Cyber Security R&D Challenges

A Perspective from DHS

Homeland Security

Science and Technology

January 10, 2017

Dr. Dan Massey

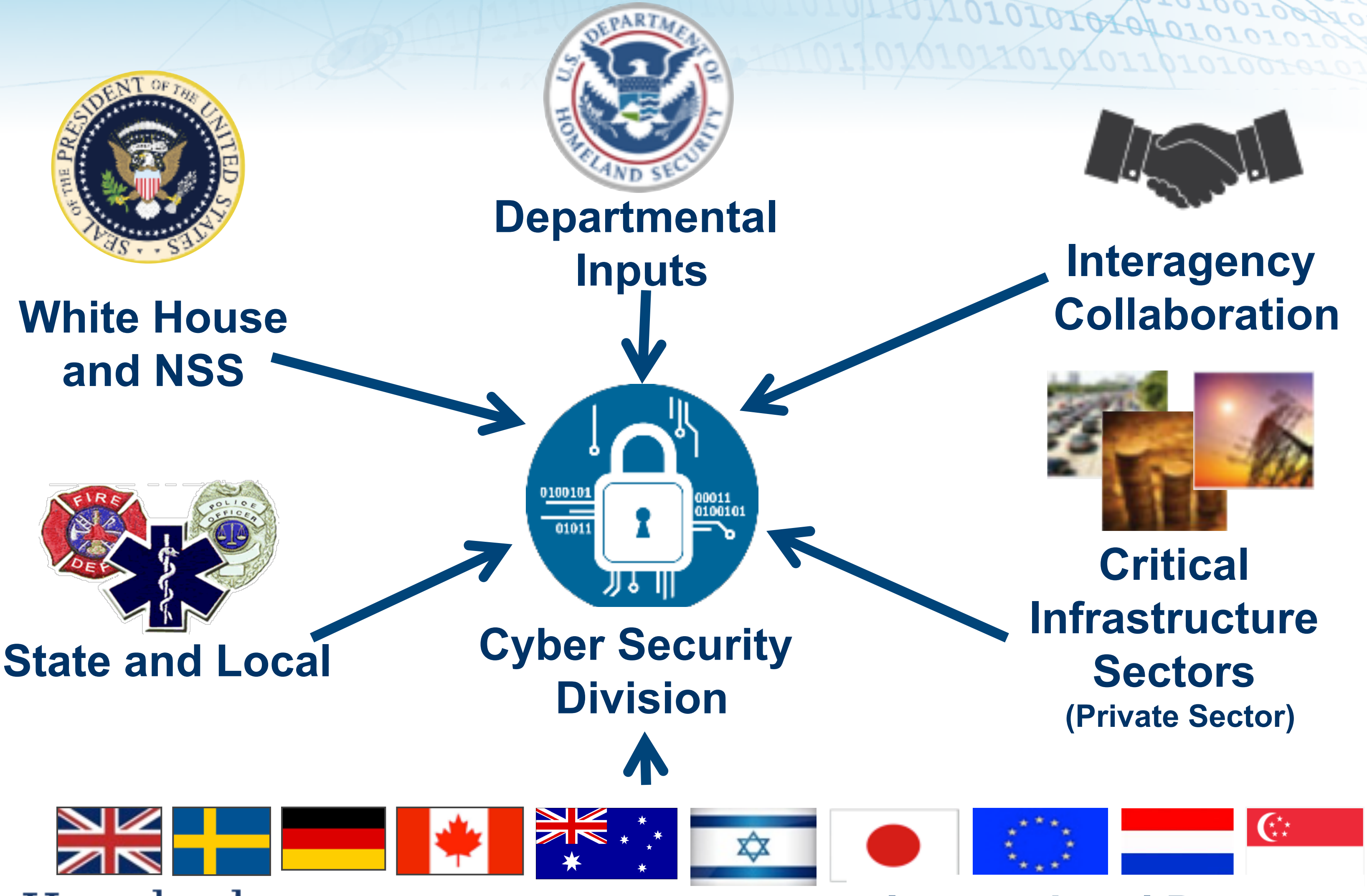
Program Manager
Cyber Security Division
Science and Technology Directorate

2016 Federal Cybersecurity R&D Strategic Plan

- Critical Areas:
  - Scientific Foundations
  - Human Aspects
  - Transitioning Successful Research into Pervasive Use
  - Enhancing the Infrastructure for Research.
  - Enhancements in Risk Management
  - Workforce development

- Recommendations
  - Prioritize basic and long-term research in Federal cybersecurity R&D.
  - Lower barriers and strengthen incentives for public and private organizations that would broaden participation in cybersecurity R&D.
  - Assess barriers and identify incentives that could accelerate the transition of evidence-validated effective and efficient cybersecurity research results into adopted technologies, especially for emerging technologies and threats.
  - Expand the diversity of expertise in the cybersecurity research community.
  - Expand diversity in the cybersecurity workplace.

