EMERGENCY MANAGEMENT PLANNING

FOR

AMERICA'S CRITICAL INFRASTRUCTURE

INFRAGARD

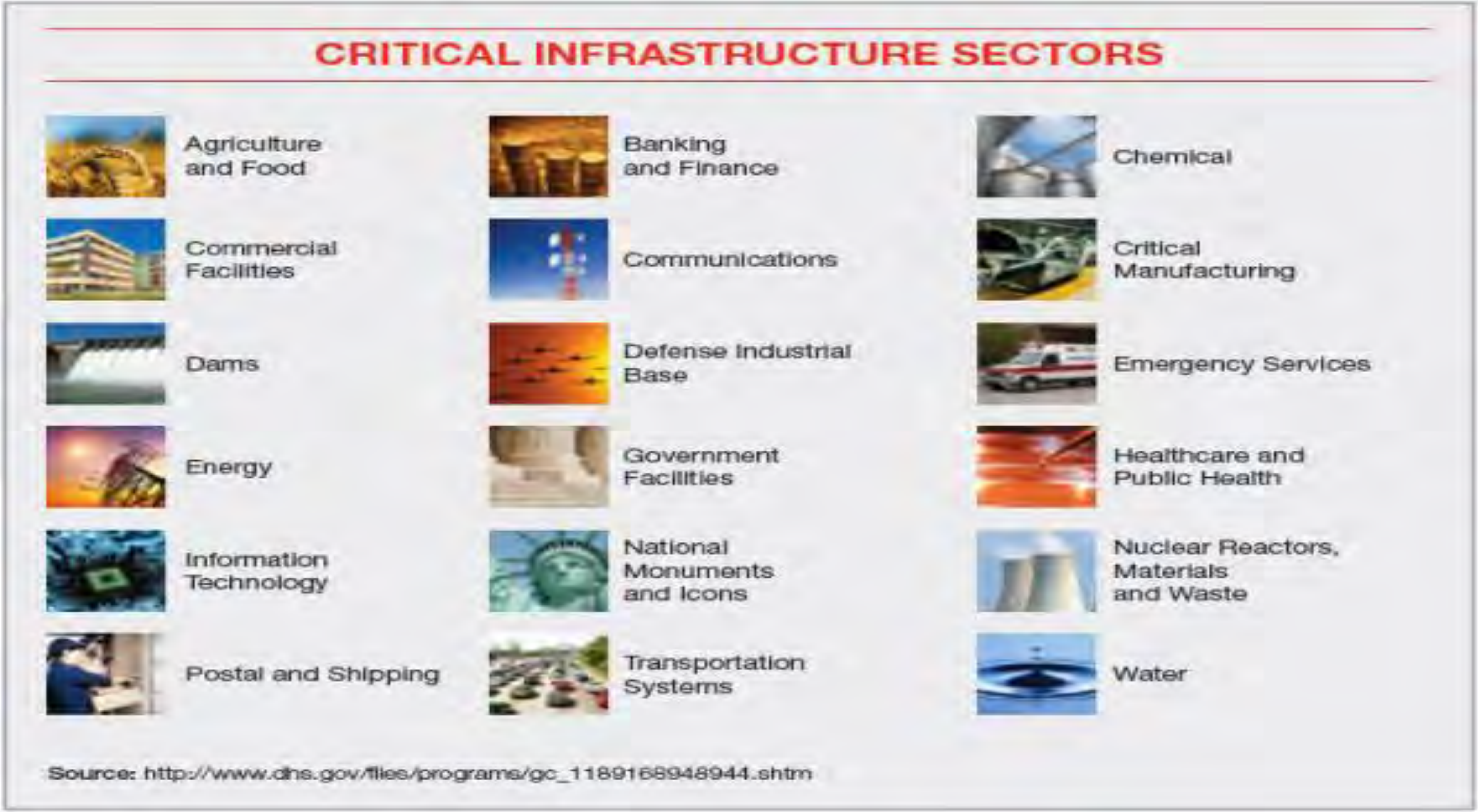
NOVEMBER 6, 2018

Agenda

- Critical Infrastructure
    - Definition
    - Sixteen Sectors of Critical Infrastructure
    - Emergency Services
    - North Alabama Critical Infrastructure
    - How they connect
- Disaster Categories
- Threats – External/Internal
    - Cyber
    - Terrorism
    - Electromagnetic Pulse
    - Space Weather
- Requirements to Identify Critical Infrastructure
    - Three Strategic Imperatives
    - Hometown Security
    - Innovations, Research and Development
- Critical Infrastructure Protection
    - Home Town Security
    - Assessment Resources
- **Comments and Questions**

