GRANT CALL 2018

NATIONAL CYBERSECURITY R&D PROGRAMME

- Whole-of-Government (WoG) initiative to promote collaboration among agencies, academia, research institutes and private sectors in cybersecurity

Develop R&D expertise in cybersecurity for Singapore

Coordinate and prioritise R&D efforts in cybersecurity across agencies

Create platforms for R&D collaborations among agencies, academia, research institutes and industry

NATIONAL RESEARCH FOUNDATION
PRIME MINISTER'S OFFICE
SINGAPORE

CSA SINGAPORE

NSCS NATIONAL SECURITY COORDINATION SECRETARIAT

MINISTRY OF HOME AFFAIRS

MINDEF SINGAPORE

GOVTECH SINGAPORE

EDB singapore

IMDA INFOCOMM MEDIA DEVELOPMENT AUTHORITY

RESEARCH CAPABILITIES

TRUSTWORTHY SOFTWARE SYSTEMS

Binary Analysis & Hardening

Led by NUS National University of Singapore

Build Secure Verified Systems

Led by NANYANG TECHNOLOGICAL UNIVERSITY

CYBER-PHYSICAL SYSTEMS SECURITY

Cyber-Physical System (CPS) and IoT Security

Led by SUTD Singapore University of Technology and Design

Securing Urban Transportation Systems

Led by Institute for Infocomm Research A*STAR

CYBER FORENSICS SYSTEMS

Cyber Forensics and Intelligence

Led by Institute for Infocomm Research A*STAR

MOBILE SECURITY & CLOUD SECURITY

Mobile Security & Cloud Security

Led by SMU

Cloud Security

Led by NYP Nanyang Polytechnic

Grant Call 2016

Supported 9 Academia—Companies' joint technology development in 2017

S/N	NCR S/N	Title of Project	IHL/ RI, Company
1	NCR002-012	Malware Source Attribution through Multi-Dimensional Code-Feature Analysis	NUS, Kaspersky
2	NCR002-020	Advanced Anti-Malware Solution Using Deep Learning	NUS, SecureAge
3	NCR002-022	Build Next-generation Secure Environments on Smartphones for Critical Mobile Applications	SMU, iSprint
4	NCR002-025	Cybersecurity Protocol and Mechanism for e-Logistics of Dangerous Goods Tracking Using Block Chain	NTU, iSprint
5	NCR002-027	To Research and Develop Assessment Tool and System – OpsTrace	NTU, Attila CyberTech
6	NCR002-026	Smart Binary-level Vulnerability Assessment for Cyber-attack Prevention	NTU, Scantist
7	NCR002-004	A Secure, Privacy-preserving Data Exchange/Computation Platform for the Smart Nation	NTU, Acronis
8	NCR002-023	Advanced Intelligent Anomaly Detection System	SUTD, Attila CyberTech
9	NCR002-028	Testing for Blockchain Security by Design	SUTD, TNO

