NIIN
National Industry Innovation Network

Research Development
+ Innovation Program

Research, Development & Innovation (RD&I)

Impact Report 2026

Accelerating applied innovation in Australia

RESEARCH CHAIRS · INDUSTRY ALUMNI · SPECIALISED LABS

Contents

01 The RD&I Program 4

What it is, how it works and where the capability sits

02 National challenges 10

Health, critical infrastructure and defence, AI and cyber security, energy and sustainability

03 Case studies 19

Work that has left the laboratory and is now in use

04 Where to from here 26

Sovereign AI infrastructure, Cisco Research and new industry partners

Australia does not have a research quality deficit. It has a translation problem.

Our universities produce research of genuine international standing. Where we don't do as well is moving that work into hospitals, utilities, manufacturing plants and companies where value can be created for the economy and society.

Australia ranks last among OECD nations for industry–research collaboration. Readiness for artificial intelligence is improving: Cisco's AI Readiness Index found the share of Australian organisations fully ready to deploy AI rose from 4 per cent in 2024 to 22 per cent in 2025. But Australia still lags other nations in adopting it. Only 45% of the country's research and development workforce is employed in industry, against an OECD average of 68 per cent.

In 2026 the Australian Government released *Ambitious Australia*, the final report of its Strategic Examination of Research and Development. It called for greater investment, and for universities to collaborate with industry on priorities of national importance. It also gave the work a name that fits what we do: RD&I.

The reasons are structural rather than cultural. Australia relies on formal collaboration instruments that demand large upfront commitments and payback periods out of step with the way companies plan. A company with a problem and a modest budget has had nowhere obvious to take it.

Cisco established the National Industry Innovation Network in 2020 to work on exactly that gap. Six years on, the network spans ten Australian universities, has supported more than 350 industry projects and engaged more than 3,000 students. Few individual universities can convene industry at this scale. A national network can.

The RD&I Program is its applied research engine. In 2026 we brought the Research Chairs, the Industry Alumni and the Specialised Labs together under a single program with common governance, reporting and planning, so that every partner university can draw on the full capability of the network.

This report is the first time that work has been brought together in one place. The case studies show the model in practice: a system that gives nurses warning before a patient becomes violent, a private mobile network that keeps a container terminal running, an artificial intelligence that investigates cyber attacks on a live network, and an irrigation platform now sold across Australia.

An independent assessment puts the potential economic contribution of the network at around $380 million between 2026 and 2030. What follows is the evidence behind that number: the problems industry brought us, and what came back.

Emeritus Prof John Dewar AO
Chair, NIIN Advisory Council

Prof Ross Young
Chair, NIIN RD&I Program
Deputy Vice-Chancellor (Research and Innovation), University of the Sunshine Coast

01

The RD&I Program

Research Chairs, Industry Alumni and Specialised Labs — what they are, how a problem moves through them, and where the capability sits.

IN THIS SECTION

The National Industry Innovation Network 5
The three pillars of the RD&I Program 6
The RD&I model 7
The RD&I Program across Australia 8
The RD&I Program within the broader NIIN 9

The National Industry Innovation Network

Cisco started the NIIN in 2020 in response to stagnating productivity, slow digital adoption and the lowest rate of industry–research collaboration in the OECD. It has grown to become a major Australian industry-university collaboration network, bringing together ten Australian universities and a wide group of industry partners. It is industry-led, with Cisco co-funding the Research Chairs, supplying technology and investing in the Innovation Centrals. The network delivers through three initiatives, underpinned by two national alliances.

THREE INITIATIVES OF THE NIIN

Innovation Central Network

Facilities on university campuses where industry partners work alongside researchers and students to build, test and commercialise solutions. Six across Australia and one in Singapore.

THIS REPORT

The RD&I Program

The network's applied research engine: Research Chairs, Industry Alumni and Specialised Labs working on problems defined by industry. This report covers its work in 2026.

Skills + Talent Development

Programs that build the digital workforce the technology depends on, from the Cisco Networking Academy to micro-credentials and the AI Skills Challenge.

UNDERPINNED BY TWO NATIONAL ALLIANCES: CYBER + HEALTH

The alliances pool capability in two areas of national significance.

NIIN Health Alliance

Builds collective health innovation capacity and creates critical mass around shared health priorities.

NIIN Cyber Alliance

Accelerates cybersecurity research, innovation and education while providing support for national cybersecurity policy.

"If we are really focused on achieving great innovation in terms of the application of ideas, we need to have the problems and the partners in the room at the start."

Professor Alec Cameron Vice-Chancellor and President, RMIT University, in InnovationAus, August 2026

innovationaus.com/australias-innovation-challenge-is-no-longer-diagnosis-its-delivery

The three RD&I Program pillars

As the NIIN has matured, the RD&I Program has grown into one national program: industry-led, backed by Cisco and built to scale.