Critical Infrastructure

- The U.S. Government states that the country's critical infrastructure is: the ***infrastructure*** and ***assets*** vital to national security, governance, health, safety, economy and public confidence.
- Presidential Policy Directive 21 (PPD-21) Critical Infrastructure Security and Resilience – **advances** a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.
- National Infrastructure Protection Plan (NIPP) – was created in 2013 to outline how both public and private sector entities would work together to protect our critical infrastructure in the U.S.
- National Response Framework (NRF) - how the Nation responds to all types of disasters and emergencies. It is built on scalable, flexible, and adaptable concepts identified in the ***National Incident Management System*** to align key roles and responsibilities across the Nation.



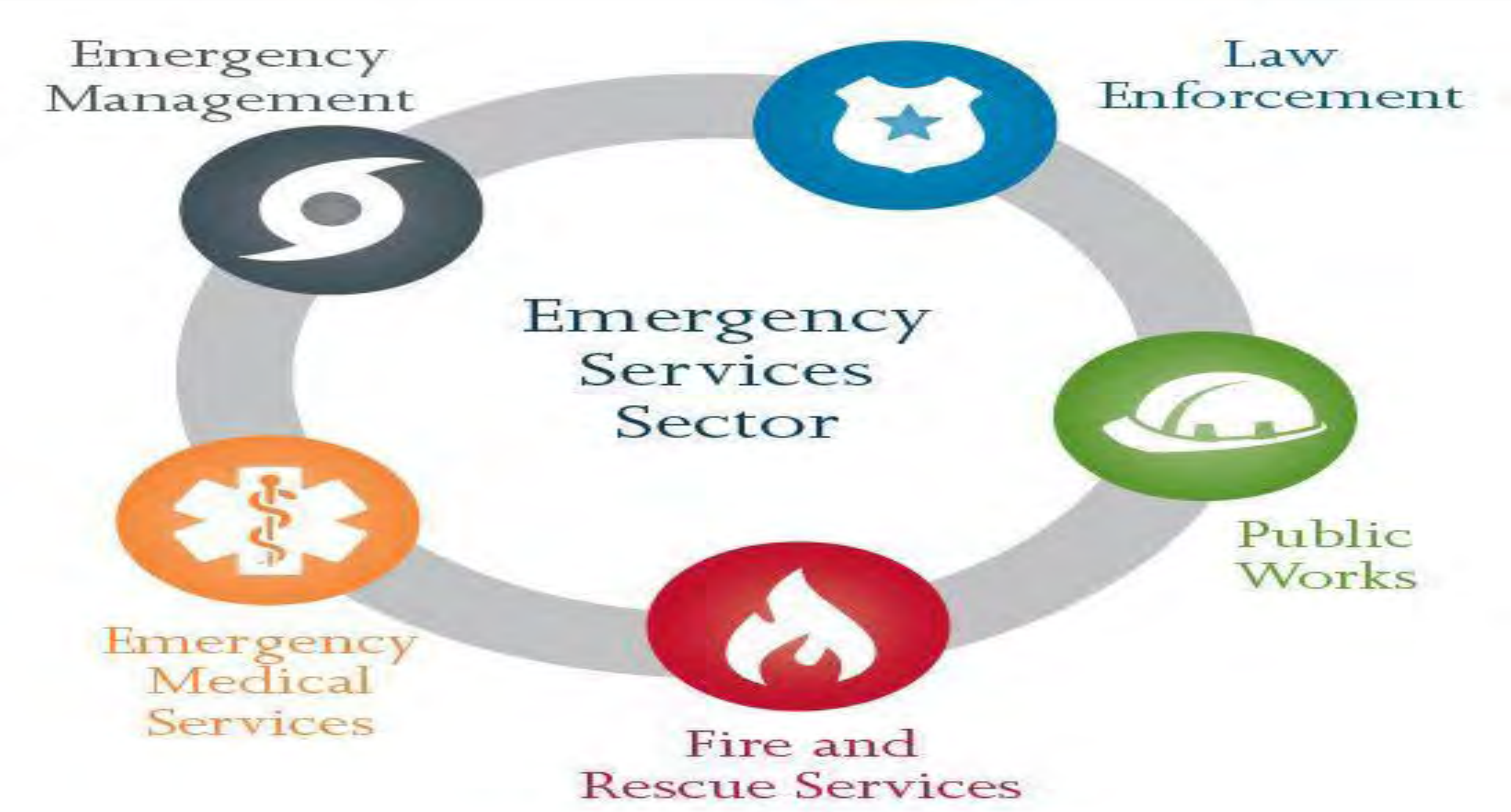
CRITICAL INFRASTRUCTURE SECTORS

- Agriculture and Food
- Banking and Finance
- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Government Facilities
- Healthcare and Public Health
- Information Technology
- National Monuments and Icons
- Nuclear Reactors, Materials and Waste
- Postal and Shipping
- Transportation Systems
- Water

