Annex A – Translation and Innovation Grant 2025 and PROPEL-X

About Translation and Innovation Grant 2025

The CyberSG R&D Programme Office Translation and Innovation Grant supports early-stage cybersecurity technologies from academia with clear commercialisation potential via spin-offs or industry partnerships.

By mandating industry collaboration and rigorous assessment of technical novelty, business viability, and market relevance, the grant strengthens academia-industry linkages, and reinforces Singapore's position as a launchpad for next-generation cybersecurity solutions.

13 new research projects were awarded up to a total of $13.2 million under the Translation and Innovation Grant (October 2025). These projects cover important areas such as Cybersecurity for Critical Information Infrastructure, Cybersecurity through Agentic Artificial Intelligence (AI), fully Homomorphic Encryption-protected machine learning models, etc. These research project team will be incorporated onto the PROPEL-X.

S/N	Project Team	Project Information
1	• Nanyang Technology University, Singapore (NTU) • Zama	**Efficient Fully-Homomorphic Encryption-Protected Machine Learning Models** The team is developing efficient machine learning models that run directly on encrypted data using Fully Homomorphic Encryption (FHE). By leveraging their patented TTnet architecture with Zama's FHE stack, the solution makes encrypted AI practical for image and multimodal tasks, ensuring privacy, compliance, and security without sacrificing accuracy or speed. Team is also interested in spinoff company and earlier received NTU Gap Fund for explainable AI for TTNet patent productisation.
2	• NTU • HY M&E Consultancy Services	**Cyber-Physical Risk Assessment for Power Grid Networks using Advanced Digital Twin** The team is developing a real-time Digital Twin–based cyber-physical co-simulation testbed for modern power systems, with a focus on inverter-based resources (IBRs). The platform enables stakeholders to model cyber-attacks, assess vulnerabilities, and test mitigation strategies in a safe, Hardware-in-the-Loop (HIL) environment. The team will work with core stakeholders such as SP Group, EMA, MPA, and DSTA to validate and adopt the testbed.
3	• NTU • Antarex	**AutoSOC: A Knowledge-Driven Agentic AI System for Automated SOC Operations**

		AutoSOC is a knowledge-driven, agentic AI system that automates SOC alert triage and investigation with explainable response plans. Built on a two-phase agent architecture, it separates reasoning (signal extraction via tools) from solution planning (case retrieval with Chain-of-Thought reasoning and reinforcement learning), mirroring analyst workflows. The project will be piloted with Antarex Cyber on its MXOC platform, with NTU leading technical development and Antarex providing real-world SOC data, environments, and feedback.
4	• NTU • Cyber Sierra	**ComplianceAgent: Autonomous Cybersecurity Compliance through Multi-Agent Coordination** The team is building a functional prototype of an end-to-end multi-agent system for automated cybersecurity compliance. The system features an AI-driven Orchestrator Agent that coordinates modular task agents using a shared compliance knowledge base and memory module. It will be delivered as a modular, extensible prototype that can integrate with Cyber Sierra's SierraAI platform and demonstrated through real-world compliance scenarios, with the goal of future licensing.
5	• A*STAR I²R • StrongKeep	**vCISO: An Agentic Approach to Build a Virtual CISO** The team is developing an Agentic AI Virtual CISO that orchestrates decision-making covering all the functions of cybersecurity, across an entire business. The Virtual CISO works with multiple tool-based security agents, contextualises unstructured external data such as threat intelligence, and derives and executes specific real-time actions to deliver holistic cybersecurity protection for SMEs, at low cost. Existing tool-based AI security agents only optimise for their own narrow functionality but are unable to have visibility across other aspects of a business (e.g. training results, compliance requirements), which a human CISO could. StrongKeep is a cybersecurity SaaS provider serving SMEs and is developing this to enable this industry segment to have access to simple, affordable, effective, and holistic cybersecurity protection for their business.
6	• Singapore-ETH Centre • Nexusguard	**FIREx - Future Internet Resilience Exchange** FIREx is an open platform for DDoS defense that standardises scrubbing, allowing multiple operators to offer

