

Position Description – *Cisco Research Chair –Defence Capability and Security*

Updated 2 July 2026

POSITION DETAILS

College/Portfolio	College of Science and Engineering
Organisational Unit	Engineering & Design
Supervisor (Title)	Vice President and Executive Dean (or delegate)
Classification	Research Academic Level E
Employment Type	Fixed Term (5 years)

POSITION SUMMARY

The Cisco NIIN Research Chair in Defence Capability and Security is a senior academic appointment at Flinders University, co-funded in partnership with Cisco Systems Australia. This is the first Cisco NIIN Research Chair in Defence — a strategically significant appointment reflecting Australia's urgent need to accelerate digital transformation in Defence.

The Chair operates with broad autonomy, reporting to the Dean of Research, College of Science and Engineering. The position provides intellectual and research leadership at the intersection of digital technology and defence capability across one or more strategic focal areas: advanced manufacturing for defence; AI for defence and national security; autonomous systems; and cyber security for defence and critical national infrastructure.

Working in direct partnership with Cisco, the Australian Defence Force, the Department of Defence, and the sovereign defence industrial base, the Chair leads applied research programmes that translate innovative technology platforms into real-world defence capability outcomes. The Chair also delivers postgraduate and executive education, supervises HDR candidates, and contributes to Flinders University's transdisciplinary hubs and South Australia's defence ecosystem.

The Chair will lead a small team of research staff and postgraduate students and participate in the national NIIN Research Chair network.

CISCO RESEARCH CHAIR PARTNERSHIP PROGRAM

This position is funded through the Cisco National Industry Innovation Network (NIIN) Research Chair Program, a partnership between Flinders University and Cisco Systems Australia. The NIIN is one of Australia's most effective industry-university collaboration models, established to bridge the gap between cutting-edge research and real-world industry application.

Research Chairs Program operates on a principles of co-designing applied research with Cisco and industry partners that moves swiftly from discovery to prototype, policy or commercial adoption. Key features of the NIIN Research Chair program include:

- Industry-led research co-designed with Cisco and national defence partners, producing prototypes, policies and improved practices.
- Early access to next-generation Cisco technologies: networking, security, AI/ML platforms, and IoT infrastructure.

**Changing 10 Million Lives.
Every One Matters.**

Agenda 2035



- Connection to the NIIN Research Chair network and Innovation Central hubs across Australia.
- Matched co-investment from Cisco and Flinders University, focused on scalable, transferable solutions with national impact.

STRATEGIC AREAS of FOCUS

The Chair will focus on one or more of the following areas, consistent with the candidate's expertise, the University's research strengths, and Cisco's strategic technology portfolio:

Focal Area 1: Advanced Manufacturing for Defence

- Additive and smart manufacturing; Industry 4.0/5.0 for defence production;
- sovereign industrial capability and digital supply chain resilience;
- digital design-to-manufacture pipelines and model-based systems engineering;
- Networking and IoT for connected factory and manufacturing execution systems for defence;
- AUKUS Pillar II advanced manufacturing technology development.

Focal Area 2: Artificial Intelligence for Defence and National Security

- AI-enabled command, control, communications and intelligence;
- Machine learning for intelligence analysis, threat detection and situational awareness;
- Human-machine teaming and trusted autonomous decision-making;
- AI assurance, safety and governance in high-stakes environments;
- AI enabled infrastructure for defence-grade AI deployments; adversarial AI and counter-AI operations.

Focal Area 3: Autonomous Systems — with particular emphasis on Maritime Applications

- Uncrewed surface vehicles (USV), autonomous underwater vehicles (AUV/UUV) and air-maritime autonomous systems;
- Autonomous mission planning, multi-vehicle coordination and swarming;
- Data fusion and maritime domain awareness;
- Resilience and assurance in contested or denied environments;

Focal Area 4: Cyber Security for Defence and Critical National Infrastructure

- Cyber resilience of defence networks, platforms and supply chains;
- AI-driven threat detection
- Quantum cryptography and post-quantum network security;
- sovereign cyber workforce development.

UNIVERSITY EXPECTATIONS AND VALUES

All staff at Flinders are responsible for understanding their obligations as set out in the University's code of conduct and are expected to:

- demonstrate commitment to the University's values of Integrity, Courage, Innovation, Excellence, and the underlying ethos of being Student Centred;
- contribute to the efficient and effective functioning of the team or work unit in order to meet the University's objectives. This includes demonstrating appropriate and professional workplace behaviours, providing assistance to team members if required and undertaking other key responsibilities or activities as directed by one's supervisor;
- promote and support an inclusive workplace culture which values diversity and embraces the principles of equal opportunity;

**Changing 10 Million Lives.
Every One Matters.**

Agenda 2035



- perform their responsibilities in a manner which reflects and responds to continuous improvement; and
- familiarise themselves and comply with the University's Work Health and Safety, Injury Management and Equal Opportunity policies.

