25th anniversary
annual INCOSE
international symposium
Seattle, WA
July 13 - 16, 2015

Critical Infrastructure Protection and Recovery (CIPR) Working Group

July 2015

Mike deLamare,

Loren Mark Walker,
John Juhasz

Topics

- Introductions
- The High Impact Threats (Solar (CME/GMD), EMP and Cyber)
- Critical Infrastructure Perspectives
- CIPR Working Group
  - Purpose and Goals
  - Products and Services
  - INCOSE WGs that can be involved
- Upcoming Events
- Open Discussion

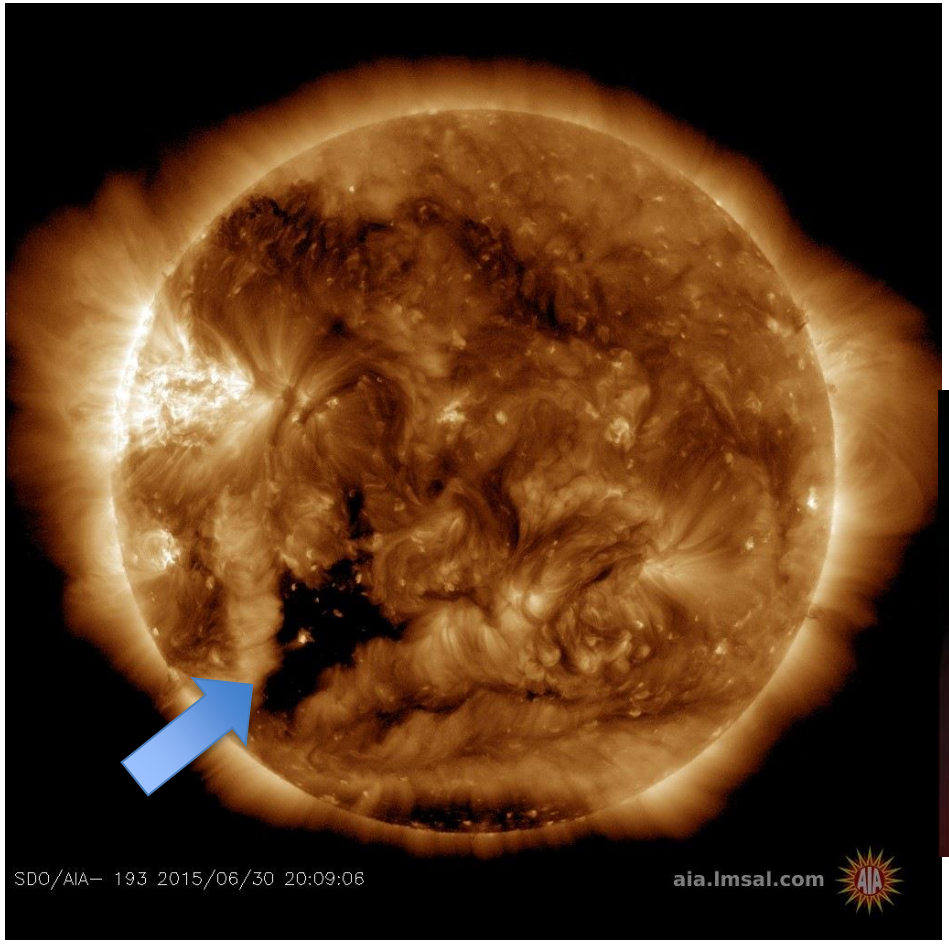
THE HIGH IMPACT THREATS TO POWER GRID (SOLAR, EMP AND CYBER)

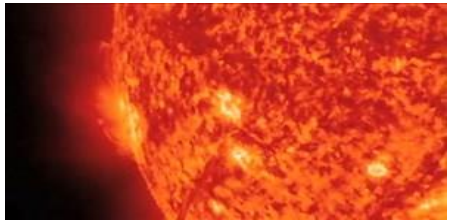
BACKGROUND INFORMATION

25th anniversary annual INCOSE international symposium
Seattle, WA
July 13 - 16, 2015

Solar Flares (Coronal Mass Ejections (CME)/Geomagnetic Disturbances (GMD))

Solar wind flowing from the indicated coronal hole should reach Earth on July 6-7. Credit: SDO/AIA.