NATIONAL CYBERSECURITY R&D GRANT CALL 2018

Applications close 1 November 2018

Brought to you by

NATIONAL RESEARCH FOUNDATION
PRIME MINISTER'S OFFICE
SINGAPORE

CSA SINGAPORE

NSCS NATIONAL SECURITY COORDINATION SECRETARIAT

MINISTRY OF HOME AFFAIRS

MINDEF SINGAPORE

GOVTECH SINGAPORE

EDB singapore

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

In partnership with

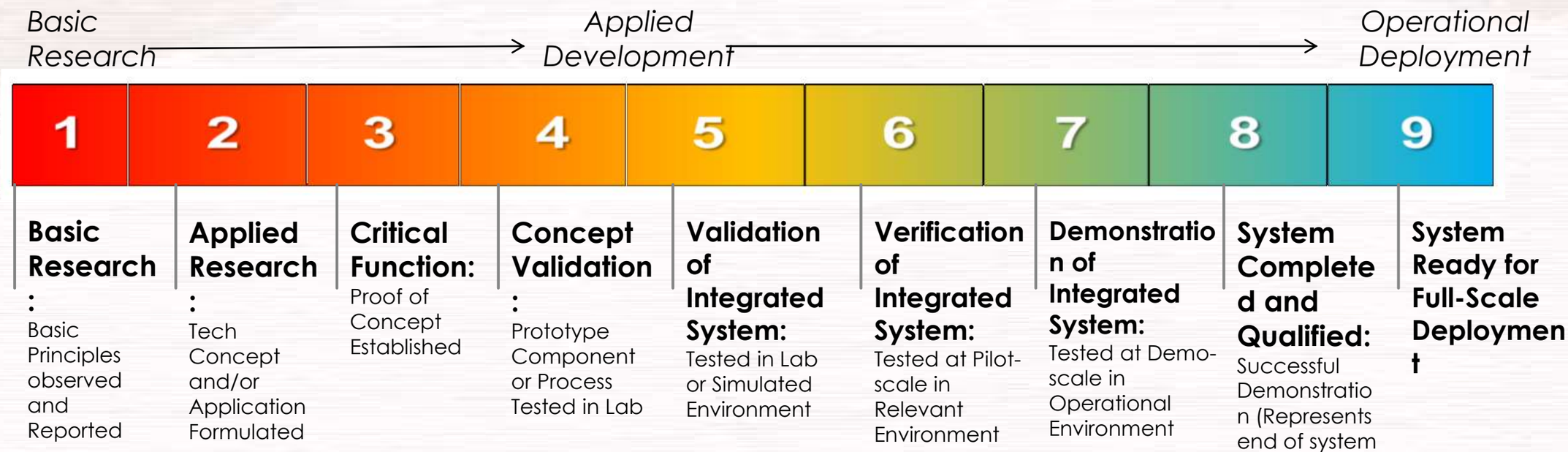
ENERGY MARKET AUTHORITY
Smart Energy, Sustainable Future

GRANT CALL 2018 OBJECTIVE

Offers funding to **applied** research programmes that address specific cybersecurity needs of government and national security

- Should span approximately from TRL* 4 to TRL 7
- Open to companies, Institutes of Higher of Learning (IHLs) and Research Institutions (RIs) to collaborate and build cybersecurity tools & capabilities
- Up to $2M per project

*Technology Readiness Level ("TRL") is a schema to assess the maturity of technologies



HOW TO APPLY

Step 1. Eligibility

- Singapore-based IHLs, RIs
- Singapore-based companies
- Not recipient of grants from the Singapore government for a similar project

Step 2. Team up

- Host Institution (Company) + Partner Institution (IHL/RI)

FUNDING SUPPORT

Agency	Partner Institution	Host Institution	
	Institutes of Higher Learning / Research Institutes	*Small and Medium Enterprises*	*Large local enterprises and Foreign companies*
National Research Foundation	100% of costs		
EDB Singapore			Up to 30% of company's total project costs
IMDA Infocomm Media Development Authority		Up to 50% of qualifying costs	
Energy Market Authority – Smart Energy, Sustainable Future Only applicable to topics related to "Cybersecurity for the Energy Sector"	100% of costs	Up to 50% of qualifying costs	Up to 30% of company's total project costs

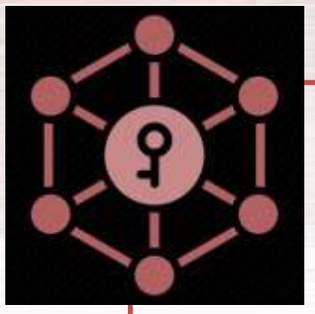
PROBLEM STATEMENTS

A. Cybersecurity Forensics and Investigations

Build research capabilities to acquire data, and analyse and contextualize evidence for law enforcement and investigations.

- **Topic 1**: IOT Forensics & Investigation Analysis
- **Topic 2**: Investigative Tools for Distributed Ledgers
- **Topic 3**: Deeper Awareness and Machine Learning of Logs for Threat Intelligence, Risk Management and Investigations

PROBLEM STATEMENTS



B. Adaptive Network Security

Proactive, AI-enabled security mechanisms that can provide continuous security against persistent and evolving network threats.

- **Topic 4**: Cyber Self Protection for Enterprise Network

PROBLEM STATEMENTS

C. Security Architectures and Composable Security Components for Data Privacy & Protection in the Cloud

Innovative and modular solutions to secure data and applications in a multi-tenancy cloud environment.

- **Topic 5**: Security Architecture and Composable Security Components for Data Privacy & Protection in the Cloud

PROBLEM STATEMENTS

D. Cyber Inoculation Against Human Incompetence and Frailties

Help the vulnerable avoid online scams and other cognitive/semantics attacks

- **Topic 6**: Cyber Inoculation Against Human Incompetence and Frailties

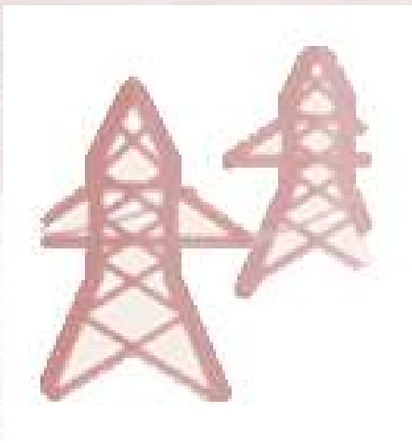
PROBLEM STATEMENTS

E. Enhanced Security Evaluation & Assurance

Improvements in engineering designs, testing and standards to include strong security principles.