DHS S&T RESEARCH REQUIREMENT INPUTS



White House and NSS

Departmental Inputs

Interagency Collaboration

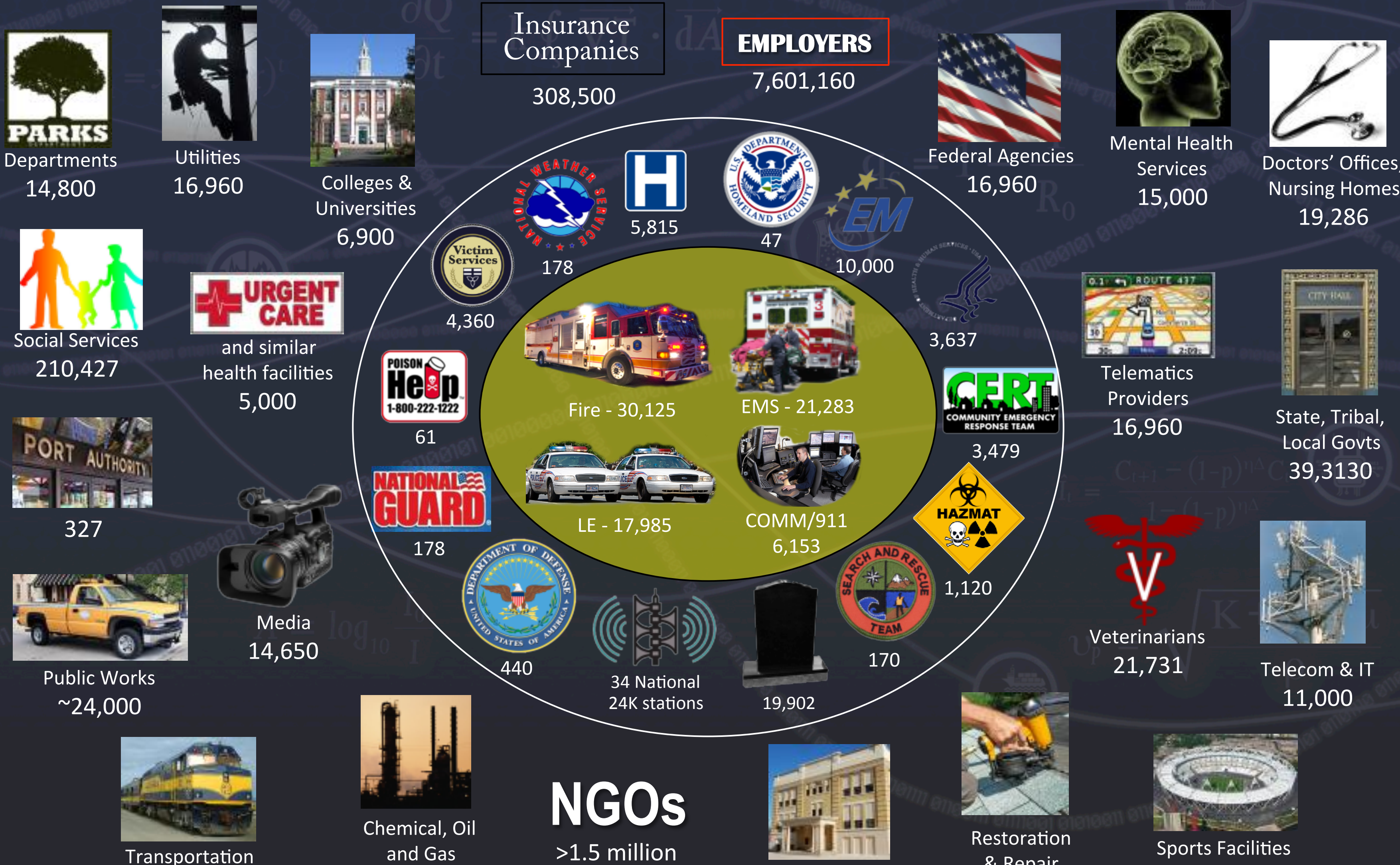
State and Local

Cyber Security Division

Critical Infrastructure Sectors
(Private Sector)