Until 2026 the Research Chair program, Industry Alumni and Specialised Labs were separate. They now operate as one program, with shared governance, a single quarterly reporting template and a common plan. It responds directly to Ambitious Australia, the National AI Plan and Australia's long-standing under-performance in research commercialisation. Together they give a university the researcher, the translator and the room, which is what it takes to turn an industry problem into something that gets used.

THE RESEARCHER

Research Chairs

Senior academics appointed into partner universities to lead applied research in an area of national significance, funded jointly by Cisco and the university.

A Chair is chosen for industry depth as much as research record, and works on problems that matter to industry partners.

Chairs get early access to Cisco technology, and to frontier research the company has not yet brought to market.

Every project is scoped with an industry partner and supported by students and early-career researchers.

THE TRANSLATOR

Industry Alumni

Experienced former industry engineers and business leaders sitting inside partner universities, typically one to two days a week.

They operate as translators. They know how a company operates, how a project gets funded and what is needed from a prototype to de-risk adoption.

They mentor researchers and students, and increasingly teach, bringing current industry practice into the curriculum.

They link Chairs with Cisco teams, customers and industry partners, and clear blockages so the research keeps moving.

THE FACILITY

Specialised Labs

Labs and facilities at NIIN universities, equipped with Cisco and partner technology, where solutions are built, tested and demonstrated.

A place where a customer sees capability working rather than described, helping to turn a conversation into a workable solution.

They are technology-focused (e.g. in AI and IoT, future networks and private 5G), or industry-focused (e.g. in digital health).

The RD&I model

The RD&I program moves beyond traditional Research and Development (R&D) by focusing on Innovation and Development (I&D) – driving ideas from the lab into industry applications. This is a critical distinction: Research is focused on discovery and generating new knowledge, while Innovation responds directly to industry needs, shaping research towards practical applications.

	NIIN 'SWEET SPOT'	
Research	**Innovation**	**Development**
Discovery and knowledge generation, typically undertaken in universities	Problem-solving aligned to industry needs	Adoption in commercial offerings

EVERY PROJECT MOVES THROUGH THE SAME FOUR STEPS

01

An industry problem

A partner identifies a potential challenge to delivering effective business outcomes and commits a person to it.

02

Scoped and endorsed

A Research Chair and an Industry Alumnus turn it into a defined project, endorsed before work starts.

03

Built and tested

Prototyped in a Specialised Lab or Innovation Central, with students on the team.

04

Scaled / incubated

Trialled with the partner, then adopted, commercialised, or written into a standard.

UNDERPINNED BY

Co-investment

Industry, Cisco and the university all put something in.

Cisco technology

Including early sight of research not yet in market.

Ten universities

A problem can be answered by combining the best placed assets across the network.

Capability

Students and early-career researchers for analysis and prototyping.

Governance

Every project endorsed, then reviewed every quarter.

The RD&I Program across Australia

Six Research Chairs are in place, with further appointments in recruitment, each working alongside Industry Alumni and, at most universities, a Specialised Lab where the work is built, tested and shown.

IN RECRUITMENT

Sports Technology
Queensland University of Technology

Defence Capability and Security
Flinders University

AI Cyber Security
Adelaide University

AI in Health Systems
La Trobe University

Agentic AI
Curtin University

RESEARCH CHAIRS AND SPECIALISED LABS

A/Prof Alison Craswell
Digital Health and Ageing · University of the Sunshine Coast
UniSC Digital Health Productivity Lab

Prof Marius Portmann
Network Security · University of Queensland
UQ Centre for Future Networks

A/Prof Ilaria Barletta
Sustainable Engineering · University of Technology Sydney

Prof Frank den Hartog
Critical Infrastructure · University of Canberra
UC Private 5G Lab

Prof Wei Xiang
AI and IoT · La Trobe University
La Trobe Centre for AI and IoT

Prof Trish Williams
Digital Health · Flinders University
Flinders Digital Health Research Centre

RMIT University
Specialised Lab
RMIT Health Transformation Lab

THE PROGRAM IN NUMBERS

6
Research Chairs, with five more in recruitment

8
Specialised Labs established or in establishment

10
Industry Alumni appointed or committed

15+
Students and early-career researchers on project teams

The RD&I Program within the broader NIIN

The RD&I Program is one of three NIIN initiatives and works hand in hand with another, the Innovation Centrals, on university campuses across Australia and in Singapore. Each makes the other stronger, and both draw on the same infrastructure.