- **Topic 7**: Enhanced Security Evaluation & Assurance of Autonomous Unmanned Vehicles (Land, Sea, Air) and Automation Assets

PROBLEM STATEMENTS



F. Cybersecurity for the Energy Sector

Securing and strengthening the resilience of our energy delivery systems.

- **Topic 8**: Innovative anomaly detection schemes that leverage on the unique physical processes within the power system
- **Topic 9**: Secure system architecture and protocols that are both lightweight and scalable, for the power system
- **Topic 10**: Testing tools, infrastructure, or capabilities that enable the rigorous validation of new or existing cybersecurity solutions for the power system

PROBLEM STATEMENTS

G. Novel Implementation of Cybersecurity Technology

Innovative proposals that do not fall under any of the previous categories.

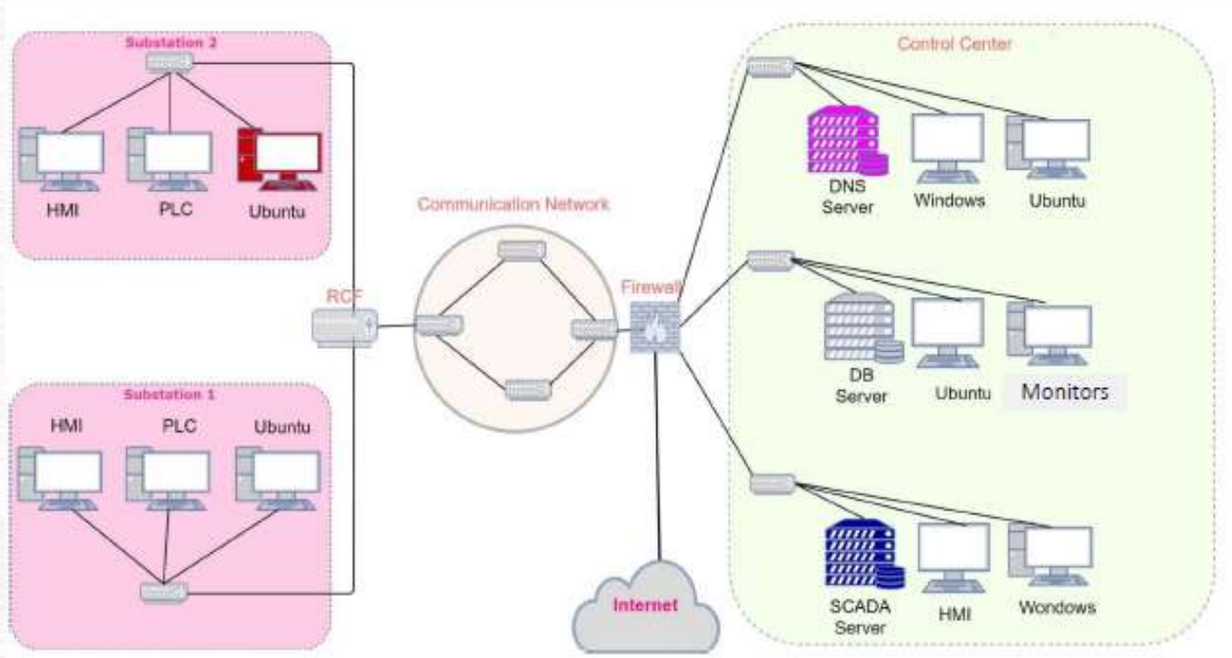
- **Topic 11**: Novel Implementation of Cybersecurity Technology

SUPPORTING RESEARCH AND TECHNOLOGY VALIDATIONS

SUGGESTED PLACEMENT FOR EMA SLIDES

NATIONAL CYBERSECURITY R&D LABORATORY (NCL)

The NCL provides computing resources, vulnerable environments and data sets for repeatable cybersecurity investigation and experimentation environments



Visit: https://ncl.sg to find out more
Email: support@ncl.sg

USE OF ITRUST LABS

World-class Testbeds

- The rich set of one-of-a-kind testbeds offer a tremendous opportunity for research and business development in the design of the secure critical infrastructure.

Contact:

itrust@sutd.edu.sg to request the use of testbed and training platform