	• Blindspot Technologies s.r.o • Giesecke+Devrient ePayments Asia	filtering capacity. It introduces a market for "Filter Slots," letting companies reserve protection in advance at transparent, market-based prices, improving flexibility, resilience, and cost-efficiency compared to traditional single-provider solutions. FIREx will be spun off as a platform company with support from partners like Nexusguard, Blindspot, and Giesecke+Devrient ePayments Asia for distributed scrubbing infrastructure, testing, and validation.
7	• Illinois Advanced Research Centre, Singapore (IARCS) • Cybernatics	**Intelligent and Accessible Threat Modelling** The team had developed an AI-driven threat modelling platform that automatically generates system-specific attack paths and actionable security controls from minimal system information. The immediate plan is to expand adoption within GovTech and extend the use of the tool across government agencies, with interest already expressed by HTX and Singapore Power. Its commercialisation will be pursued through a spinoff, focusing on automated ingestion of system documentation to facilitate onboarding, and development of domain-specific threat model databases for sectors such as finance, healthcare, and critical infrastructure.
8	• National University of Singapore (NUS) • AIQURIS	**Bridging the AI trust gap with LLM-powered Program Analysis** AutoExe is a software verification platform that bridges the trust gap in AI-generated code by combining program analysis with LLM reasoning. It automatically detects bugs and vulnerabilities, reducing the manual review burden and ensuring secure, compliant deployment in critical industries. The team aims to spin off a company based on AutoExe as a Singapore-based deep tech startup, building on their progress in the National GRIP. With AIQURIS as an industry collaborator and strong early market validation, the team will scale AutoExe from TRL5 to TRL8+, positioning it for licensing to their own spinoff, adoption by critical sectors, and expansion into the global market for secure AI-assisted development.
9	• NUS • Ensign Infosecurity	**Agentic-VAPT: Empowering Vulnerability Assessment and Penetration Testing using Agentic AI** The project delivers an AI-Agentic Penetration Testing Platform that automates the full penetration testing workflow from reconnaissance to reporting, using large

		language models, agentic workflows, and interoperability with standard security tools. The platform will be co-developed and piloted with Ensign InfoSecurity, ensuring alignment with industry standards and real-world needs. Initial deployment will focus on regulated sectors and enterprises in Singapore, with MSSPs as key distribution partners.
10	• NUS • i-Sprint Innovations	**A Closed-Loop, Interpretable, and Lightweight AI-based IAM Framework** The team is developing an AI-driven Identity and Access Management (IAM) framework that is adaptive, explainable, and edge-ready. It introduces novel techniques for early interpretable anomaly detection, synthetic data augmentation under scarcity, analyst-friendly explainability, and lightweight deployment, moving beyond static rule-based IAM systems to real-time, transparent, and self-improving security. The framework will be integrated into i-Sprint's IAM product suite, validated through joint academic–industry prototyping with NUS, and scaling via partnerships and deployments in high-security sectors.
11	• NUS • UOB • ProofSpace	**Anonymous Payment for Consortium Blockchain Among Singapore Banks** The team is developing an anonymous payment system for Singapore banks using zero-knowledge proof (ZKP) technology. The system hides transaction details – including sender, receiver, and amount – while allowing validation on both private and public blockchains. The system targets Singapore's major banks, enabling privacy-preserving, compliant, and high-speed blockchain payments.
12	• SMU • DigiDations	**AutoIntelligence: An End-to-End Agentic Platform for Software Security Intelligence** AutoIntelligence is an AI platform that collects and analyses software supply chain intelligence, then fuses it with traditional threat intelligence to deliver comprehensive, actionable insights. The platform transforms fragmented threat data from diverse sources into reliable intelligence linked to real software components. In partnership with digiDations, AutoIntelligence will launch as a subscription service, piloted with local partners before scaling to MSSPs, enterprises, and critical infrastructure. By adhering to global

		cybersecurity standards, it positions Singapore as a leader in AI-driven threat intelligence for the software supply chain.
13	• SUTD • Ensign Infosecurity	**Cloud-based Intelligent OT-Centric Asset Monitoring for Critical Infrastructure** The team has developed a scalable version of iTrust's flagship technologies, Distributed Anomaly Detection (DAD) and AICrit, for deployment in large-scale water and wastewater treatment plants. This is a cloud-based OT-centric monitoring platform that can automatically generate, deploy, and manage DAD and AICrit models at scale. The team will be partnering with Ensign InfoSecurity to translate DAD and AICrit into commercial solutions for critical infrastructure operators such as PUB, government agencies, and utilities.

About PROPEL-X

PROPEL-X is a first-of-its-kind Gen-AI-enabled coaching and collaboration platform. It is designed to strengthen Singapore's cybersecurity talent pipeline and accelerate research-to-industry innovation. The platform connects students, researchers, government, and industry professionals to collaborate and learn more effectively.

Key features

- **Gen-AI enabled guidance:** Helps users emergently sharpen judgment, build clarity, and create value through continuous learning.

- **Incremental growth model:** Inspired by the "Atomic Habits" approach – the idea that small actions, repeated consistently, can lead to big, long-term improvements.

- **Beyond task tracking:** Captures rapid moments of insight, collaboration, and innovation to provide a richer view of progress and talent development over and beyond traditional KPIs.

Why it matters

- **Innovation through collaboration:** PROPEL-X makes the gradual process of shared learning and discovery visible and measurable.

- **Human-AI partnership:** As AI reshapes the cybersecurity landscape, PROPEL-X develops deep thinkers, agile learners, and effective collaborators.

- **National advantage:** By nurturing adaptable and forward-thinking talent, PROPEL-X supports Singapore's resilience and competitiveness in the digital age.