HOW THEY CONNECT

SHARED INFRASTRUCTURE

Specialised Labs
Equipped with Cisco and partner technology at NIIN universities

Innovation Central spaces
Hubs on university campuses across Australia and in Singapore

NIIN Sovereign AI Cloud
Australian-hosted AI computing for sensitive data and models

HOW THEY WORK TOGETHER

Bringing industry in

The Innovation Centrals are the NIIN's front door, working with many more companies than the Research Chairs could reach alone. When a problem needs more than a short project, it can become the brief for a Research Chair, drawing the partner into the RD&I Program.

Adding depth

The RD&I Program brings what a short project cannot: senior researchers, the experience of the Industry Alumni and early access to Cisco technology. What a Research Chair proves can then be taken to more companies through the Innovation Centrals.

Sharing infrastructure

Both draw on the same infrastructure, a significant investment in its own right. Research Chairs prototype with students in Innovation Centrals and Specialised Labs, and both use the Sovereign AI Cloud for sensitive data.

BUILDING ON EACH OTHER

Over time the two strengthen each other. An Innovation Central's industry partners can create the demand that justifies a Research Chair, and a Research Chair's work can create the depth and relationships an Innovation Central needs to grow.

02

National challenges

The areas of national importance the program works in, the capability the network brings to each, and the problems being solved.

IN THIS SECTION	NATIONAL INNOVATION PILLAR	
Health	Health and medical	11
Critical Infrastructure and Defence	Defence; Resources	13
AI, Networks and Cyber Security	Technology; Agriculture and food	15
Energy and Sustainability	Environment and energy	17

National Innovation Pillars as proposed in Ambitious Australia, the final report of the Strategic Examination of Research and Development.

Health

Health represents our most significant expenditure. An ageing population, workforce shortages and rising aggression towards clinical staff are colliding with health systems that were not designed to share data or automate routine work. The prize is productivity, safety and access to care, and it is largest in regional and aged care settings.

RESEARCH CHAIRS

A/Prof Alison Craswell

Digital Health and Ageing, University of the Sunshine Coast

A nurse researcher who works closely with local Health Services and providers of aged care on the problems their own staff raise.

Prof Trish Williams

Digital Health, Flinders University

A leading researcher in health system security and digital maturity, whose assessment frameworks have been taken up in international standards.

In recruitment

AI in Health Systems, La Trobe University

Will focus on where AI can safely take work off a stretched clinical workforce.

SPECIALISED LABS

UniSC Digital Health Productivity Lab

Machine vision, sensor technology and workflow, used to host clinicians, organisational partners, Cisco customers and students.

Flinders Digital Health Research Centre

Computational solutions for managing health across clinical, workplace and home settings.

RMIT Health Transformation Lab

Design, systems thinking and technology applied to care delivery. Leads the Health Alliance's annual Health x Digital Transformation Report.

INDUSTRY & GOVERNMENT PARTNERS

Cisco · Sunshine Coast Hospital and Health Service · Queensland Government, Queensland Health · Government of South Australia, SA Health · Grampians Health · comlink Australia

Impact the work has created

01

A clinical Wi-Fi framework written into an international standard

In a hospital a dropped connection can mean a missed alarm, and there was no agreed basis for specifying wireless where that matters. The framework Flinders built for Wi-Fi 7 in clinical settings is now part of ISO/CD 81001-4-1, so it becomes the reference every manufacturer and health service designs to.

02

365 health workers upskilled in a single pilot

RMIT, Grampians Health and the Cisco Networking Academy built five short courses for IT and clinical staff in a regional health service. 365 people completed them and 86 per cent reported high satisfaction. It is now the network's model for lifting digital skills in services that cannot release staff for long training.

03

Nurses given warning before a patient becomes violent

Aggression towards staff on dementia and delirium wards is common, and privacy rules keep cameras out of patient areas. A system that reads agitation at the bedside without video leaving the ward is now a working proof of concept, demonstrated at Cisco Live Melbourne, with a point-of-care trial planned for 2027.

04

A white paper that put nurses' time back on the agenda

Working with frontline staff, the UniSC Chair mapped where automation can safely take routine work off nurses and, just as importantly, where it cannot. The white paper was published in September 2026 and launched at Innovation Central Brisbane with the clinicians who shaped it.

Critical Infrastructure and Defence

Australia's essential services are being digitised faster than they are being secured. Operational technology that was once isolated now connects to the internet, and obligations under the Security of Critical Infrastructure Act have tightened accordingly. Defence is the priority sector the network is now moving to address at scale, as sovereign capability requirements and overlapping security standards push Australian suppliers, most of them small companies, to lift their maturity quickly.

