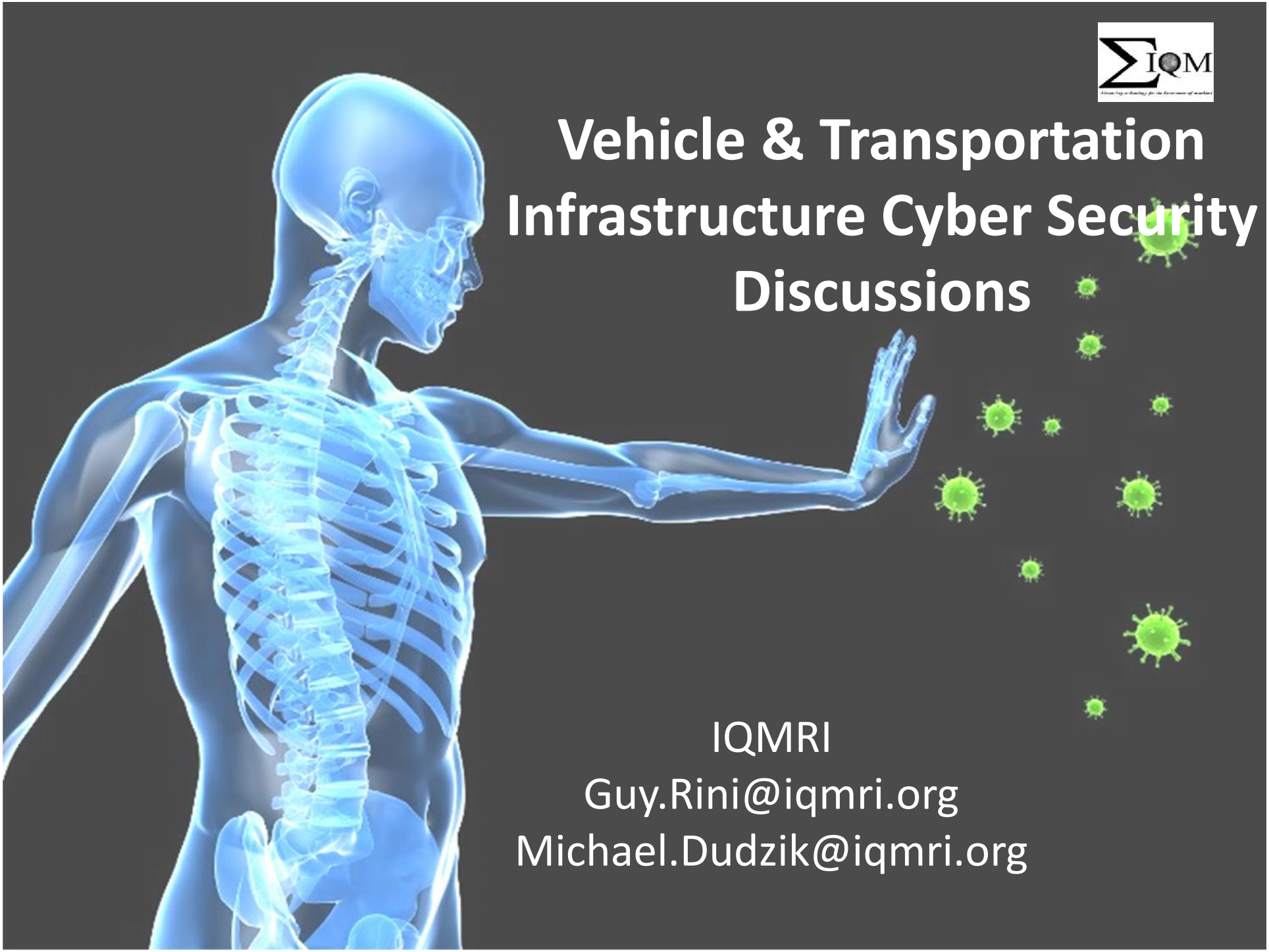
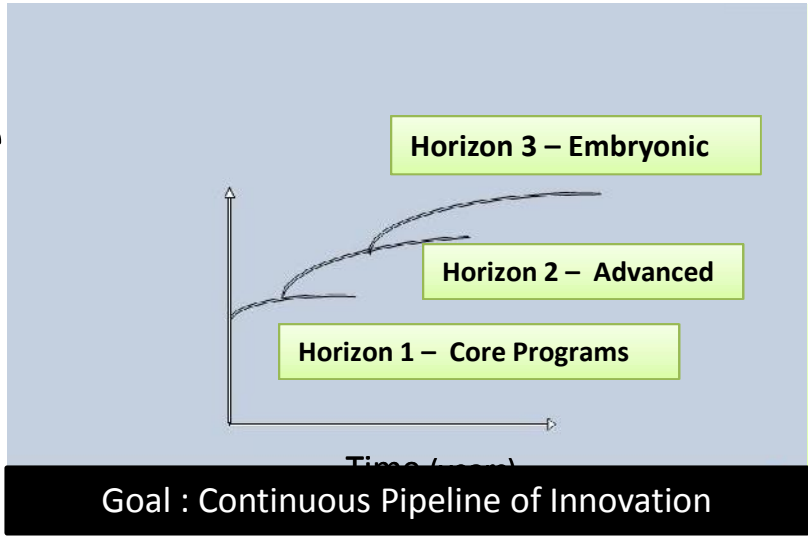