[Raw Video: NASA Captures Dramatic Solar Flare]

Solar Flare Will Probably Trigger Northern Lights
June 24, 2015 5:13 PM

1:07
Raw Video: NASA Captures Dramatic Solar Flare

Growing Threat From an EMP Attack

- **James Woolsey**
  12th August 2014 - The Wall Street Journal
- ***Co-authored with Peter Vincent Pry***
- **In a recent letter to investors, billionaire hedge-fund manager Paul Singer warned that an electromagnetic pulse, or EMP, is "the most significant threat" to the U.S. and our allies in the world. He's right. Our food and water supplies, communications, banking, hospitals, law enforcement, etc., all depend on the electric grid. Yet until recently little attention has been paid to the ease of generating EMPs by detonating a nuclear weapon in orbit above the U.S., and thus bringing our civilization to a cold, dark halt.**
- **Recent declassification of EMP studies by the U.S. government has begun to draw attention to this dire threat. Rogue nations such as North Korea (and possibly Iran) will soon match Russia and China and have the primary ingredients for an EMP attack: simple ballistic missiles such as Scuds that could be launched from a freighter near our shores; space-launch vehicles able to loft low-earth-orbit satellites; and simple low-yield nuclear weapons that can generate gamma rays and fireballs.**
- **The much neglected 2004 and 2008 reports by the congressional EMP Commission—only now garnering increased public attention—warn that "terrorists or state actors that possess relatively unsophisticated missiles armed with nuclear weapons may well calculate that, instead of destroying a city or a military base, they may gain the greatest political-military utility from one or a few such weapons by using them—or threatening their use—in an EMP attack……..."**
- **- See more at: http://www.defenddemocracy.org/media-hit/r-james-woolsey-the-growing-threat-from-an-emp-attack/#sthash.dVtQAMDz.dpuf**

EMP defined (Wikipedia)

- An **electromagnetic pulse** (**EMP**), also sometimes called a transient electromagnetic disturbance, is a short burst of electromagnetic energy. Such a pulse may occur in the form of a radiated, electric or magnetic field or conducted electric current depending on the source, and may be natural or man-made. The term "electromagnetic pulse" is commonly abbreviated to the initialism **EMP** (which is pronounced by saying the letters separately, "E-M-P").
- EMP interference is generally disruptive or damaging to electronic equipment, and at higher energy levels a powerful EMP event such as a lightning strike can damage physical objects such as buildings and aircraft structures. The management of EMP effects is an important branch of electromagnetic compatibility (EMC) engineering.
- The damaging effects of high-energy EMP have been used to create EMP weapons. These are typically divided into nuclear and non-nuclear devices. Such weapons, both real and fictional, are becoming known to the public by means of popular culture.
- Types of EMP 2.1 Lightning
- 2.2 Electrostatic discharge (ESD)
- 2.3 Switching pulses
- 2.4 Nuclear (NEMP) and high altitude nuclear (HEMP)
- 2.5 Non-nuclear electromagnetic pulse (NNEMP)
- 2.6 Electromagnetic forming

Cyber-Attacks (Wikipedia)

