Auto-ISAC Overview

Josh Davis

GVP & Chief Cybersecurity Officer, Toyota Motor North America

SVP & Chief Cybersecurity Officer, Toyota Connected North America

PGM & Senior Advisor for Global Enterprise Security, Toyota Motor Corporation

Chairperson, Automotive-ISAC

AUTO-ISAC

The Department of Homeland Security (DHS) Traffic Light Protocol (TLP) Chart

Label	When Should This Label Be Used?	How Should This Information Be Shared?
TLP:RED  *Not for disclosure; restricted to participants only*	• Additional parties **cannot take effective action** to prevent further harm • **Impact to privacy, reputation, or operations** if misused	• **Do not share with any parties** outside of the specific exchange, meeting, or conversation in which it was originally disclosed
TLP:AMBER  *Limited disclosure; restricted to participants' organizations*	• **Requires support** to be effectively acted upon • Carries **risks to privacy, reputation, or operations** if shared outside of the organizations involved	• **Only share within your own organization**, and with clients or customers who need to know the information **to protect themselves or prevent further harm**
TLP:GREEN  *Limited disclosure; restricted to the community*	• Useful for the **awareness of all participating organizations and peers** within the broader community	• **Share with peers and partner organizations** within your sector, but not via publicly accessible channels • May circulate widely within a particular community, but **may not release outside of the community**
Today's classification **TLP:WHITE**  *Disclosure is not limited*	• **Minimal or no foreseeable risk of misuse**	• May be distributed **without restriction** *(subject to copyright rules)*

AUTO-ISAC

What is an ISAC and Why is it Needed?

Created in 1998, Information Sharing & Analysis Centers (ISACs) were a product of a US Presidential directive to help protect critical infrastructure from cyber attacks. Today there are over 24 ISACs across different sectors, including Auto-ISAC.

ISAC Purpose

1 Facilitate exchange of threat intelligence

- Anonymous Submission
- Limitation on the use of information

2 Protect critical infrastructure & key resources

- Elevate **"security and resilience"** across industries by sector

3 Provide unique capabilities for sharing of threat intelligence

- Member-to-member sharing
- Diverse partnership network

ISAC Member Legal Protections

ISACs are given special protections that allow for **sharing and receiving threat intelligence with less legal risk** *(when shared in accordance with US federal procedures)*.

AUTO-ISAC

About the Automotive ISAC (Auto-ISAC)

*Established in 2015, Auto-ISAC's mission is to provide an **unbiased, central point of coordination and communication** for the global automotive industry through the analysis and sharing of **trusted and timely cyber threat information**.*

Membership is open to:

1. Light and Heavy-Duty Vehicle **OEMs**
2. Light and Heavy-Duty Vehicle **Suppliers**
3. **Commercial** Vehicle Companies

Core Services

Member Benefits

Gain access to an expansive network of companies dedicated to making our industry more secure, together:

- Leverage the resources of the Auto-ISAC community to improve your cyber program.
- Get timely and actionable threat intelligence through Auto-ISAC's community driven intelligence sharing services.

One company's detection of a threat...

could help another prevent or better respond to an incident.