RESEARCH CHAIRS

Prof Frank den Hartog

Critical Infrastructure, University of Canberra

Works where operational technology meets the internet: the networks behind ports, utilities and defence suppliers. His research has gone to the Department of Home Affairs and to Telstra.

In recruitment

Defence Capability and Security, Flinders University

Will take the network into defence industry security in the state where much of Australia's defence manufacturing sits.

SPECIALISED LABS

University of Canberra Private 5G Lab

Standalone private 5G hardware with Cisco Unified Edge installed. Use cases are proven here before a customer has to commit to one, and student projects run on the same platform.

INDUSTRY & GOVERNMENT PARTNERS

Impact the work has created

01

Private 5G proven on a working container terminal

Cisco's private 5G offering was designed around the United States market, and Australian take-up had stalled below half its potential. The University of Canberra built and tested a standalone network across a live container terminal, showing a return well above ten to one. Cisco and IPTel Solutions now have an offering they did not have before, and a mining sector trial follows in 2027.

02

A whitepaper that went to Home Affairs

Commissioned by DroneShield, the work set out the cyber threat aerial drones pose to critical infrastructure and what operators should do about it. It went to the Department of Home Affairs, which is a long way from where most university research on the subject ends up.

03

A national resilience assessment for Telstra

Telstra asked how digital resilience is actually implemented across Australian critical infrastructure environments, as opposed to how it is specified. The assessment returned five recommendations and a picture of the gap between policy and practice.

04

One compliance map instead of three

An Australian defence supplier must satisfy DISP here, CMMC in the United States and the Essential Eight besides, which is a serious burden for a small company. With the Industry Capability Network, the three are being mapped into a single web tool a small business can actually use.

AI, Networks and Cyber Security

Australian organisations are getting ready for AI, but there is further to go: in Cisco's AI Readiness Index the share fully ready to deploy it rose from 4 per cent in 2024 to 22 per cent in 2025, yet Australia still lags other nations in adoption. Security alerts have long outrun the teams meant to triage them, and the computing power serious AI needs sits largely offshore, which becomes a hard constraint the moment the data cannot leave the country.

RESEARCH CHAIRS

Prof Marius Portmann

Securing Future Networks, University of Queensland

Builds and tests AI security systems on real networks rather than in simulation. His team's agentic AI investigator has run on UQ's production network for months.

Prof Wei Xiang

AI and IoT, La Trobe University

Takes AI and sensor technology into places that do not usually get them: cane farms, supermarket aisles, community health. His Specialised Lab produced the network's first commercial product.

In recruitment

AI Cyber Security, Adelaide University

Will anchor the network's AI security capability in South Australia.

SPECIALISED LABS

La Trobe Centre for AI and IoT

A first-of-its-kind Australian lab built around the combination of AI and connected devices, and the source of the network's first commercialised product.

UQ Centre for Future Networks

In establishment: a dedicated facility for secure, resilient and trusted networks, with space identified and an opening planned.

INDUSTRY & GOVERNMENT PARTNERS

Impact the work has created

01

Agentic AI running on a live production network

Plenty of research shows what agentic AI can do in a laboratory. FlowMind has run for months on the University of Queensland's own production network, investigating real activity and handing analysts an auditable account of what it found. That is the evidence a bank or a government department needs before it will consider the same step.

02

The network's first commercial product

An AI irrigation platform built by the Cisco–La Trobe Centre with Aglantis launched commercially in March 2025 and is now distributed nationally through two dealer networks. It runs on more than 15 farms covering up to 3,000 hectares, and it won the 2026 AFR AI Award for Sustainability.

03

A digital twin of a campus, and of a reef

With NVIDIA and Cisco, a physically accurate twin of La Trobe's Bundoora campus. With the Australian Institute of Marine Science, 3D models of the Great Barrier Reef built faster than photogrammetry allows. The same capability, pointed at an asset owner's problem and then at a national one.

04

Research funded from San Jose and run in Australia

Project INSPIRE, on integrated spatial perception and reasoning for robotics, is funded by Cisco Research in the United States and carried out here. It is the clearest sign that the network's research is being valued on its merits rather than as a local courtesy.

Energy and Sustainability

The energy transition is as much a data and systems problem as an engineering one. Manufacturers and asset owners are being asked to cut emissions and energy intensity without a reliable way of knowing which investment will actually pay back. At the same time the infrastructure the rest of this report depends on, data centres and AI compute, is becoming one of the fastest-growing sources of energy and water demand in the country.

RESEARCH CHAIR

A/Prof Ilaria Barletta

Sustainable Engineering, University of Technology Sydney

Ilaria works with businesses and governments to improve energy and resource performance of industrial sites, align market signals with intended outcomes, and navigate the interaction between technology, investment, energy markets and policy. Through the NIIN, she connects these challenges with complementary expertise across the network, including in emerging areas such as data centres and AI infrastructure.