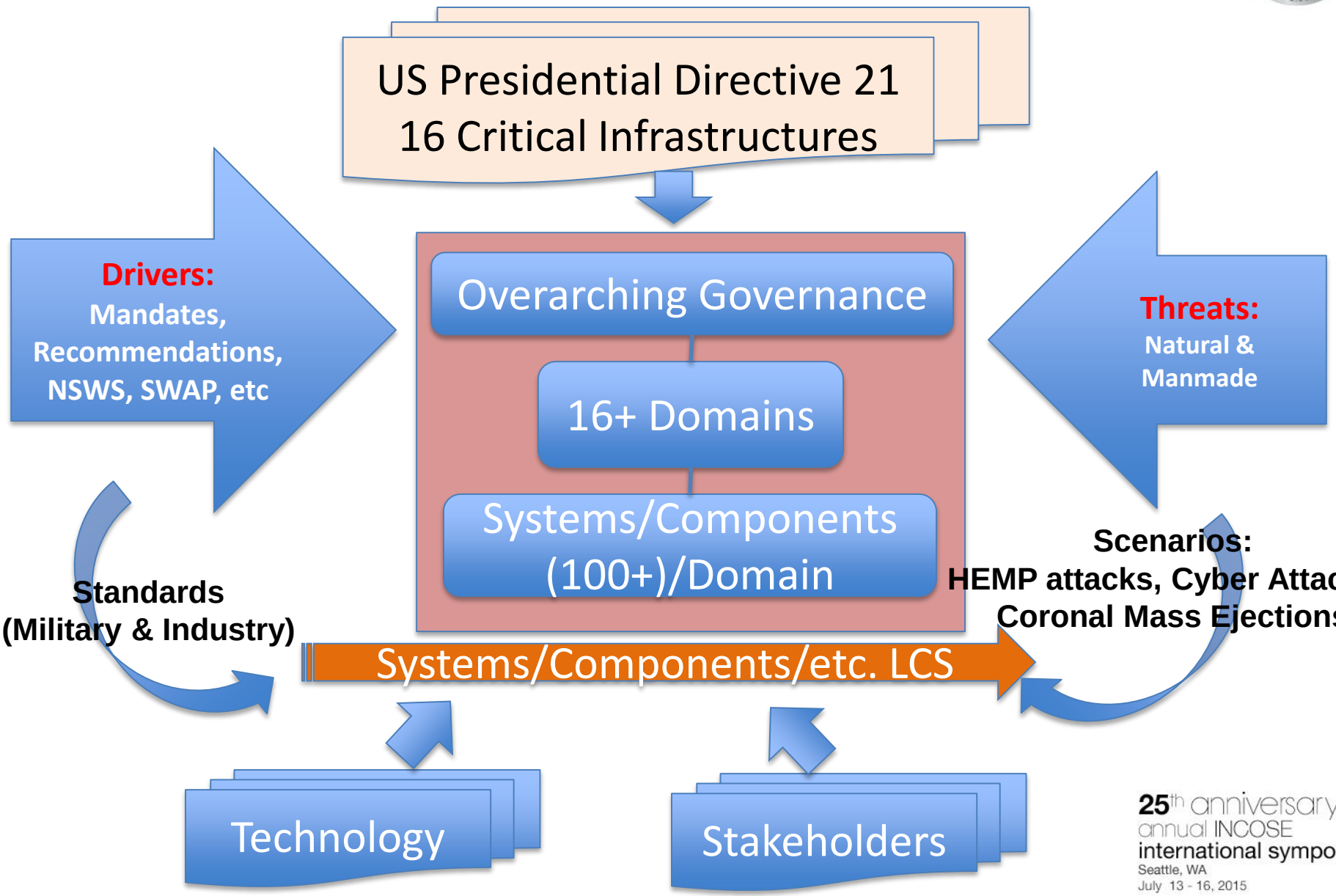
- ***Cyber-attack*** **is any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system. These can be labelled as either a Cyber campaign, cyberwarfare or cyberterrorism in different context. Cyber-attacks can range from installing spyware on a PC to *attempts to destroy the infrastructure of entire nations.* Cyber-attacks have become increasingly sophisticated and dangerous as the Stuxnet worm recently demonstrated.[1]**
- ***Cyberwarfare*** **utilizes techniques of defending and attacking information and computer networks that inhabit cyberspace, often through a prolonged Cyber campaign or series of related campaigns. It denies an opponent's ability to do the same, while employing technological instruments of war to attack an opponent's critical computer systems. *Cyberterrorism,* on the other hand, is "the use of computer network tools to *shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population.*"[2] That means the end result of both cyberwarfare and cyberterrorism is the same, *to damage critical infrastructures and computer systems linked together within the confines of cyberspace.***
- **Cohen Interview:**
- **http://www.newsmax.com/Newsfront/William-Cohen-defense-chief-terrorist-attack-power-grid/2015/06/29/id/652742/**