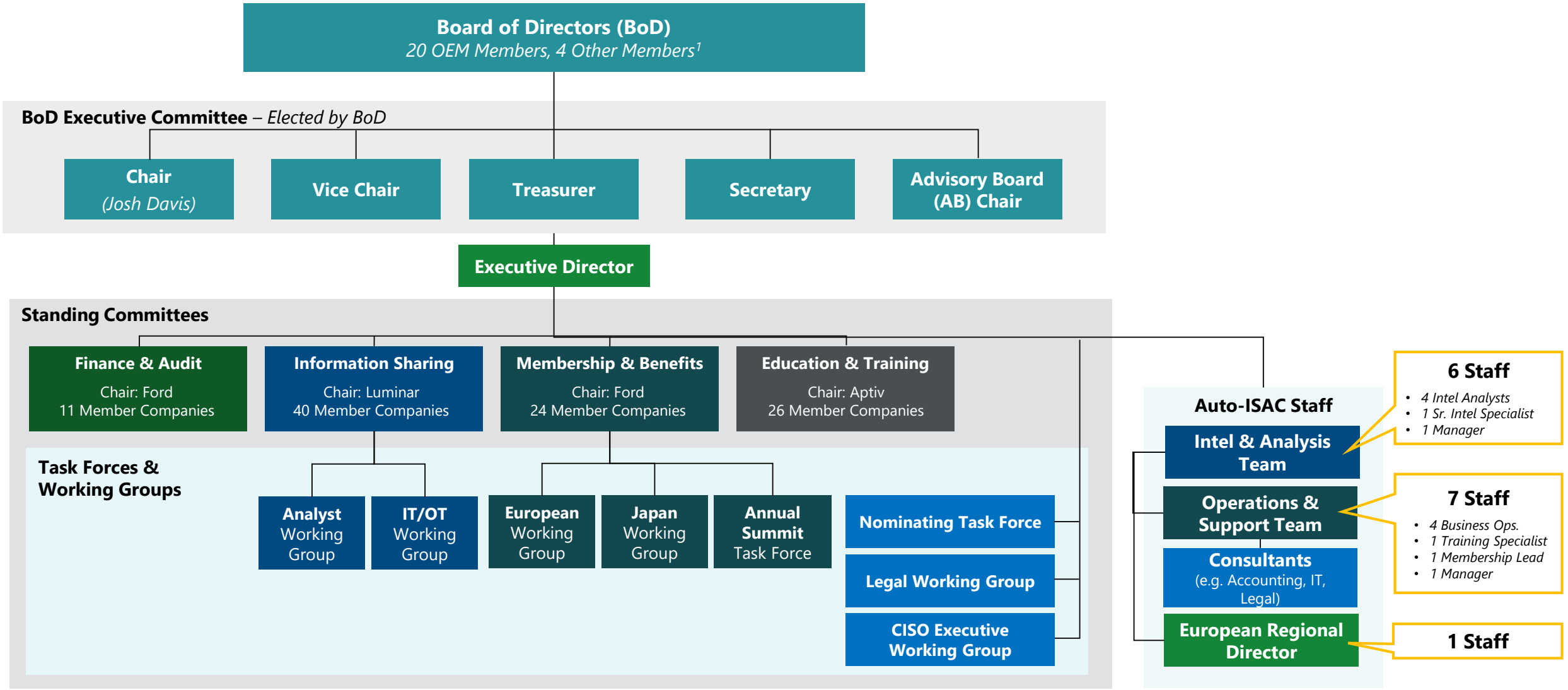
AUTO-ISAC

Auto-ISAC Member List (78 Total = 29 OEMs + 49 Suppliers)

Member Companies				
Aisin	Denso	Kia	Motional	Sumitomo Electric
Allison Transmission	e:fs	Knorr Bremse	Navistar	Thyssenkrupp
American Axle & Manufacturing	Faurecia	KTM	Nexteer Automotive Group	Tokai Rika
Aptiv	Ferrari	Lear	Nissan	Toyota
Argo AI, LLC	Flex	LG Electronics	Nuro	TuSimple
AT&T	Ford	Lucid Motors	Nuspire	Valeo
AVL List GmbH	Garrett	Luminar	NXP	Veoneer
Blackberry Limited	General Motors	Magna	Oshkosh Corp	Vitesco
BMW Group	Geotab	Marelli	PACCAR	Volkswagen
BorgWarner	Harman	Mazda	Panasonic	Volvo Cars
Bosch	Hitachi	Mercedes-Benz	Polaris	Volvo Group
Canoo	Honda	Meritor	Qualcomm	Waymo
ChargePoint	Hyundai	Micron	Renesas Electronics	Yamaha Motors
Continental	Infineon	Mitsubishi Electric	Rivian	ZF
Cummins	Intel	Mitsubishi Motors	Stellantis	
Cymotive	John Deere Electronic	Mobis	Subaru	