Vehicle & Transportation Infrastructure Cyber Security Discussions

IQMRI
Guy.Rini@iqmri.org
Michael.Dudzik@iqmri.org

IQM Research Institute

- IQMRI created in response to the structural changes in delivery of Innovation Worldwide
  - Builds upon 50+ years of Innovation
  - Physics-based Applied R&D Programs
  - Collaboration and Consortium Focus
  - World Class Subject Matter Experts
  - Unbiased Technology & Integration
- Locations
  - Ann Arbor, MI (HQ & Labs)
  - Offices
    - Washington, DC
    - Atlanta, GA
    - Palo Alto, CA



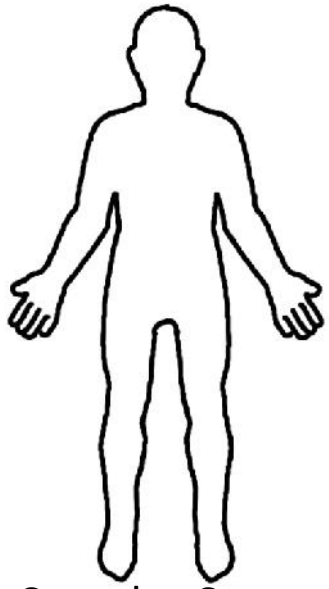
Cyber Security Analogy

Human Body

- 26% of Human Body is Defensive Against
- 98% Cell Replacement <2years

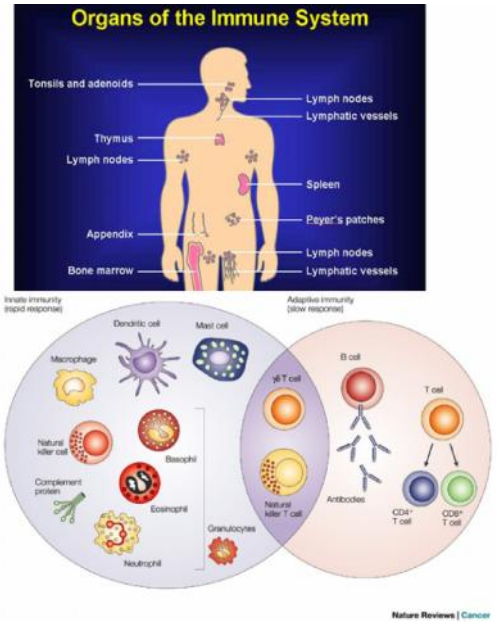
Embedded Systems

- Digital Architectures in Vehicles & Transportation
- Constant Software Upgrades



Complex System

Cyber Threats



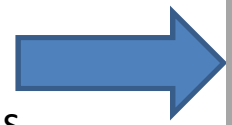
Cyber Security Defense In-Depth

Threats

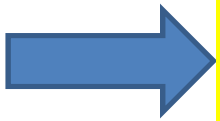
Level of Threat

- **Level I – Hacker Threat**
  - Hacker Pathways – Wireless, OBDII, Embedded
  - Protection of Driver Generated Data
- **Level II – Unknown/Unknown Threat**
  - Evolution of new Open Architectures and subsystems
  - Design, manufacture, aftermarket, infrastructure
- **Level III – Nation State Attack**
  - Outside Transportation Industry R&D Purview

