored...	N/A
Security	1				OVERALL: 0%

For personal use only

For personal use only

mobility, outsourcing, Work-from-Home, and changing attacker tactics prompted the update and supports an enterprise's security as they move to both fully cloud and hybrid environments.

**CMMC 2.0**

The Cybersecurity Maturity Model Certification (CMMC) is a standard for implementing cybersecurity in the Defense Industrial Base (DIB) aimed at measuring the maturity of an organization's cybersecurity processes toward enhancing the protection of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). The CMMC framework was developed in cooperation between the United States Department of Defense (DOD), DOD stakeholders, University Affiliated Research Centers (UARC)s Federally



**NIST 800-171**

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

**Essential Eight**

The Australian Signals Directorate (ASD) has developed prioritised mitigation strategies, in the form of the Strategies to mitigate cybersecurity incidents, to help organisations protect themselves against various cyberthreats. The most effective of these mitigation strategies are the Essential Eight. The Essential Eight has been designed to protect organisations' internet-connected information technology networks. While the principles behind the Essential Eight may be applied to enterprise mobility and operational technology



## CASHFLOW

- Revenue receipts for the Quarter was US\$335K
- WhiteHawk continues to manage expenses below planned budget, expending US\$272K on average per month in total operating expenses over the last quarter.
- Group incurred net cash outflows from operations in the Quarter of US\$406K.
- Payments of US\$210K made to related parties include salaries; director fees and payments made for services provided by Key Management Personnel.

For personal use only

## DISCLOSURE STATEMENT

The Quarterly Activities Report is given in summary form and does not purport to be complete. The Quarterly Activities Report, including financial information, should not be considered as a financial projection, advice, or a recommendation to any particular or potential investors in relation to subscribing to securities in WhiteHawk. Before acting on any information, readers should consider the appropriateness of the information having regard to these matters, any relevant offer document and in particular, readers should seek independent financial advice. All securities involve risks, which include (among others) the risk of adverse or unanticipated market, financial or political developments and, in international transactions, currency risk. The Quarterly Activities Report may include statements regarding the Company's intent, belief, or current expectations with respect to our businesses and operations, market conditions, revenues, market penetration, and results of operations. Readers are cautioned not to place undue reliance on these statements. WhiteHawk does not undertake any obligation to publicly release the result of any revisions to these statements to reflect events or circumstances after the date hereof to reflect the occurrence of unanticipated events. While due care has been used in the preparation of the Quarterly Activities Report, actual results may vary in a materially positive or negative manner and are subject to uncertainty and contingencies outside WhiteHawk's control.

---

*The Appendix 4C Quarterly Cash Flow Report for the Period Ended  
30 September 2025 follows.*

---

For personal use only



## Appendix 4C

### Quarterly cash flow report for entities subject to Listing Rule 4.7B

**Name of entity**

WhiteHawk Limited

**ABN**

97 620 459 823

**Quarter ended ("current quarter")**

30 September 2025

<b>Consolidated statement of cash flows</b>		<b>Current quarter \$US'000</b>	<b>Year to date (9 months) \$US'000</b>
<b>1.</b>	<b>Cash flows from operating activities</b>		
1.1	Receipts from customers	335	1,099
1.2	Payments for		
	(a) research and development	(143)	(450)
	(b) product manufacturing and operating costs	(73)	(289)
	(c) advertising and marketing	-	(20)
	(d) leased assets	(62)	(132)
	(e) staff costs	(237)	(799)
	(f) administration and corporate costs	(228)	(621)
1.3	Dividends received (see note 3)	-	-
1.4	Interest received	2	8
1.5	Interest and other costs of finance paid	-	-
1.6	Income taxes paid	-	-
1.7	Government grants and tax incentives	-	-
1.8	Other (provide details if material)	-	-
<b>1.9</b>	<b>Net cash from / (used in) operating activities</b>	<b>(406)</b>	<b>(1,204)</b>
<b>2.</b>	<b>Cash flows from investing activities</b>		
2.1	Payments to acquire or for:		
	(a) entities	-	-
	(b) businesses	-	-
	(c) property, plant and equipment	-	-
	(d) investments	-	-
	(e) intellectual property	-	-
	(f) other non-current assets	-	-

For personal use only

Consolidated statement of cash flows		Current quarter \$US'000	Year to date (9 months) \$US'000
2.2	Proceeds from disposal of:		
	(a) entities	-	-
	(b) businesses	-	-
	(c) property, plant and equipment	-	-
	(d) investments	-	-
	(e) intellectual property	-	-
	(f) other non-current assets	-	-
2.3	Cash flows from loans to other entities	-	-
2.4	Dividends received (see note 3)	-	-
2.5	Other (provide details if material)	-	-
<b>2.6</b>	<b>Net cash from / (used in) investing activities</b>	<b>-</b>	<b>-</b>
<b>3.</b>	<b>Cash flows from financing activities</b>		
3.1	Proceeds from issues of equity securities (excluding convertible debt securities)	1,167	1,502
3.2	Proceeds from issue of convertible debt securities	-	-
3.3	Proceeds from exercise of options	-	18
3.4	Transaction costs related to issues of equity securities or convertible debt securities	(79)	(100)
3.5	Proceeds from borrowings	-	-
3.6	Repayment of borrowings	-	(358)
3.7	Transaction costs related to loans and borrowings	-	-
3.8	Dividends paid	-	-
3.9	Other (Payment by Lind for Initial Shares)	-	60
<b>3.10</b>	<b>Net cash from / (used in) financing activities</b>	<b>1,088</b>	<b>1,122</b>
<b>4.</b>	<b>Net increase / (decrease) in cash and cash equivalents for the period</b>		
4.1	Cash and cash equivalents at beginning of period	313	1,074
4.2	Net cash from / (used in) operating activities (item 1.9 above)	(406)	(1,204)
4.3	Net cash from / (used in) investing activities (item 2.6 above)	-	-