International Partners

The Broad Homeland Security Enterprise



Parks Departments 14,800

Utilities 16,960

Colleges & Universities 6,900

Insurance Companies 308,500

EMPLOYERS 7,601,160

Federal Agencies 16,960

Mental Health Services 15,000

Doctors' Offices, Nursing Homes 19,286

Social Services 210,427

URGENT CARE and similar health facilities 5,000

Port Authority 327

Media 14,650

Public Works ~24,000

Transportation 217,926

Chemical, Oil and Gas 2,500

NGOs >1.5 million

Schools 132,656

Restoration & Repair 402,440

Sports Facilities 1,965

Telecom & IT 11,000

Veterinarians 21,731

State, Tribal, Local Govts 39,3130

Telematics Providers 16,960

National Weather Service 178

Hospitals 5,815

U.S. Department of Homeland Security 47

EM 10,000

Victim Services 4,360

Health & Human Services 3,637

Poison Help 1-800-222-1222 61

CERT Community Emergency Response Team 3,479

National Guard 178

HAZMAT 1,120

Department of Defense 440

34 National 24K stations

19,902

Search and Rescue Team 170

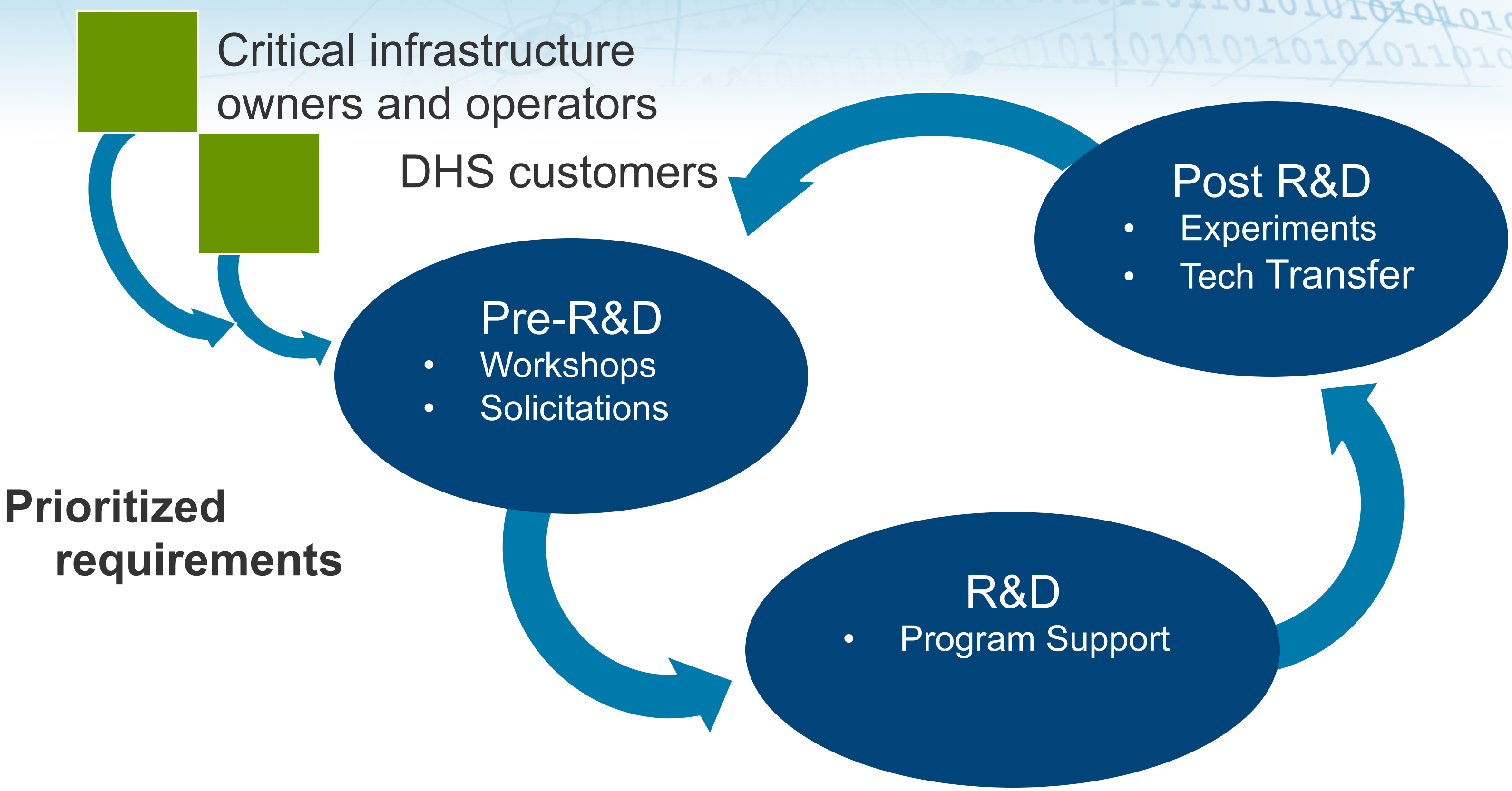
Fire - 30,125

EMS - 21,283

LE - 17,985

COMM/911 6,153

CSD R&D EXECUTION MODEL



Critical infrastructure owners and operators

DHS customers

Prioritized requirements

Pre-R&D
- Workshops
- Solicitations

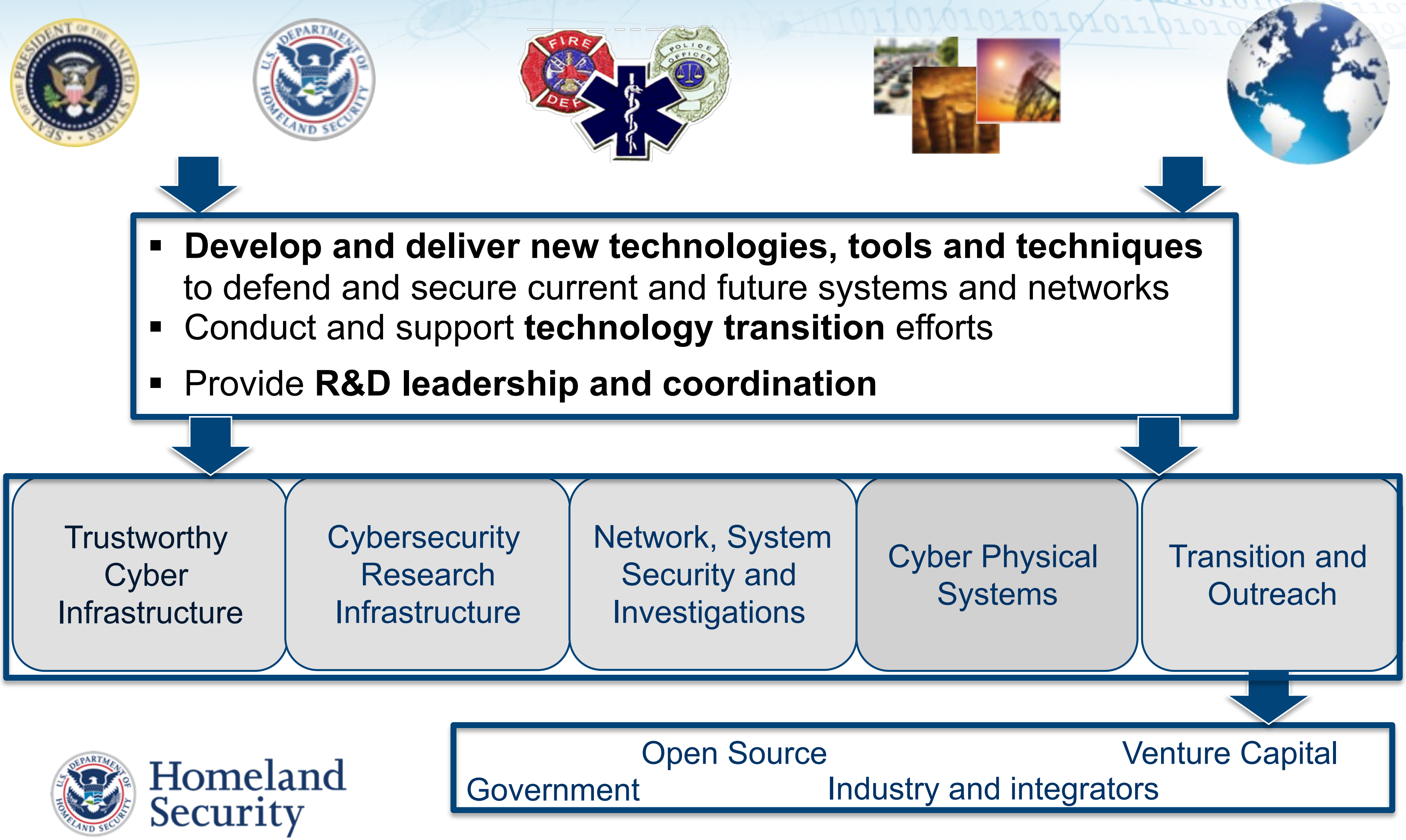
R&D
- Program Support

Post R&D
- Experiments
- Tech Transfer

"Crossing the 'Valley of Death': Transitioning Cybersecurity Research into Practice,"
IEEE *Security & Privacy*, March-April 2013,