Other Cyber Related Issues

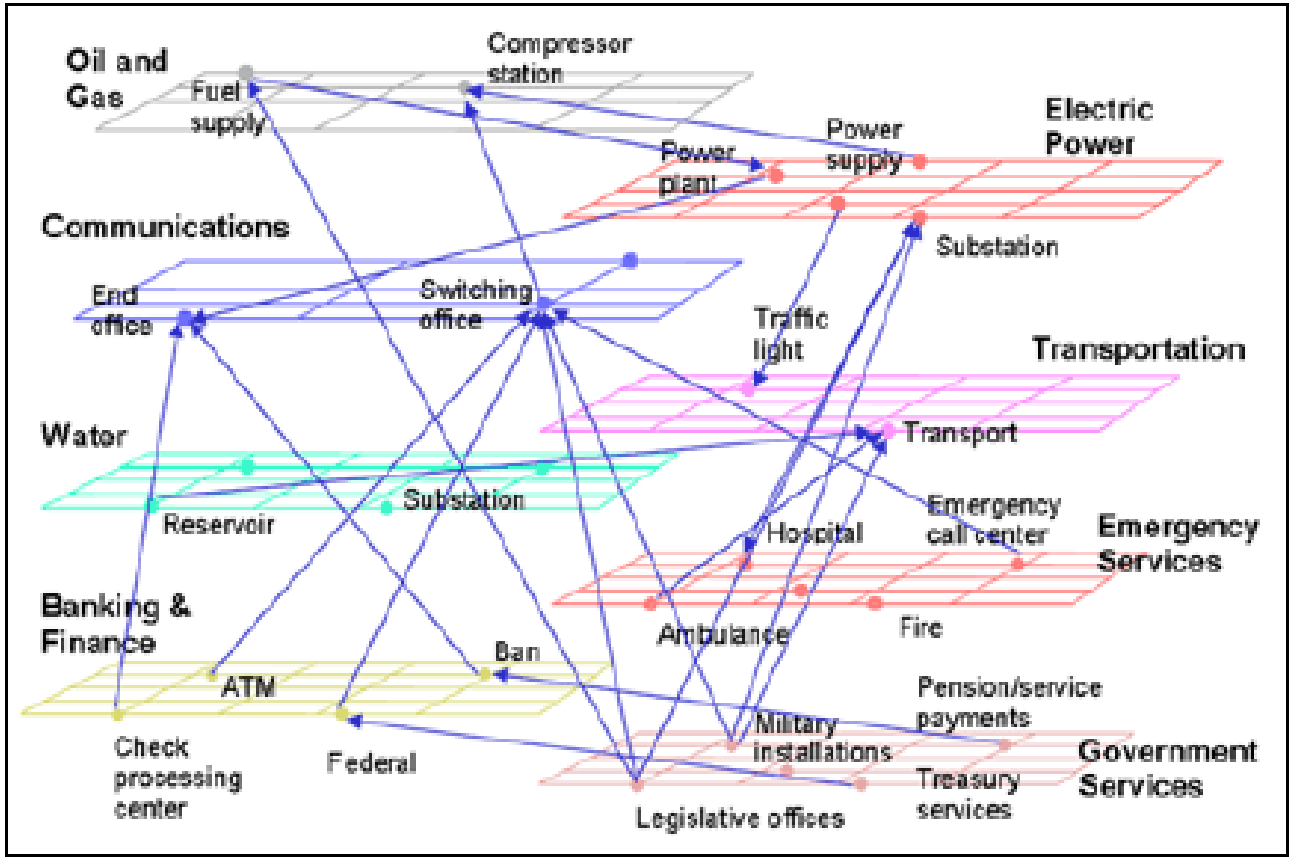
- Unintentional disruptions-
  - Accidental, software glitches, Human/HMI
- Non-IT attacks: Industrial Controls/Standards-
  - ISA 99, SCADA, NERC, etc.
- Design Errors
- Lack of full scope requirements
- Domain unique
- Interface Issues,
- IV&V, unique domain testing requirements
- Training, procedures, ….
- Etc.

CRITICAL INFRASTRUCTURE PERSPECTIVES

CIPR Environment/Context with SoS & Systems Engineering/Technical Perspective & Threats



Connections and interdependencies across the economy. Schematic showing selected interconnected infrastructures and their qualitative dependencies and interdependencies. Source: www.fcc.gov and EMP-SIG Exercise Read-Ahead_Final.pdf



Critical Infrastructure Domains

1) Chemical and other industrial bases
2) Communications
3) Electrical & Energy production and distribution
4) Emergency Services
5) Financial Services
6) Food and Agriculture
7) Government Services & Facilities
8) Healthcare and Public Health
9) Information Technology
10) Nuclear Reactors, Materials, and Waste
11) Transportation
12) Water storage, treatment and distribution
13) Waste handling and disposal (water, refuse, hazardous)
14) Society at large

CIPR WG Challenges

- Understanding critical infrastructure domains
- Understanding cross-domain interactions
- Understanding threats
- Gaining cooperation within and across domains
- Sensitivity of information
- Verifiability of concepts and solutions
- Rapid evolution of threats and domains
- Scale of the problem
- Capturing Information in SE products, architecture, requirements, life cycle, etc. to support decision makers

INCOSE's Challenge:

a Real World Problem that Needs Solutions!

CIPR WORKING GROUP

CIPR Purpose & Goals

- Provide a forum to address Critical Infrastructure Protection and Recovery (CIPR)
  - manmade and natural threats
  - disruptions for periods of a month or more.
  - systems engineering principles, practices, applications and solutions
- Exchange knowledge, systems engineering information and solutions regarding CIPR
- Develop systems engineering products (e.g. architectures, requirements, IV&V, etc.

CIPR WG provides Integration Among INCOSE WGs to provide products, support, etc.