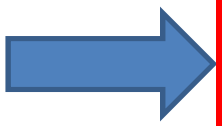
Recent Examples



" 20-year-old Omar Ramos-Lopez, a disgruntled former employee of Texas Auto Center remotely disabled more than 100 customers' vehicles by hijacking the dealership's vehicle immobilization system using a stolen password"



"Fiat Chrysler Automobiles will recall 1.4 million cars and trucks to protect them from cybersecurity attacks after Wired magazine revealed that a Jeep Cherokee could be hacked remotely through a DSRC vulnerability"



"The Guardians of Peace (North Korea) hacked Sony computers in response to allocations of the insults to their leadership. The attackers indicated that Sony had failed to meet their demands. "We've already warned you, and this is just the beginning. We continue till our request be met."

Vehicle Industry

Moving on a Positive Vector

- **Cyber Security is One of the Industry's Top Priorities**
  - The Auto industry is conducting R&D to enhance vehicle security
  - Focus is on cost-driven solutions
  - Prevent, Find/Fix, Culture Change, Standards follows Crash Safety Paradigm
  - Building upon ISO 262 Series Risk-based Standards
- **The Cyber Security levels in Future Commercial Vehicles Based on Three Determinates:**
  - Cyber Risk ,Regulatory Requirements, Consumer Driven Demand
- **OE /Supplier Ecosystem is Building Awareness and Capability in Cyber Security for Components & Systems**
  - Requirements and Investment greater than Federal Agencies
- **Fleet Owner/Operator Concern Growing**

Requirements & Standards

Long View Needed

- Cyber Security Design Requirements vs Performance Intent
  - Baseline System Design Strategy
    - Liability Assignment
    - Defense in-depth (Constructive, Operational, Reactive)
  - Procurement Strategy
    - Baseline Systems
    - Custom Developed Solutions
  - Requirements Security
  - Procurement Validation

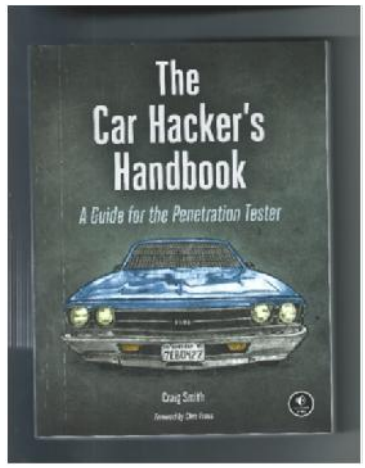
Problem:
How does an organization develop a purchasing description ?

- Standards and Rulemaking
  - Federal Transportation Agencies (DOT/NHTSA/FWA)
  - SAE – J 3061
  - IEEE
  - UL
  - ISO - 26262
  - NIST
  - DHS/DOT - ISACs

Requirements & Standards Are A Significant Gap

Penetration Testing

- Test Equipment Expanding
  - Hardware > 25 off the shelf systems
  - Software Toolsets – Vehicle Spy
- Trends
  - Consultant Segmentation
  - More in-house capability
  - AI-based (learning upon previous systems)
- Significant Role for Public Private Partnerships
  - Cryptology
  - Pen-Team Metrics & Training
  - Hack-a-thons
  - Ecosystem Support (Joint TARDEC/Industry Center)
  - Validation