Maughan, Douglas; Balenson, David; Lindqvist, Ulf; Tudor, Zachary
http://www.computer.org/portal/web/computingnow/securityandprivacy

Homeland Security
Science and Technology

CYBER SECURITY DIVISION MISSION



- **Develop and deliver new technologies, tools and techniques** to defend and secure current and future systems and networks
- Conduct and support **technology transition** efforts
- Provide **R&D leadership and coordination**

Trustworthy Cyber Infrastructure

Cybersecurity Research Infrastructure

Network, System Security and Investigations

Cyber Physical Systems

Transition and Outreach

Open Source
Government
Industry and integrators
Venture Capital

Program Manager Discussion	Recurring Solicitation
Fed Only Review	Panel of Your Peers
Thumbs Up/Down Decision	Panel Review and Summary
Contract	Grant
Stateful	Stateless
Shared International funding	International partner
Industry Partner or Lead	Industry Support Letter
Tech Transition	Broader Impacts

Homeland Security

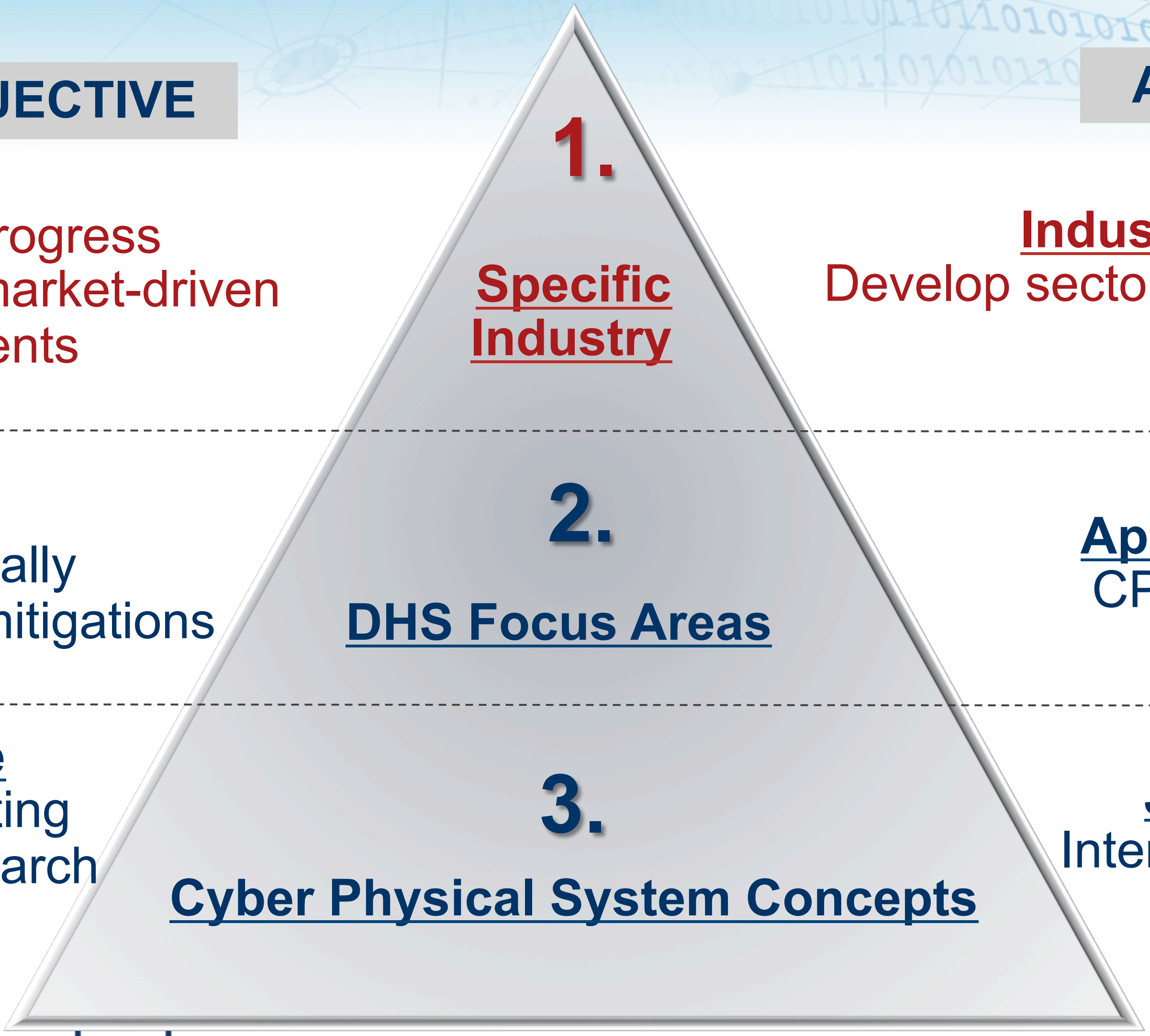
Science and Technology

Heilmeier Questions

- What are you trying to do? Articulate your objectives using absolutely no jargon.
- How is it done today, and what are the limits of current practice?
- What is new in your approach and why do you think it will be successful?
- Who cares? If you succeed, what difference will it make?
- What are the risks?
- How much will it cost?
- How long will it take?
- What are the mid-term and final “exams” to check for success?