In 2026, her contribution has focused on bringing together industry, research and policy perspectives while developing research on energy performance and the sustainability of emerging digital infrastructure.

SPECIALISED LABS

In planning

INDUSTRY & GOVERNMENT PARTNERS

Cisco · ceda · Centre for Environmental Governance

Impact the work has created

01

Exploring AI in environmental regulation

A/Prof Ilaria Barletta contributed to the CEDA roundtable *Unlocking AI and Data for Environmental Approvals* in April 2026, with a particular focus on regulatory sandboxes and the potential for AI to augment regulatory processes and regulatory technology, areas the NIIN is well placed to explore. Environmental approvals are one of the slowest parts of building anything in Australia, and this is the network's evidence entering that debate.

02

A seat at the table on data centres and the environment

A/Prof Ilaria Barletta was a speaker and panellist at the Centre for Environmental Governance in Canberra in September 2026, alongside CDC, TBH Consulting and the ACT Government. Data centre growth is becoming an important environmental policy question. In ongoing discussions around adaptive governance and social licence, the NIIN is bringing a perspective that balances the opportunities of digital infrastructure with its energy, resource and broader sustainability implications.

03

Case studies

Work that has left the laboratory and is now in use outside the university that built it.

IN THIS SECTION

Identifying potential issues early on a hospital ward 20
Helping universities understand gaps in their digital infrastructure 21
A private mobile network in settings where dropping out is not an option 22
AI that proactively searches for and investigates cyber attacks 23
Taking the guesswork out of watering a cane farm 24
A compliance map for skills held by suppliers to defence forces 25

CASE STUDY · HEALTH

Identifying potential issues early on a hospital ward

Cameras and sensors that recognise a patient becoming agitated, so nurses have information and time rather than only instinct.

THE PROBLEM

On wards, caring for people with dementia and delirium, aggression towards staff is common. Nurses are injured and some leave the profession altogether. Patients are restrained or sedated when a different approach, taken ten minutes earlier, might have settled things.

Privacy rules rightly keep cameras out of patient areas, so the one tool used everywhere else in the hospital is unavailable where it is most needed.

WHAT THE NIIN DID

The team built a system that processes everything at the bedside, so no video leaves the ward. It reads three things at once: changes in the patient's face that signal rising agitation, larger body movements, and biometric data from sensors.

Just as important, the team asked the staff first. Interviews with nurses, later widened to patients and families, shaped what the system does and what it does not.

WHAT HAS CHANGED

A working proof of concept was demonstrated at Cisco Live Melbourne 2026. It is built to provide evidence for the clinician to determine the best moment to intervene, and on whether a change in treatment is reducing a patient's agitation.

The clearest sign the health service values the work is that it has asked for more. Several follow-on projects are under way, and ethics approval is being sought for a point-of-care trial in 2027.

PROJECT AT A GLANCE

RESEARCH CHAIR	INDUSTRY PARTNERS	CORE TECHNOLOGY	STATUS
A/Prof Alison Craswell, University of the Sunshine Coast	Sunshine Coast Hospital and Health Service; Queensland Health	Cisco Meraki Cameras	Proof of concept complete; point-of-care trial planned for 2027

CASE STUDY · HEALTH

Helping universities understand gaps in their digital infrastructure

A maturity framework built for hospitals, rebuilt for universities, so an institution can see the state of its digital infrastructure before it spends on changing it.

THE PROBLEM

Every university is under pressure to digitise so it can deliver better service at a lower cost. Students expect high levels of digital experience, researchers depend more and more on computing, and cyber attacks are more common and more complex to counter.

For universities there are myriad potential projects to invest in, but the challenge is understanding how to prioritise areas of greatest risk. Readiness for AI has made this challenge even more acute.

WHAT THE NIIN DID

Professor Trish Williams had already solved a version of this problem elsewhere, in healthcare. The maturity model she co-developed for hospitals gave health services a structured way to judge where they stood. With Cisco, she rebuilt it for higher education as Campus Insight.

It assesses five areas that matter in practice, then places the institution on an eight-level scale. Each level is described by what staff and students actually experience, not only the technology installed.

WHAT HAS CHANGED

Campus Insight was completed in 2026 and published with Cisco Australia. It gives the sector a common language for digital maturity and a roadmap that ties investment to strategy rather than to the technology cycle. Cisco is working through how to take it to the wider market.

It is also a good illustration of how the network is meant to work: a framework built for one sector has moved into another, because the underlying problem was the same.