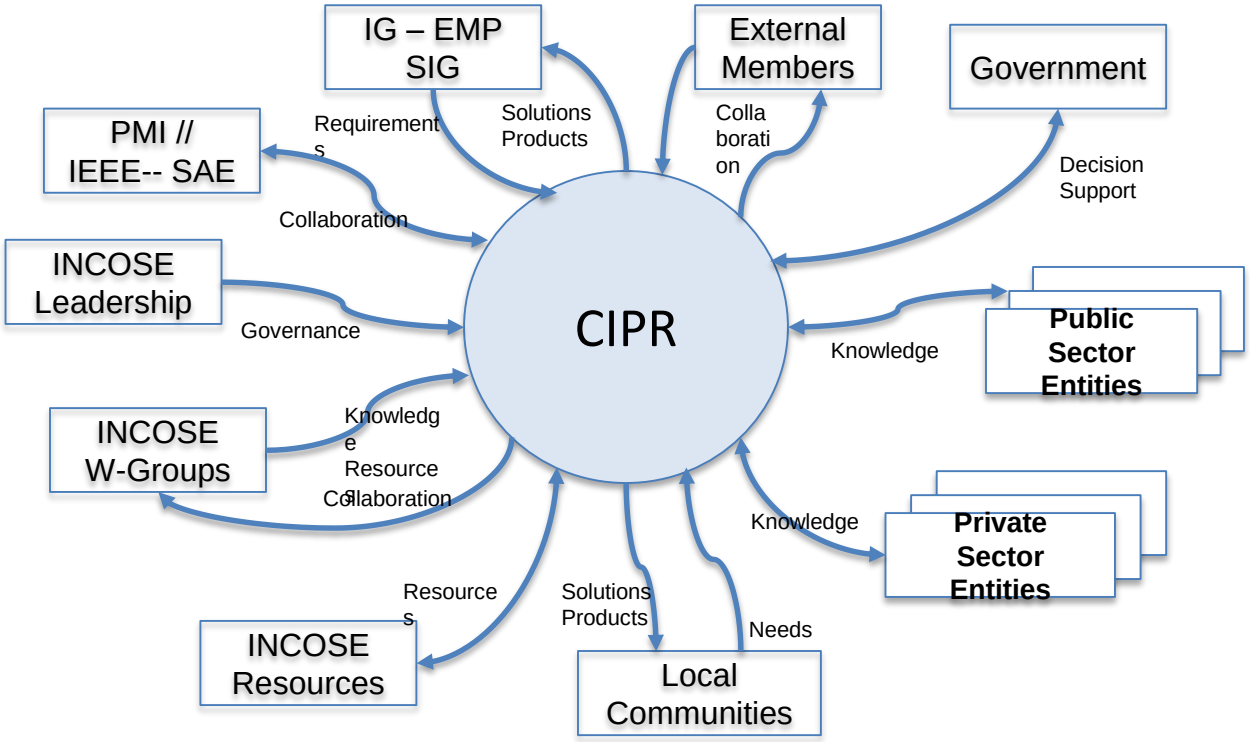
Products & Services

- National Reference Model for Systems and SoS
  - Domain-specific and Cross-domain
- Threat Models
- SE Products (architecture, recommendations)
- Pamphlets, Articles, Papers, Panels
- Tutorials, Training
- Information Distribution for Non-Sensitive Information
- Standards Modification and Development
- Conference Tracks
- Expert Assistance in Use of Products
- Reference Lists