Homeland Security
Science and Technology

CPS SECURITY PYRAMID



OBJECTIVE

APPROACH

1. **Specific Industry**

Enable progress through market-driven requirements

Industry Consortium
Develop sector-specific groups

2. **DHS Focus Areas**

Develop economically feasible mitigations

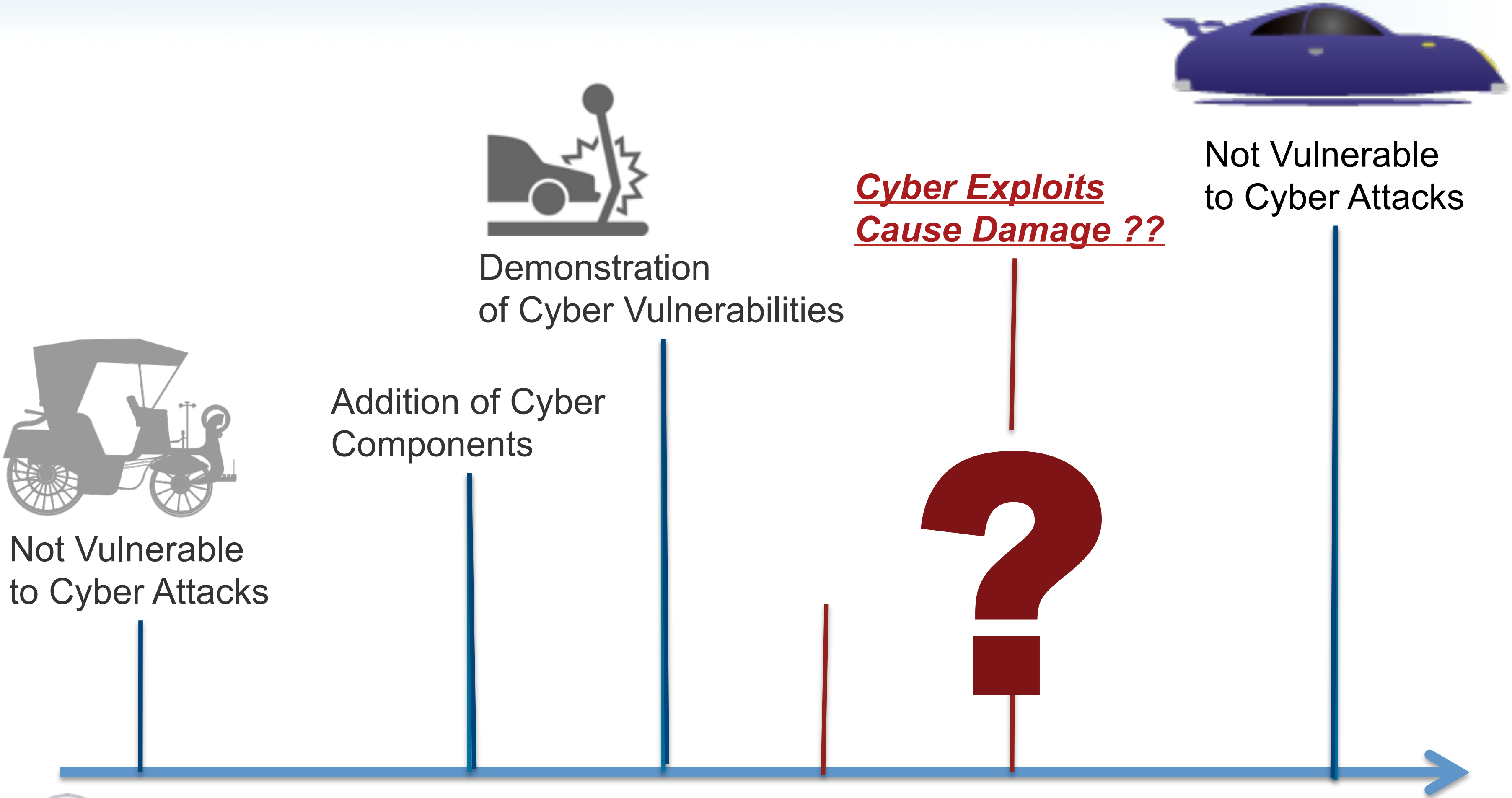
Applied Research
CPSSEC Program

3. **Cyber Physical System Concepts**

Leverage cross-cutting CPS research

Joint Research
Inter-Agency Efforts

Why Is The DHS S&T *Cyber Security Division* Looking at Vehicles?



Not Vulnerable to Cyber Attacks

Addition of Cyber Components

Demonstration of Cyber Vulnerabilities

Cyber Exploits Cause Damage ??

Not Vulnerable to Cyber Attacks

You are Here

THE DAILY NEWS

Thursday, April 16, 2018 THE WORLD'S FAVORITE NEWSPAPER $1.25

CHAOS AND TERROR

Cyber-Sabotaged Fire Trucks Crash Into Bombing Scene

Fire trucks responding to the bombing scene careened out of control after being sabotaged in apparent cyber attacks.

At least 20 people are dead and hundreds are injured in what appears to be a coordinated terrorist attack. Fire trucks and police units rushing down city streets to the scene of a downtown car bombing had their brakes and steering remotely disabled by cyber attacks.