PROJECT AT A GLANCE

RESEARCH CHAIR
Prof Trish Williams, Flinders University

INDUSTRY PARTNER
Cisco Australia

PUBLISHED
Campus Insight: Digital Infrastructure Maturity Assessment for Higher Education
Adapted from the INFRAM hospital maturity model (Williams et al., 2019)

STATUS
Complete; commercial pathway under consideration with Cisco

CASE STUDY · CRITICAL INFRASTRUCTURE AND DEFENCE

A private mobile network in settings where dropping out is not an option

Standalone private 5G designed for Australian sites; proven first on a container terminal.

THE PROBLEM

A container terminal, a mine or a water utility needs coverage that does not fail. Public mobile networks are not necessarily built in or for those environments and Wi-Fi only covers some of the needs of a working site. Private 5G offers benefits but Australian take-up has reached less than half of what the market should support.

The reason is not the technology. Cisco's offering was designed around the United States market. For Australia the use cases and the proof that it pays back had to be developed here.

WHAT THE NIIN DID

The University of Canberra established a Private 5G Specialised Lab and used it to work through the problems a customer would actually encounter.

With Cisco and IPTel Solutions, the team stitched private 5G and Wi-Fi into one secure network across a container terminal. It tested whether Cisco's Unified Edge hardware could run several different 5G cores, which decides what a deployment costs. And it built the business case from market research.

WHAT HAS CHANGED

The work showed that a return well above ten to one is achievable for private 5G vendors here, which turns a technical conversation with a customer into a commercial one.

Cisco and IPTel now have an offering for container terminals that did not exist before. Other organisations have asked to join with use cases of their own. A mining trial follows in 2027, alongside a new partnership with the National University of Singapore.

"This partnership allows us to move beyond concept into deployment, leveraging cutting-edge research and industry expertise to deliver practical, scalable solutions in edge technologies."

Costa Athanassiou
Chief Operating Officer, IPTel Solutions

PROJECT AT A GLANCE

RESEARCH CHAIR	INDUSTRY PARTNERS	CORE TECHNOLOGY	STATUS
Prof Frank den Hartog, University of Canberra	Cisco; IPTel Solutions; BAI; CloudRAN.AI	Cisco Unified Edge; private 5G and Wi-Fi	In commercial use; mining sector trial in development for 2027

CASE STUDY · AI, NETWORKS AND CYBER SECURITY

AI that proactively searches for and investigates cyber attacks

FlowMind investigates suspicious activity on a network by itself, gathers the evidence, and hands a human analyst a clear account of what it found.

THE PROBLEM

Modern networks produce a high volume of activity; most of it is routine. Hidden in the traffic are indicators that an attack might have been launched. To date, network security teams have never had enough people to look at everything, so they triage, and triage means things get missed.

It is getting harder. Attackers have begun using autonomous AI agents of their own, so defenders who investigate at human speed are being probed at machine speed.

WHAT THE NIIN DID

Researchers at the University of Queensland, with Cisco's support, built FlowMind: an AI system that conducts the investigation itself. It decides what to look at, queries existing security tools, and produces an auditable account of what it found and why.

The design question that mattered most was control. FlowMind is secure by design: access to sensitive data is tightly constrained, every step is recorded, and humans keep the decisions that matter.

WHAT HAS CHANGED

FlowMind is not a demonstration. It is deployed on the University of Queensland's own production network and has run for months against real operational traffic.

Plenty of research shows what agentic AI can do in a laboratory. Very little shows what happens on a live network people depend on. That evidence is what a bank, a hospital or a government department needs before it will consider the same step.

"FlowMind implements a secure-by-design agentic AI for network security investigations. Months of testing on our production network have demonstrated its potential to detect anomalous activity and support our investigations."

David Gwynne
Infrastructure Architect, University of Queensland

PROJECT AT A GLANCE

RESEARCH CHAIR
Prof Marius Portmann, University of Queensland

INDUSTRY PARTNER
Cisco

CORE TECHNOLOGY
Open-weight large language models; Cisco Foundation-sec-8B; NVIDIA DGX Spark; NVIDIA GB300

STATUS
Operating; next phase, Bioagentic Network Defence, under development

CASE STUDY · AI, NETWORKS AND CYBER SECURITY

Taking the guesswork out of watering a cane farm

An AI irrigation platform, built in a university lab and now sold across Australia, that runs pumps and valves automatically and tells growers when and how much to water.

THE PROBLEM

On the cane farms in the Shire of Burdekin, irrigation is still largely done by hand. Aglantis estimates growers spend up to five hours a day switching pumps and chasing water, roughly 38 days a year.

About half the water that leaves the pump never reaches the crop, and over-watering carries fertiliser towards the Great Barrier Reef. Sensors have existed for years, but cost, software lock-in and patchy mobile coverage kept growers away.