INCOSE WGs that could be involved

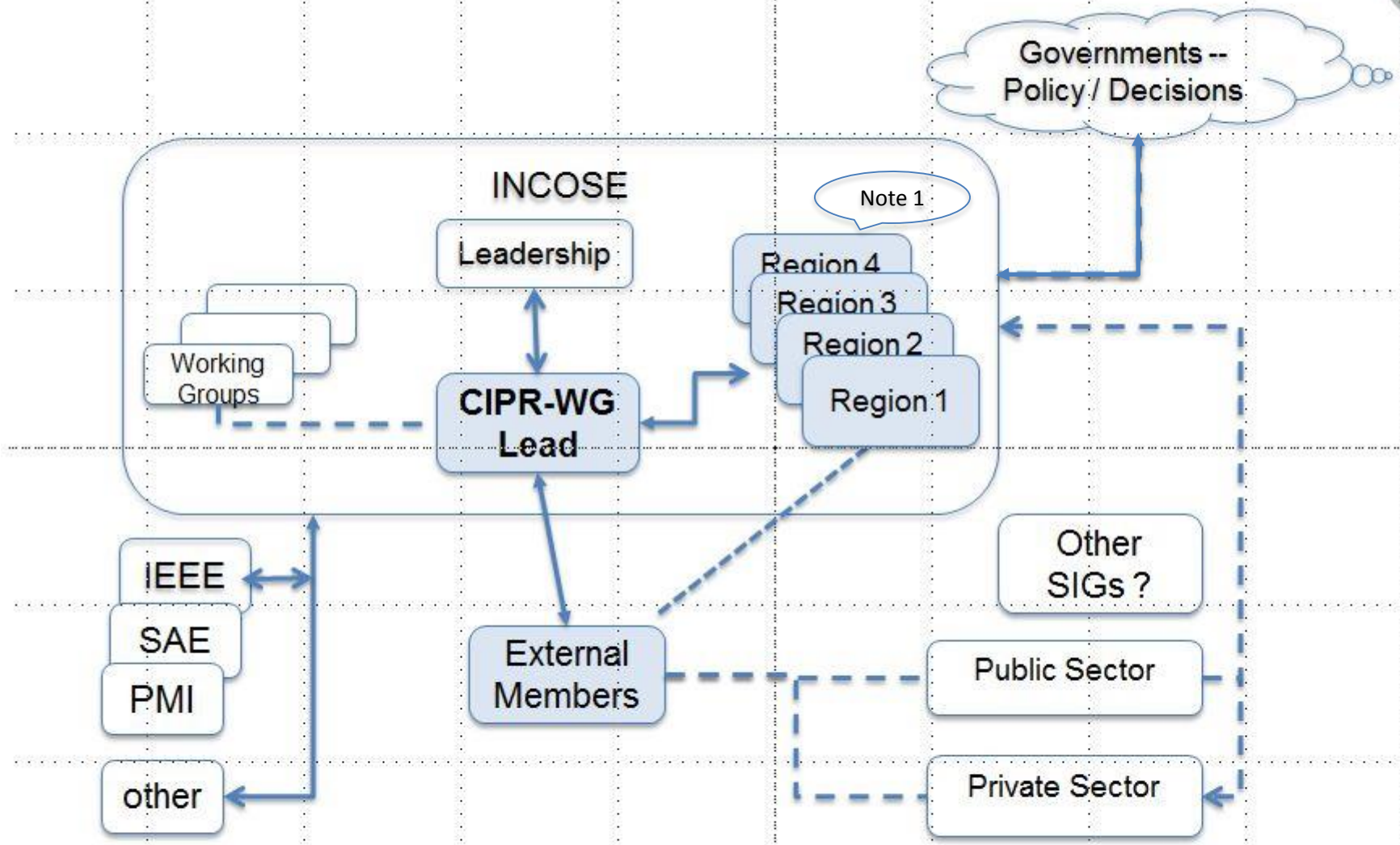
- Infrastructure- (Already Involved)
- Power and Energy Systems- (Already Involved)
- OOSEM (Already Involved)
- Anti-Terrorism Systems (Already Involved)
- Standards (ISA99, NIST 800, SCADA standards, etc.)
- SoS
- MBSE
- Architecture
- Requirements
- Risk Management
- Complex Systems
- Security
- Defense Systems
- Life Cycle Management
- Reliability
- Others?