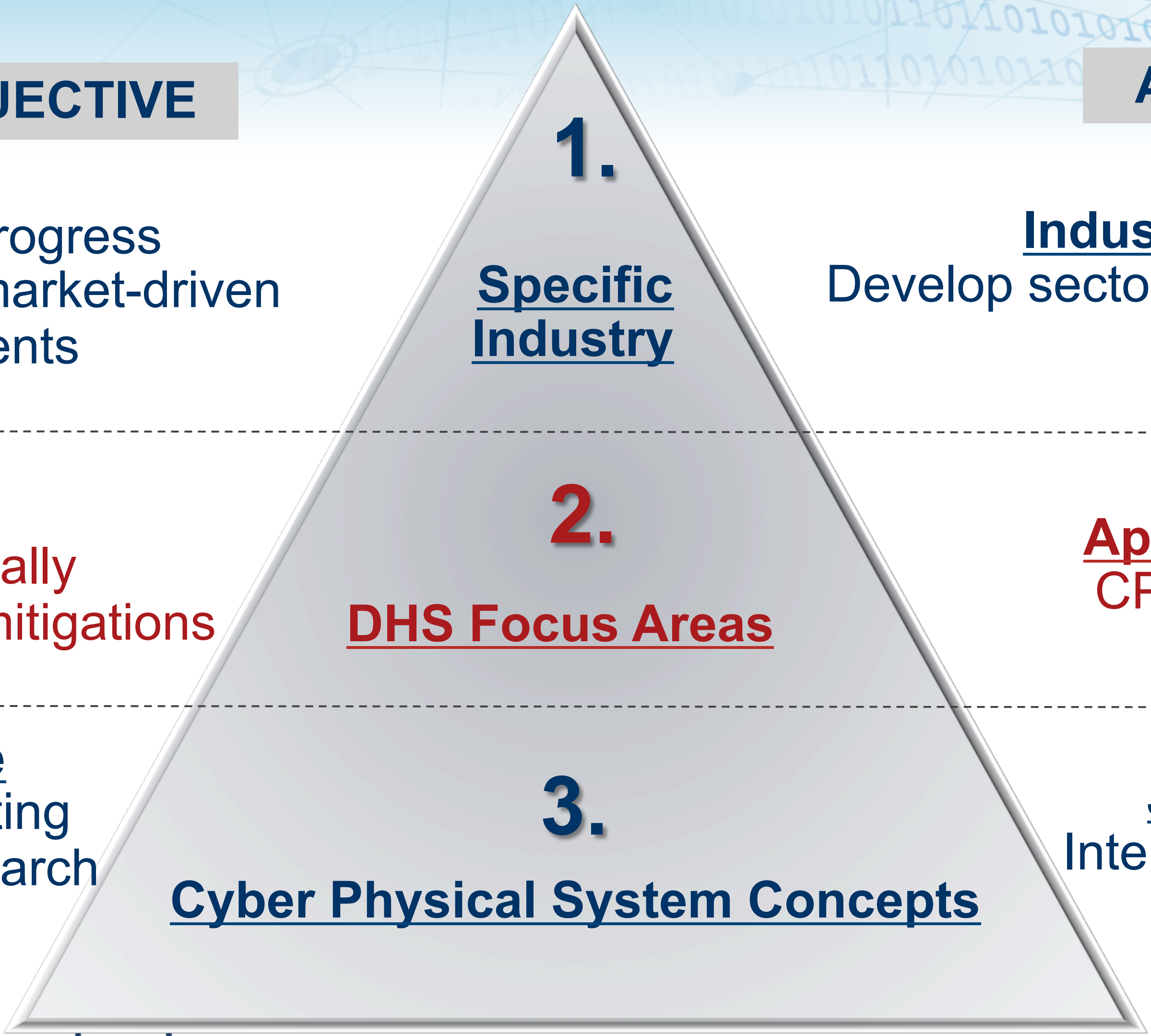
Hundreds of bomb victims lay injured in the streets waiting for hours for help and many died because they did not get to a hospital in time.

According to police sources, officials have been aware for some time that emergency vehicles could be vulnerable to remote "car hacking" attacks but they did not consider it a likely terrorist threat.

GOVERNMENT CRITICIAL MISSION USE

- First responder and law enforcement vehicles – fire, rescue, ambulance, police
  - Must be safe and reliable
- Undercover vehicles – mission critical
  - Must be safe and reliable
  - Blend in – not tracked or identified either by emanating too much or by not emanating at all
- Government official / overseas embassy vehicles (e.g., "Black SUV")
  - Must be safe and reliable but does not need to hide