WHAT THE NIIN DID

The Cisco–La Trobe Centre for AI and IoT and Aglantis built a system around what a grower already owns. At its centre is a solar-powered node designed at La Trobe that can run a pump, open a valve or monitor soil, and retrofits to existing equipment.

The nodes talk over long-range radio, which is what makes it work where mobile coverage does not. Above them sits an AI model of the farm that advises when to irrigate and how much.

WHAT HAS CHANGED

Built in a sandbox at La Trobe, installed on a Burdekin cane farm in late 2024 and launched commercially in March 2025, it is the first commercial product out of the Centre.

It now runs on more than 15 farms covering up to 3,000 hectares, with over 160 customers and national distribution through two dealer networks. On farm: about 20 per cent less water, electricity bills down by as much as half, and labour savings of 30 to 45 per cent.

"It essentially takes the guesswork out of farming. Farmers no longer need to wake at 2am to shut off the water or worry about losing valuable water to runoff. This system makes sustainability both practical and achievable."

Luke Malan
Managing Director, Aglantis

PROJECT AT A GLANCE

RESEARCH CHAIR
Prof Wei Xiang, La Trobe University

INDUSTRY PARTNERS
Aglantis (Ayr, Queensland); Cisco; more than 15 farms in the Lower Burdekin

CORE TECHNOLOGY
Solar-powered IoT nodes, long-range radio and an AI model of the farm

STATUS
Deployed on farms with strong outcomes: About 20% less water, electricity bills down up to 50%, labour savings of 30–45%

2026 AFR AI Awards, Sustainability category

CASE STUDY · CRITICAL INFRASTRUCTURE AND DEFENCE

A compliance map for skills held by suppliers to defence forces

A systematic comparison of the US and Australian defence cyber security programs, built into a web tool a small supplier can use.

THE PROBLEM

Any company that sells to the US military must hold the right level of Cybersecurity Maturity Model Certification (CMMC). That includes Australian companies. At home, the same company must meet the Defence Industry Security Program (DISP), and the Essential Eight besides.

The two programs look alike but are not the same. A supplier certified under one cannot easily tell what more the other requires, which is a serious burden for a small company, and most of Australia's defence suppliers are small companies.

WHAT THE NIIN DID

Under the guidance of the University of Canberra Research Chair, Masters research students undertook a systematic comparison of CMMC and DISP with the Australian Cyber Collaboration Centre. The two were first mapped against each other on paper.

The mapping was then extended to ISO 27001 and the Essential Eight, and built into a web-based tool, completed in February 2025. To extend the mapping also to the other standards suppliers already work to, including NIST 800-171/172, Common Criteria, and IRAP, the team is automating the mapping using knowledge graphs and modern Compliance Operations languages such as OSCAL and Catala.

WHAT HAS CHANGED

Australian suppliers now have one map across the standards they face, presented so a small business can navigate it rather than working through each standard on its own.

The mapping is being updated for the new DISP requirements, particularly the Essential Eight. The tool will then be tested with suppliers, likely through the Defence Trailblazer, before it is published and kept up to date.

PROJECT AT A GLANCE

RESEARCH CHAIR
Prof Frank den Hartog, University of Canberra

PARTNERS
Australian Cyber Collaboration Centre (Aus3C); Industry Capability Network; Cisco

STANDARDS MAPPED
CMMC; DISP; ISO 27001; Essential Eight. Being added: NIST 800-171/172; Common Criteria; IRAP

STATUS
Web tool built; being updated for new DISP requirements before testing with suppliers

04

Where to from here

The infrastructure the next phase depends on, the research partnership behind it, and a way in for the industry partners who come next.

IN THIS SECTION

The NIIN Sovereign AI Cloud 27
Working with Cisco Research 28
Bringing on more industry partners 29
The RD&I network 29

Running research workloads on the NIIN Sovereign AI Cloud

The computing power serious AI needs sits largely offshore, which becomes a hard constraint the moment the data cannot leave the country. The NIIN Sovereign AI Cloud is designed to be a shared, Australian-hosted AI cloud that gives the ten NIIN universities and their industry partners GPU compute, common tools and built-in governance, so sensitive research, data and the models trained on it stay under Australian control.

WHERE IT SITS

	THE GAP IT FILLS	
Supercomputers	**Sovereign AI Cloud**	**Commercial clouds**
Pawsey and NCI. Large batch jobs: submit the job, collect the results later.	Applied, always-on AI on sensitive data, kept under Australian control.	Real-time services at global scale. Costly when sustained, and not sovereign.

WHAT MAKES A GOOD SOVEREIGN AI WORKLOAD

01

Runs AI models
Training, fine-tuning or, most often, inference on the researcher's own data.