CIPR – General Context Diagram



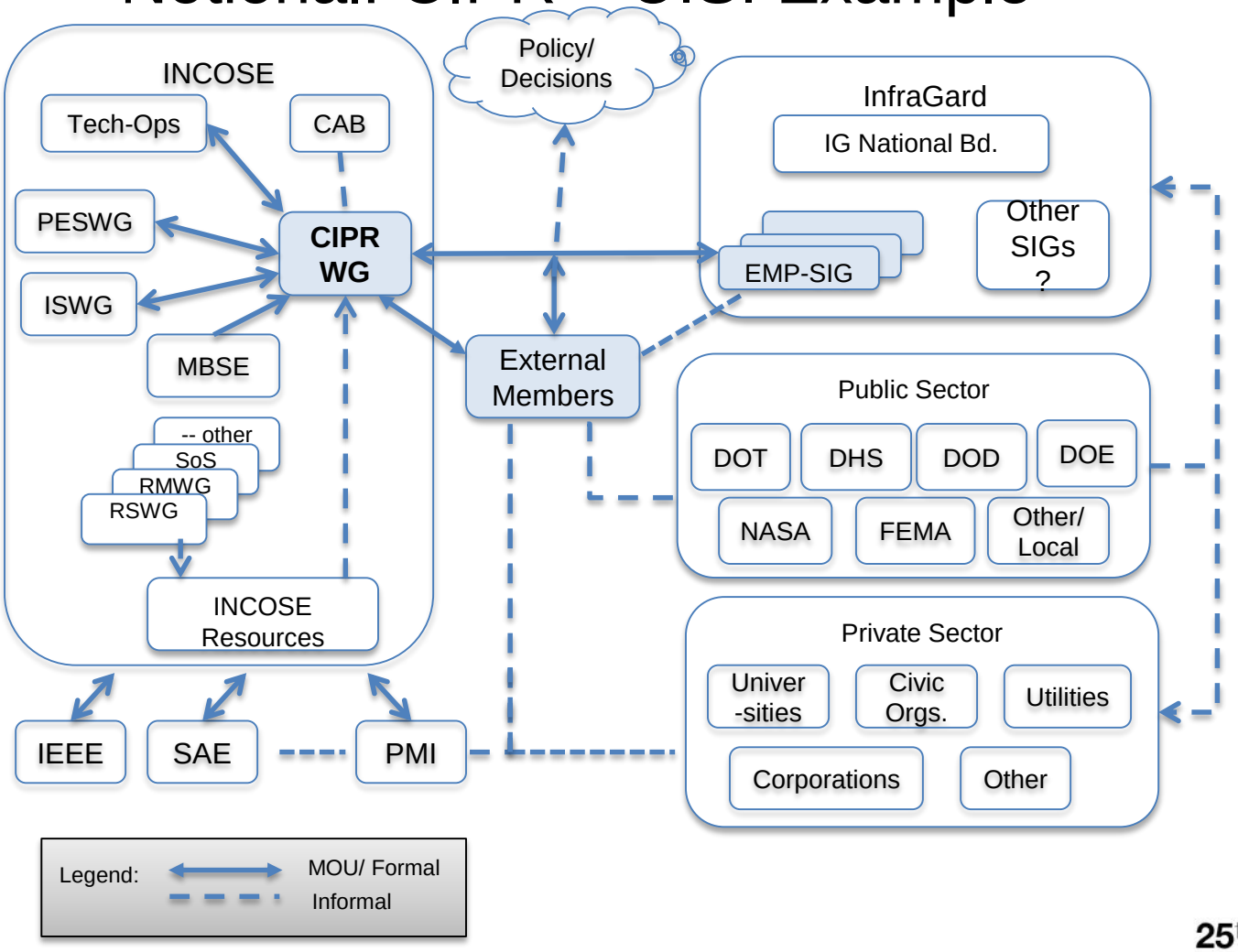
This diagram needs to be tailored to each Country or Region by a local CIPR sub-group

Notional: CIPR Relationships - Global



Note 1: Regional orgs may be based on country, geographical or other logical boundaries (TBD)