Pen-Testing Breaks Down the Silo's between Requirements and Results

Infrastructure

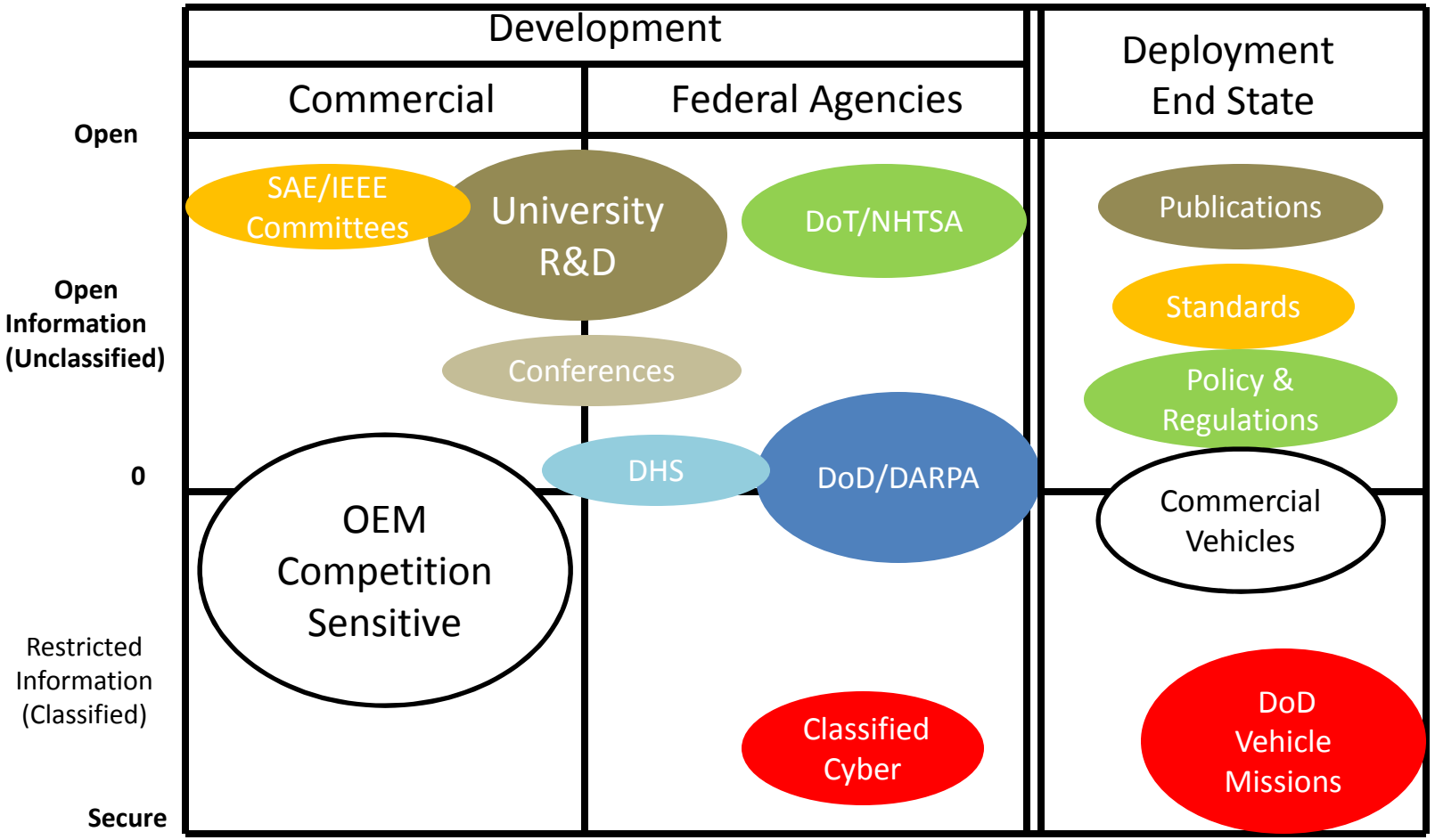
The Emerging "Hard Problem" in this Century

- **Vast Transportation Infrastructure Ecosystem**
  - High Future Growth and Increasing Efficiency Dependence
  - 5- 10X Complexity of Vehicle Cyber Security
  - Previous Studies Identified Major Cyber Security Issues
    - Mixture of Public & Private Systems (Passenger, Fleet, 1st Responder)
    - Old and New Architectures (Signage, V2X, etc)
    - Data Integrity
    - Communication Security

- **Assignment of End-to-End Responsibility Needed (Key Issue)**
  - Whose Problem is It? – DHS or DOT or State , Local or Private ?
  - Retro/Forward-fit vs Forward-fit only
  - Approach – Constructive, Operational, Reactive
  - Confidence Building Pilots/Demonstrations Required

Infrastructure Security is a Long-Cycle Problem

Development & Deployment "Ecosystem" of Organizations



Commercial/Military Vehicle Pathfinder Study

- Delphi-based Study four task areas:
  - Current Status of Commercial & Military Truck and Tier Supplier Cyber Security Capabilities for current and near term products
  - Pending Federal (DoD, DOT, DHS, FCC) technical and acquisition requirements that require changes to the OEM/Supplier ecosystem
  - Identify the Workforce Development and Education gaps that must be overcome to meet the requirements
  - Identify the R&D strategies that encourage and reduce the cybersecurity gap reduction for Commercial and Military Truck development and operations.