CPS SECURITY PYRAMID



OBJECTIVE

APPROACH

Enable progress through market-driven requirements

1. **Specific Industry**

Industry Consortium
Develop sector-specific groups

Develop economically feasible mitigations

2. **DHS Focus Areas**

Applied Research
CPSSEC Program

Leverage cross-cutting CPS research

3. **Cyber Physical System Concepts**

Joint Research
Inter-Agency Efforts

CYBER PHYSICAL SYSTEM SECURITY BAA

Automotive Cyber Security

UMTRI
UNIVERSITY OF MICHIGAN
TRANSPORTATION RESEARCH INSTITUTE

HRL LABORATORIES

NYU

NICTA

SwRI

UCIRVINE

Medical Device Cyber Security

MDISS
Medical Device Innovation, Safety, & Security Consortium

Adventium LABS

KANSAS STATE UNIVERSITY

MICHIGAN

Building Infrastructure Cyber Security

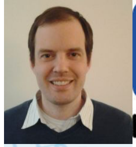
KANSAS STATE UNIVERSITY

Honeywell

USF UNIVERSITY OF SOUTH FLORIDA

UMTRI UNIVERSITY OF MICHIGAN TRANSPORTATION RESEARCH INSTITUTE

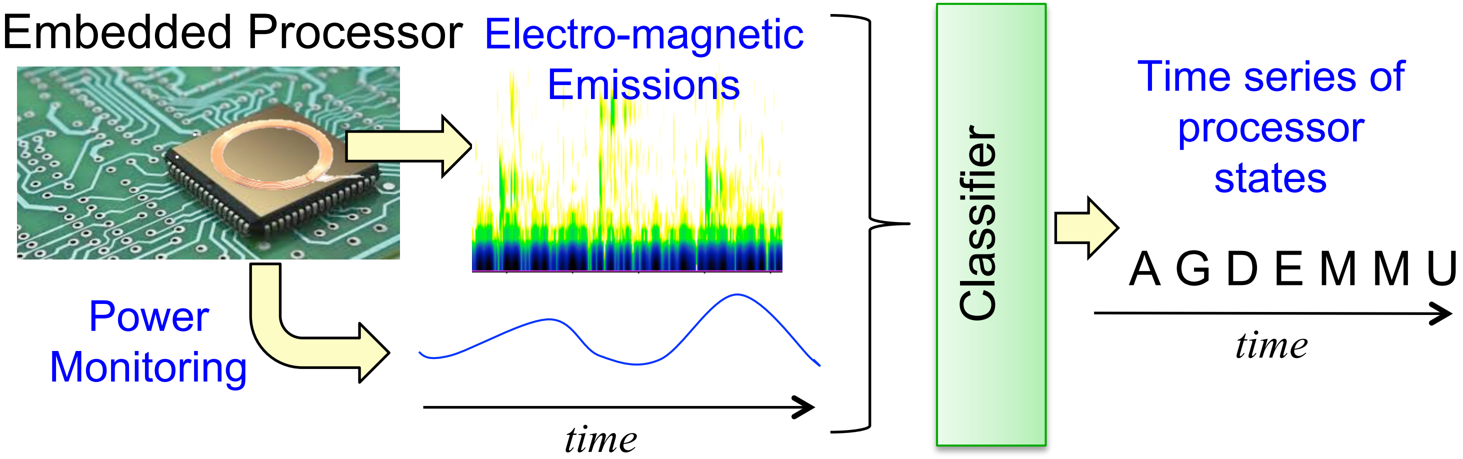
NYU



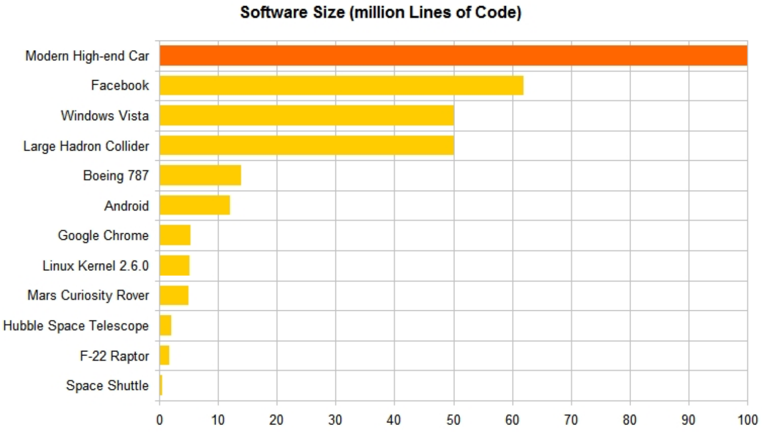
HRL LABORATORIES

BAA Efforts on Security for Automobiles

- Side Channels to Detect Faults

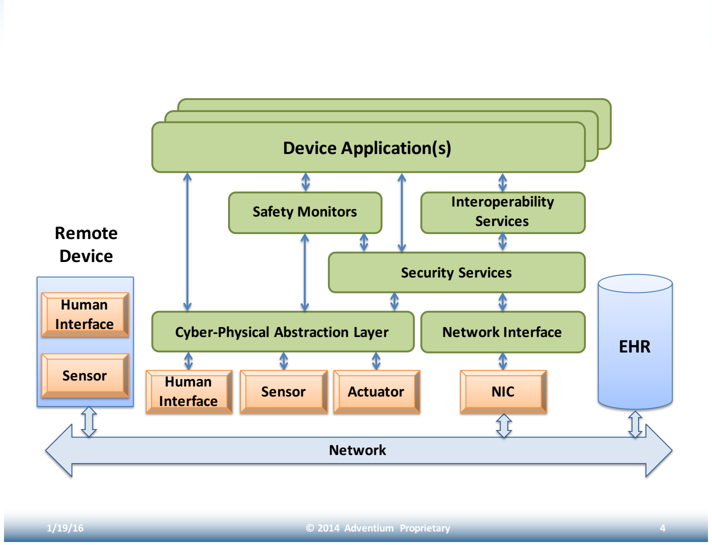


- Secure Updates for Vehicles
  - 40 Key players including Tier 1 suppliers and OEMs in newly formed working group
  - Updates essential to improving security
  - Updates done incorrectly add new vector for attack.