AUTO-ISAC

2022 Auto-ISAC Organization Chart



[1] *Other BoD representation from:*
- *Advisory Board (AB): Chair & Vice Chair*
- *Supplier Affinity Group (SAG): Chair*
- *Commercial Affinity Group (CAG): Chair*

New 2023 Auto-ISAC Board of Directors (BoD) Structure

Current Structure (2022)

2 **BoD Members**
20 OEMs[1], 4 Other

45 **BoD Executive Committee**

1. Board Chair
2. Vice Chair
3. Treasurer
4. Secretary
5. AB[3] Chair

Only OEMs[1]

Non-OEM

Challenges of a large board:

- Reaching minimum attendance to have a quorum *(at least 50% of BoD)*
- Obtaining a majority to make a decision

Future Structure (2023+)

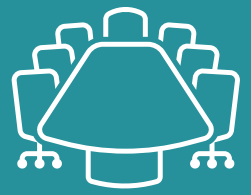
Effective January 1, 2023

10 **BoD Members**
Must always be >50% OEMs[1]

1. Board Chair
2. Vice Chair
3. Treasurer
4. Secretary
5. Flex Seat[2] #1
6. Flex Seat[2] #2
7. Flex Seat[2] #3
8. SAG[3] Chair
9. CAG[3] Chair
10. EuSC[4] Chair

Only OEMs[1]