Consolidated statement of cash flows		Current quarter \$US'000	Year to date (9 months) \$US'000
4.4	Net cash from / (used in) financing activities (item 3.10 above)	1,088	1,122
4.5	Effect of movement in exchange rates on cash held	-	3
<b>4.6</b>	<b>Cash and cash equivalents at end of period</b>	<b>995</b>	<b>995</b>

5.	Reconciliation of cash and cash equivalents at the end of the quarter (as shown in the consolidated statement of cash flows) to the related items in the accounts	Current quarter \$US'000	Previous quarter \$US'000
5.1	Bank balances	995	69
5.2	Call deposits	-	191
5.3	Bank overdrafts	-	-
5.4	Other (provide details)	-	53
<b>5.5</b>	<b>Cash and cash equivalents at end of quarter (should equal item 4.6 above)</b>	<b>995</b>	<b>313</b>

6.	Payments to related parties of the entity and their associates	Current quarter \$US'000
6.1	Aggregate amount of payments to related parties and their associates included in item 1	33
6.2	Aggregate amount of payments to related parties and their associates included in item 2	202

*Note: if any amounts are shown in items 6.1 or 6.2, your quarterly activity report must include a description of, and an explanation for, such payments.*

7. <b>Financing facilities</b>	<b>Total facility amount at quarter end \$US'000</b>	<b>Amount drawn at quarter end \$US'000</b>
<i>Note: the term "facility" includes all forms of financing arrangements available to the entity. Add notes as necessary for an understanding of the sources of finance available to the entity.</i>		
7.1 Loan facilities	-	-
7.2 Credit standby arrangements <sup>(i)</sup>	100	-
7.3 Other (please specify)	-	-
7.4 <b>Total financing facilities</b>		
7.5 <b>Unused financing facilities available at quarter end</b>		100
7.6 Include in the box below a description of each facility above, including the lender, interest rate, maturity date and whether it is secured or unsecured. If any additional financing facilities have been entered into or are proposed to be entered into after quarter end, include a note providing details of those facilities as well.		
<u>Credit standby arrangements</u>		
(i) An unsecured Line of Credit standby arrangement provided by PNC Bank with a limit of US\$100,000. The facility is currently undrawn and does not have a fixed maturity date. The applicable interest rate is PRIME of 7.50% plus 2.95% at variable market interest rate. The rate fluctuates and is correct as at the date of preparation of this report.		

8. <b>Estimated cash available for future operating activities</b>	<b>\$US'000</b>
8.1 Net cash from / (used in) operating activities (item 1.9)	(406)
8.2 Cash and cash equivalents at quarter end (item 4.6)	995
8.3 Unused finance facilities available at quarter end (item 7.5)	100
8.4 Total available funding (item 8.2 + item 8.3)	1,095
8.5 <b>Estimated quarters of funding available (item 8.4 divided by item 8.1)</b>	2.70
<i>Note: if the entity has reported positive net operating cash flows in item 1.9, answer item 8.5 as "N/A". Otherwise, a figure for the estimated quarters of funding available must be included in item 8.5.</i>	
8.6 If item 8.5 is less than 2 quarters, please provide answers to the following questions:	
8.6.1 Does the entity expect that it will continue to have the current level of net operating cash flows for the time being and, if not, why not?	
Answer: N/A	
8.6.2 Has the entity taken any steps, or does it propose to take any steps, to raise further cash to fund its operations and, if so, what are those steps and how likely does it believe that they will be successful?	
Answer: N/A	
8.6.3 Does the entity expect to be able to continue its operations and to meet its business objectives and, if so, on what basis?	
Answer: N/A	
<i>Note: where item 8.5 is less than 2 quarters, all of questions 8.6.1, 8.6.2 and 8.6.3 above must be answered.</i>	

**Compliance statement**

- 1 This statement has been prepared in accordance with accounting standards and policies which comply with Listing Rule 19.11A.
- 2 This statement gives a true and fair view of the matters disclosed.

**31 October 2025**

Date: .....

**Terry Roberts**

Authorised by: .....  
(Name of body or officer authorising release – see note 4)

**Notes**

1. This quarterly cash flow report and the accompanying activity report provide a basis for informing the market about the entity's activities for the past quarter, how they have been financed and the effect this has had on its cash position. An entity that wishes to disclose additional information over and above the minimum required under the Listing Rules is encouraged to do so.
2. If this quarterly cash flow report has been prepared in accordance with Australian Accounting Standards, the definitions in, and provisions of, *AASB 107: Statement of Cash Flows* apply to this report. If this quarterly cash flow report has been prepared in accordance with other accounting standards agreed by ASX pursuant to Listing Rule 19.11A, the corresponding equivalent standard applies to this report.
3. Dividends received may be classified either as cash flows from operating activities or cash flows from investing activities, depending on the accounting policy of the entity.
4. If this report has been authorised for release to the market by your board of directors, you can insert here: "By the board". If it has been authorised for release to the market by a committee of your board of directors, you can insert here: "By the [name of board committee – eg Audit and Risk Committee]". If it has been authorised for release to the market by a disclosure committee, you can insert here: "By the Disclosure Committee".
5. If this report has been authorised for release to the market by your board of directors and you wish to hold yourself out as complying with recommendation 4.2 of the ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations*, the board should have received a declaration from its CEO and CFO that, in their opinion, the financial records of the entity have been properly maintained, that this report complies with the appropriate accounting standards and gives a true and fair view of the cash flows of the entity, and that their opinion has been formed on the basis of a sound system of risk management and internal control which is operating effectively.