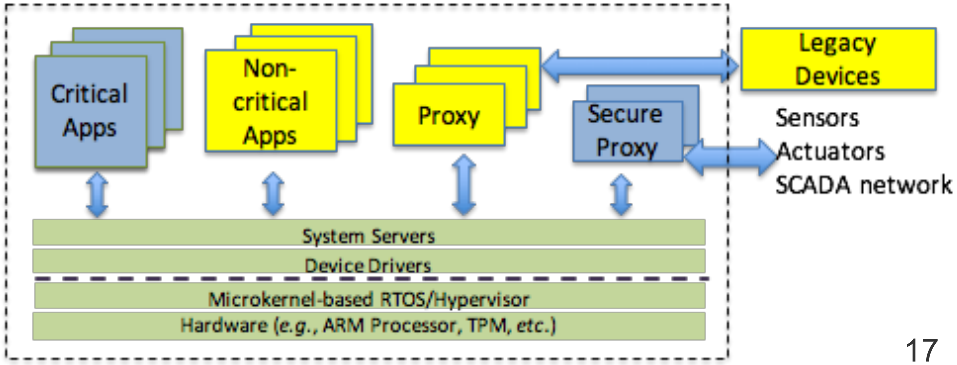


BAA Efforts on Medical and Buidlings

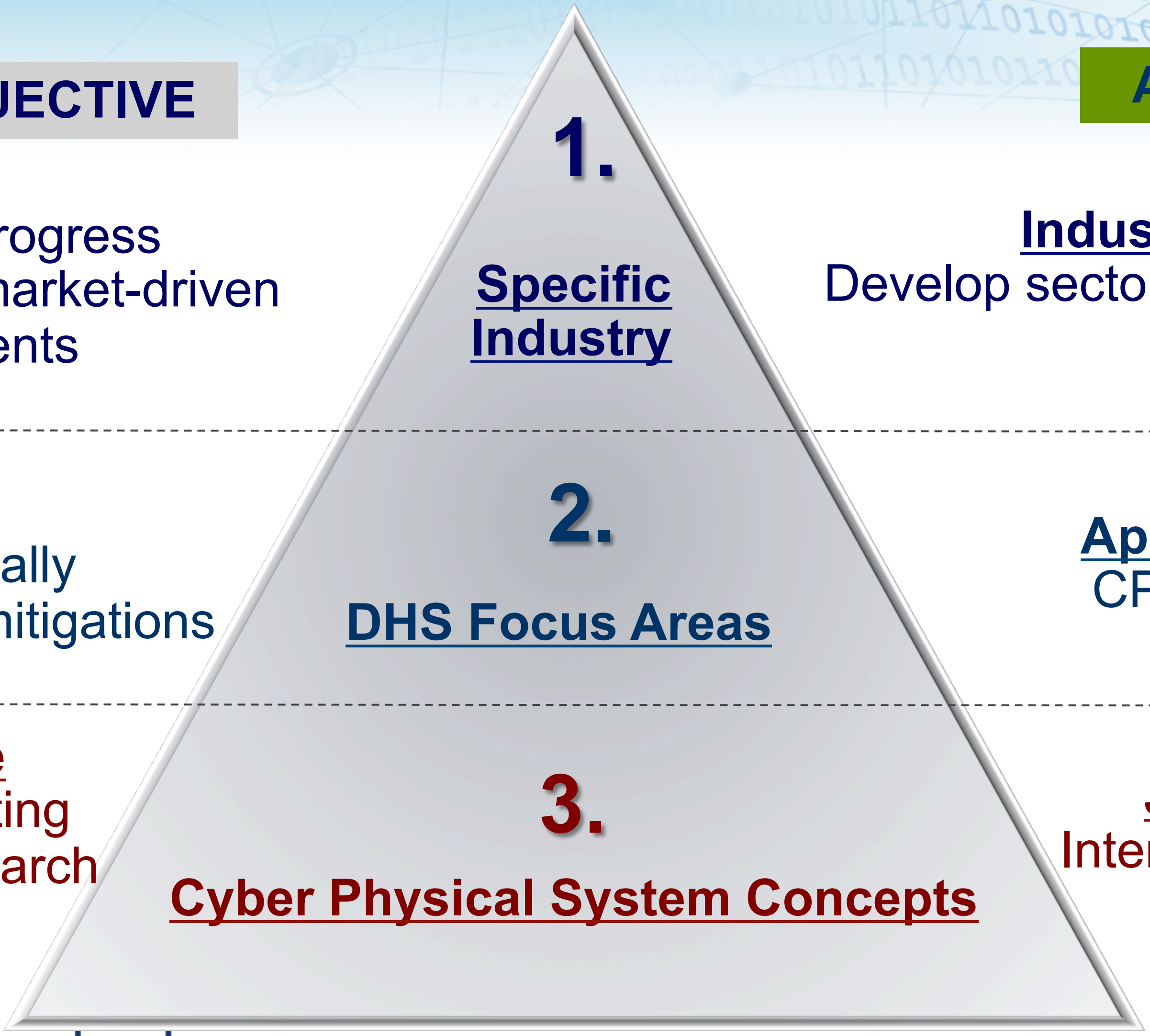
- Separation and Isolation Techniques for Medical Devices
- **Outreach to device makers and hospitals**
- **Anticipate Joint Funding with Israel and Sweden**



- Secure for Building Controls
- Secure Real Time Operating System Concepts
- **Joint Funding with UK**
- **Hospitals, Bioresearch, offices, malls**



CPS SECURITY PYRAMID



OBJECTIVE		APPROACH
Enable progress through market-driven requirements	1. **Specific Industry**	**Industry Consortium** Develop sector-specific groups
Develop economically feasible mitigations	2. **DHS Focus Areas**	**Applied Research** CPSSEC Program
Leverage cross-cutting CPS research	3. **Cyber Physical System Concepts**	**Joint Research** Inter-Agency Efforts

Homeland Security

Science and Technology

JOINT RESEARCH WITH US NATIONAL SCIENCE FOUNDATION

NSF Joint Solicitation Efforts

Researchers submit proposals that the NSF fundamental science mission with the DHS applied research and transition to practice mission

SCADA/Energy Testbed

Manimaran Govindarasu

Smart Grid Security

Lalitha Sankar & Robin Podmore

Smart Manufacturing

Jamie Camelio & Jules White

Homeland Security

Science and Technology

Homeland Security

Science and Technology