02

Always on, not batch
Continuous inference and agentic AI, which supercomputers and commercial clouds handle poorly.

03

Sovereign data
Health, defence, personal and confidential industry data that must stay in Australia.

THE FIRST RESEARCH WORKLOADS

Research Chairs and researchers across the network have nominated the first workloads through their Deputy Vice-Chancellors (Research). They run on the prototype at no cost to universities, and the cloud is being designed around them.

10 research workloads nominated and analysed

5 NIIN universities, plus wider NIIN activities

6 sectors, from health and cyber security to mining

4 forms of AI: training, fine-tuning, inference and agentic workflows

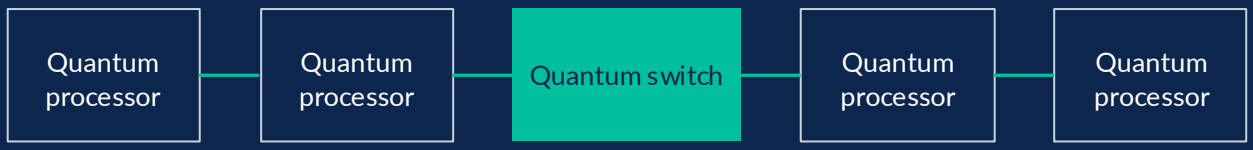
Working with Cisco Research

Cisco Research funds and collaborates with universities on technology that is still years from reaching the market. Many of its priorities, from agentic AI to advanced networking and quantum, are problems the Research Chairs already work on, on live networks and with industry partners at the table. Project INSPIRE, funded by Cisco Research and carried out in Australia, shows the connection works. Quantum is where it can go next.

QUANTUM NETWORKING AT CISCO RESEARCH

Linking small quantum computers into one larger one

Today's quantum processors are small. Rather than wait for one very large machine, Cisco Quantum Labs in Santa Monica is building the network that links many smaller ones into a single system, over the fibre already in the ground.



Entangled photons carried over standard telecom fibre

WHERE THE RESEARCH CHAIRS COME IN

Live networks to test on

The Chairs work on a university production network, a working container terminal and hospital systems. Quantum networking has to prove itself in exactly those conditions.

Security for critical infrastructure

Quantum computers will eventually break much of today's encryption. Chairs in network security and critical infrastructure work where quantum-safe protection will be needed first.

Close to Australia's quantum build

PsiQuantum is building a utility-scale quantum computer at Moreton Bay, near UniSC's Moreton Bay campus, backed by around $940 million from the Australian and Queensland governments.

Bringing on more industry partners

The model is proven. In 2026 industry partners brought real problems to the program and took away things they now use: a private 5G offering for container terminals, an AI investigator running on a production network, an irrigation platform sold across Australia, and a clinical Wi-Fi framework written into an international standard.

The next step is to bring on more industry partners with problems worth solving. A partner that joins draws on the full capability of the program across all ten universities, not a single one.

RESEARCH CHAIRS

A/Prof Alison Craswell
Digital Health and Ageing, University of the Sunshine Coast

Prof Frank den Hartog
Critical Infrastructure, University of Canberra

Prof Marius Portmann
Securing Future Networks, University of Queensland

Prof Trish Williams
Digital Health, Flinders University

Prof Wei Xiang
AI and IoT, La Trobe University

A/Prof Ilaria Barletta
Sustainable Engineering, University of Technology Sydney

In recruitment
AI Cyber Security, Adelaide University; Agentic AI, Curtin University; Defence Capability and Security, Flinders University; AI in Health Systems, La Trobe University; Sports Technology, Queensland University of Technology

INDUSTRY ALUMNI

Richard Dodsworth
Flinders University, and lead of the national Alumni program

Angelo Puglielli
University of Canberra

Drago Sijan
La Trobe University

Andrew McLean
University of Technology Sydney

Carl Solder
Curtin University

Rob de Nicolo and Marcus Lim
RMIT University

Mike Carr
University of Queensland

Adam Radford
Queensland University of Technology

Tony Saunders
University of the Sunshine Coast

SPECIALISED LABS

Private 5G Lab, Innovation Central Canberra
University of Canberra

Cisco–La Trobe Centre for AI and IoT
La Trobe University

UniSC Digital Health Productivity Lab
University of the Sunshine Coast

Cisco–RMIT Health Transformation Lab
RMIT University

Cisco–Flinders Digital Health Research Centre
Flinders University

UQ Centre for Future Networks
University of Queensland, in establishment

NIIN

National Industry
Innovation Network

NIIN.COM.AU

RESEARCH, DEVELOPMENT AND INNOVATION IMPACT REPORT 2026

© 2026 Cisco and/or its affiliates. All rights reserved.