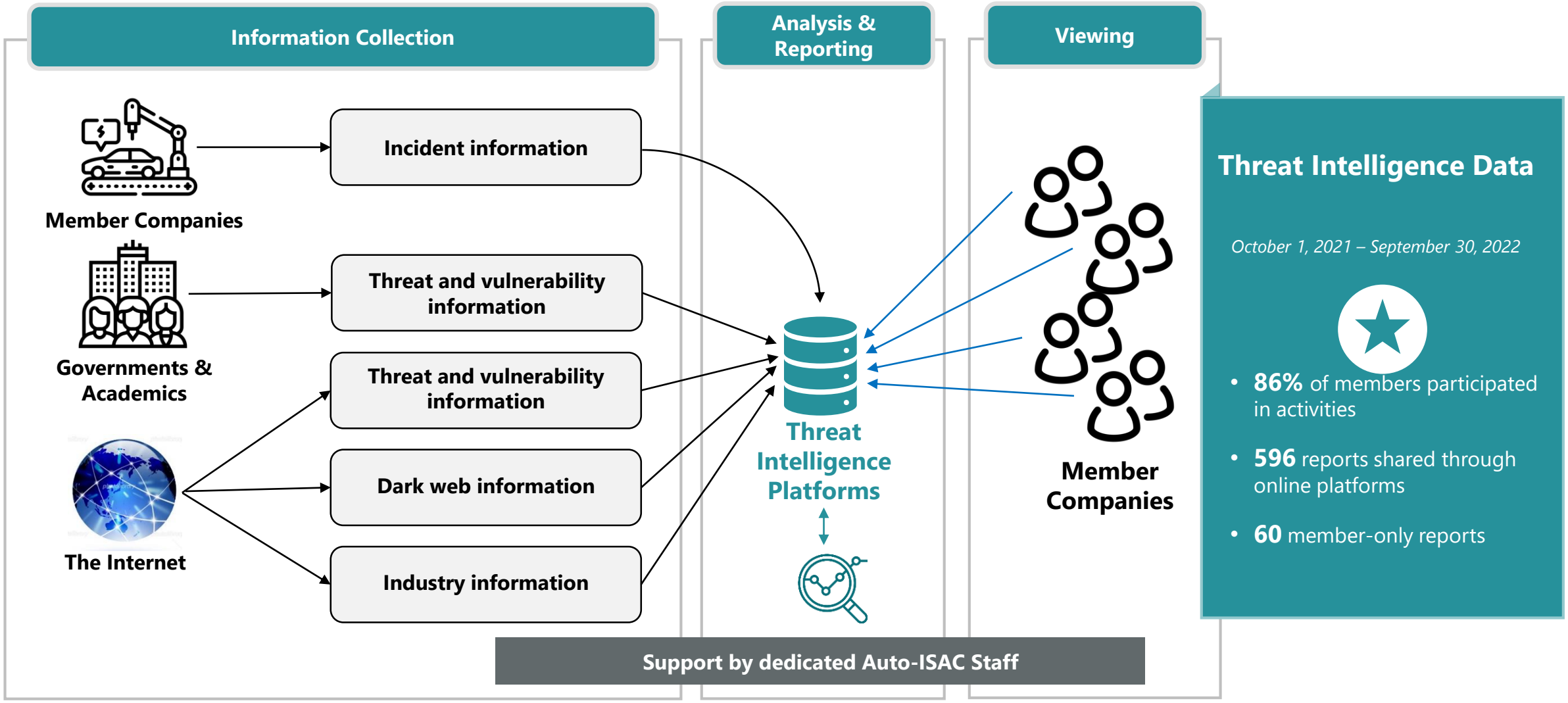
Benefits of the Future Board Structure



- ✓ Enable **faster decision making** for Auto-ISAC
- ✓ **Broader representation** of the Auto-ISAC member population

[1] Original Equipment Manufacturer (OEM) as defined by National Highway Traffic Safety Administration (NHTSA)
[2] Flex seats may be filled by an OEM or non-OEM member while ensuring the composition of the board criteria is met (>50% OEMs)
[3] Non-OEM Representation: Advisory Board (AB), Supplier Affinity Group (SAG), Commercial Affinity Group (CAG)
[4] European SC Chair (EuSC)

Auto-ISAC Threat Intelligence Sharing Model[1]



Threat Intelligence Data

October 1, 2021 – September 30, 2022

- **86%** of members participated in activities
- **596** reports shared through online platforms
- **60** member-only reports

[1]Supports cybersecurity event monitoring and sharing as noted in the National Highway Traffic Safety Administration (NHTSA) Best Practices, UN Regulation No. 155 (UNECE R155), and International Organization for Standardization/Society of Automotive Engineers 21434 (ISO/SAE 21434).

AUTO-ISAC

Auto-ISAC Additional Activities

1

Tabletop Exercises

Annual practice drills designed for members to support cyber resilience.

2

Monthly Community Calls

Knowledge sharing from leaders in cybersecurity.

3

Bi-weekly Threat Briefing

Deep discussion of recent security threats and vulnerabilities.

4

Quarterly Workshops & Webinars

Face-to-Face engagement between analysts, executives, and strategic partners.

5

Auto Cybersecurity Training (ACT[1])

Curriculum to develop "fully qualified" automotive cybersecurity practitioners.

6

Annual Summit

Automotive cybersecurity conference to showcase industry insights and member collaboration.

[1]Funded by NHTSA; Expected release in 2023

AUTO-ISAC

Auto-ISAC Reflections and Opportunities

Reflections

1. Benefit of stronger "joint" communications to customers, public, government, and media.
2. Threats targeting connected vehicle product and information systems (IT/IoT) make it necessary to include both organizations.
3. Frequent staff rotation by members can lead to many management re-introduction efforts.

Opportunities

1. Resolve which ISAC leads community regarding threats against:
   A. On-car ADAS sensors and sensor fusion techniques.
   B. Connected charging infrastructures and systems.
   C. MaaS systems such as sharing.
2. Clarify membership opportunities for companies not yet producing in-market products or services.


THANK
YOU
GRAZIE
ASANTE
MERCI
MULTUMESC
MAAKE
KIITOS
KIA ORA
OBRIGADO
MATONDO
CHOKRANE
MATUR NUWUN
DANK JE
SPASIBO
ARIGATO
VINAKA
WELALIN
JUSPAXAR
TERMA KASIH
RAIBH MAITH AGAT
MOCHCHAKKERAM
SALAMAT
CAM ON BAN
UA TSAUG RAU KOJ
DANKON
NIRRINGRAZZJAK
MAMANA