Flinders University is committed to providing a safe, respectful and inclusive environment, free from gender-based violence. Appointment to this role is conditional on the completion of required pre-employment checks and declarations, each of which must be satisfactory to the University. This includes a Gender Based Violence declaration, in accordance with the National Higher Education Code to Prevent and Respond to Gender Based Violence (2025), and a Nationally Coordinated Criminal History Check.

Note: some aspects of this role may require the holder to hold or obtain an Australian Government security clearance; the University will support eligible candidates through the sponsorship process.

KEY POSITION RESPONSIBILITIES

The Cisco NIIN Research Chair in Defence Capability and Security is accountable for:

- Lead an applied research programme co-designed with Australian defence and national security partners, delivering on the Innovation and Development continuum — from proof-of-concept through to industry-ready solutions and policy outcomes
- Leverage early access to Cisco's next-generation networking, security, AI and IoT platforms to develop and validate defence-relevant research prototypes and capability demonstrations
- Attract competitive research funding and co-investments.
- Design and deliver postgraduate coursework and executive education in digital and networked defence technologies, aligned to the NIIN Innovation & Development curriculum model
- Contribute to professional defence education and whole-of-government training programs for ADF personnel, Defence civilians, and industry professionals
- Work closely with Innovation Central Adelaide to deliver programs for industry and university partners.
- Supervise Higher Degree by Research (HDR) candidates and mentor early career researchers, building Australia's sovereign defence-capable digital technology talent pipeline
- Work as an embedded industry partner with Cisco, Innovation Central Adelaide, Department of Defence, and defence industries
- Serve as a public expert on defence technologies in Australian defence, contributing to policy forums, parliamentary submissions, and media engagement
- Support AUKUS Pillar II collaborative technology development and connection with Cisco's global research network across the US and UK
- Participate actively in the NIIN Research Chair network, including the annual Research Chair Summit and cross-chair collaboration, and contribute to the Flinders University's defence research strategy
- Produce high-quality publications, technical reports, policy briefs and capability assessments that advance knowledge and practice in the areas of impact.
- Providing leadership and expertise to foster strategic local, national and international relationships, collaboration and networks with a range of stakeholders including industry, government and other external organisations.
- Any other responsibilities in line with the level of the position as assigned by the Supervisor and/or the University.

KEY POSITION CAPABILITIES

**Changing 10 Million Lives.
Every One Matters.**

Agenda 2035



The following capabilities are required to fulfil the Key Position Responsibilities:

- A doctoral qualification in a relevant discipline OR equivalent achievement at a senior practitioner level in defence industries or national security. For applicants without a PhD, refer to the equivalency policy and procedures to demonstrate equivalence.
- Demonstrated high level of research expertise or applied track record in one or more of the strategic focal areas: advanced manufacturing for defence; AI for defence and national security; autonomous systems (particularly maritime); or cyber security for defence and critical infrastructure
- Proven ability to work at the research-to-industry interface, translating technical innovation into real-world capability outcomes
- Evidence of effective teaching or professional development delivery at postgraduate or executive level, or a demonstrable capacity to contribute at this level
- A proven record of attracting and managing competitive research funding or major industry or government-funded programmes
- Established or demonstrable networks within the Australian defence, national security, and/or digital technology ecosystem, including the ADF, Department of Defence, DST Group, ASD, and sovereign industry
- Familiarity with Cisco's technology portfolio — including networking, security (Duo, Umbrella, XDR, SASE), AI/ML platforms, or IoT — and their application to defence and critical infrastructure (desirable)
- Eligibility and willingness to obtain an Australian Government security clearance at Negative Vetting Level 1 or higher (desirable)
- Outstanding written and oral communication skills, with the ability to engage credibly across technical teams, ADF and Defence stakeholders, policymakers, and the public
- Demonstrated high level leadership skills, including the demonstrated ability to establish and make effective contributions to leadership within the College, students and industry nationally and/or internationally.
- Proven ability to mentor less experienced College Staff.

**Changing 10 Million Lives.
Every One Matters.**

Agenda 2035