Notional: CIPR – U.S. Example

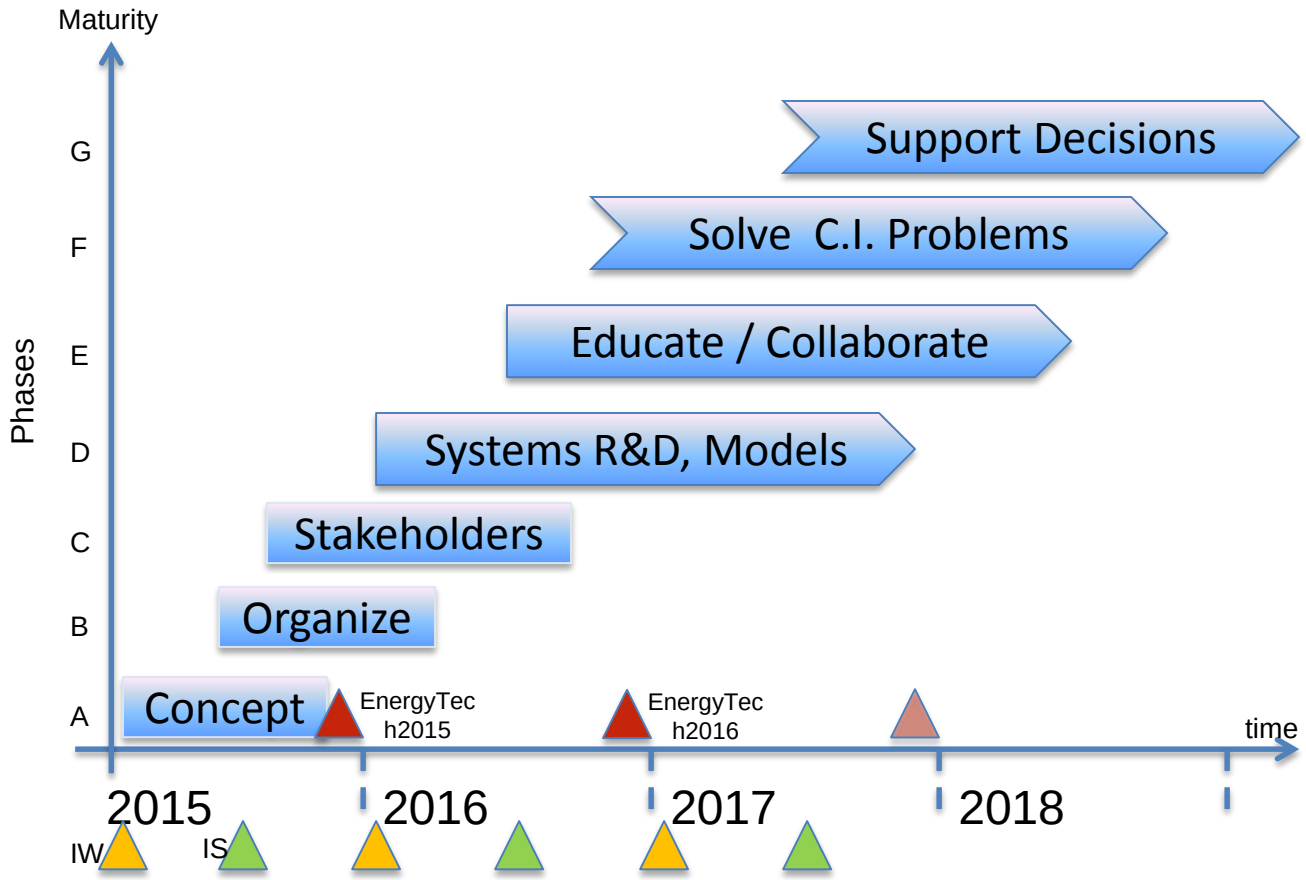


US Organizations Involved in EMP SIG

- DHS, DOD, DOE, DO Treasury, DO Transportation, EPA, DOA, DHHS, NOAA, (**Ref Presidential Directive 21**)
- National Weather Service Space Weather Prediction Center
- Policy Studies Organization (PSO)
- US National Governors Association….
- Foundation for Resilient Societies
- Congress Members
- Energy Security Program- National Defense University
- APL, Mitre, …..
- States (25 InfraGard Chapters)
  - Maryland, VA, Maine, North Carolina, NY, NJ, Connecticut, ….
- Universities:
  - James Madison, JHU, Univ of MD, US Army War College,
- Others ?

ROADMAP AND UPCOMING EVENTS

CIPR – Maturity Roadmap



CIPR-WG: Phases of Evolution

Φ	Life-cycle phase	Core Products
A	Conception	WG Charter
B	Organization	Structure, Governance Membership (Internal, External)
C	Stakeholder Engagement, Needs Threat & Recovery Scenarios	Seminars, Meetings, Conferences Needs >> Requirements Definition
D	R&D, Applied SE, Models	Critical Infrastructure Architecture Def. Fault behavior, Risk Assessment, etc. CI Reference Models; Resilient community models
E	Education & Collaboration	Publications, Briefings, Tutorials, Standards
F	Problem Solving	Policy Decision Support; MBSE Solutions SE Expertise; Resiliency recommendations
G	Ongoing	Decisions, decisions….

Upcoming Opportunities/Events

- WA State First Net Procurement Spec- 30Jul'15
- 25-27- Sep'15: Transformational SE Workshop- Global Energy Water Nexus (GWEN), Colorado (Bill Good)
- ICS Cybersecurity, Oct 26-29; Atlanta, GA (Joe Weiss)
- 30Nov'15: EnergyTech Conference, Cleveland, Ohio (John Juhasz)
- 3Dec'15: InfraGard, EMP-SIG, Washington DC (Chuck Manto)

OPEN DISCUSSION/SUGGESTIONS/ETC.

BACKUP CHARTS

Discussion Topics

- InfraGard's EMP SIG: Over 1 month shutdown of the US Electric Grid
- INCOSE Chapter Involvement with InfraGard's 25 US Chapters and States?
- Overview of Electromagnetic Pulse Sources:
  - Sun, Nuclear, Cyber, Others
- Impacts to various infrastructure industries/areas
- SoS perspectives, Family of systems, Systems & Components
- Federal, State, Local Communities, families/individuals
- Society/Social
- Protection & Recovery
- How should INCOSE and the Infrastructure WG be involved?
  - Many WGs can be involved
- Can interconnect these WGs to work towards understanding and solutions
- Way forward
- Infrastructure WG- Take the Lead for INCOSE?
- Interrelate to InfraGard's EMG SIG
- Act as POC for INCOSE WGs?
- International relationships?
- POCs?
- Discussion & Actions