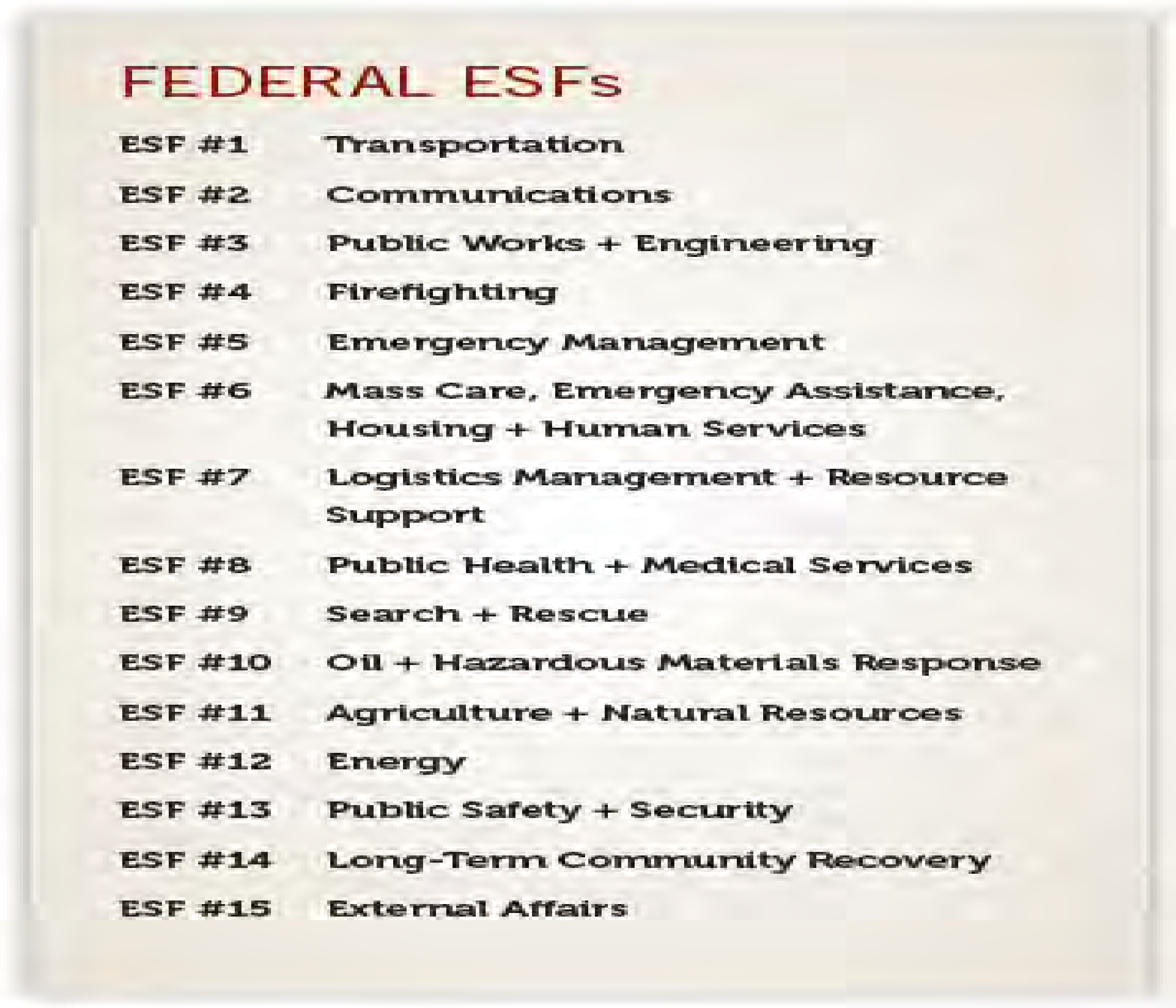
Source: http://www.dhs.gov/files/programs/gc_1189168948944.shtm

Critical Infrastructure

Emergency Services

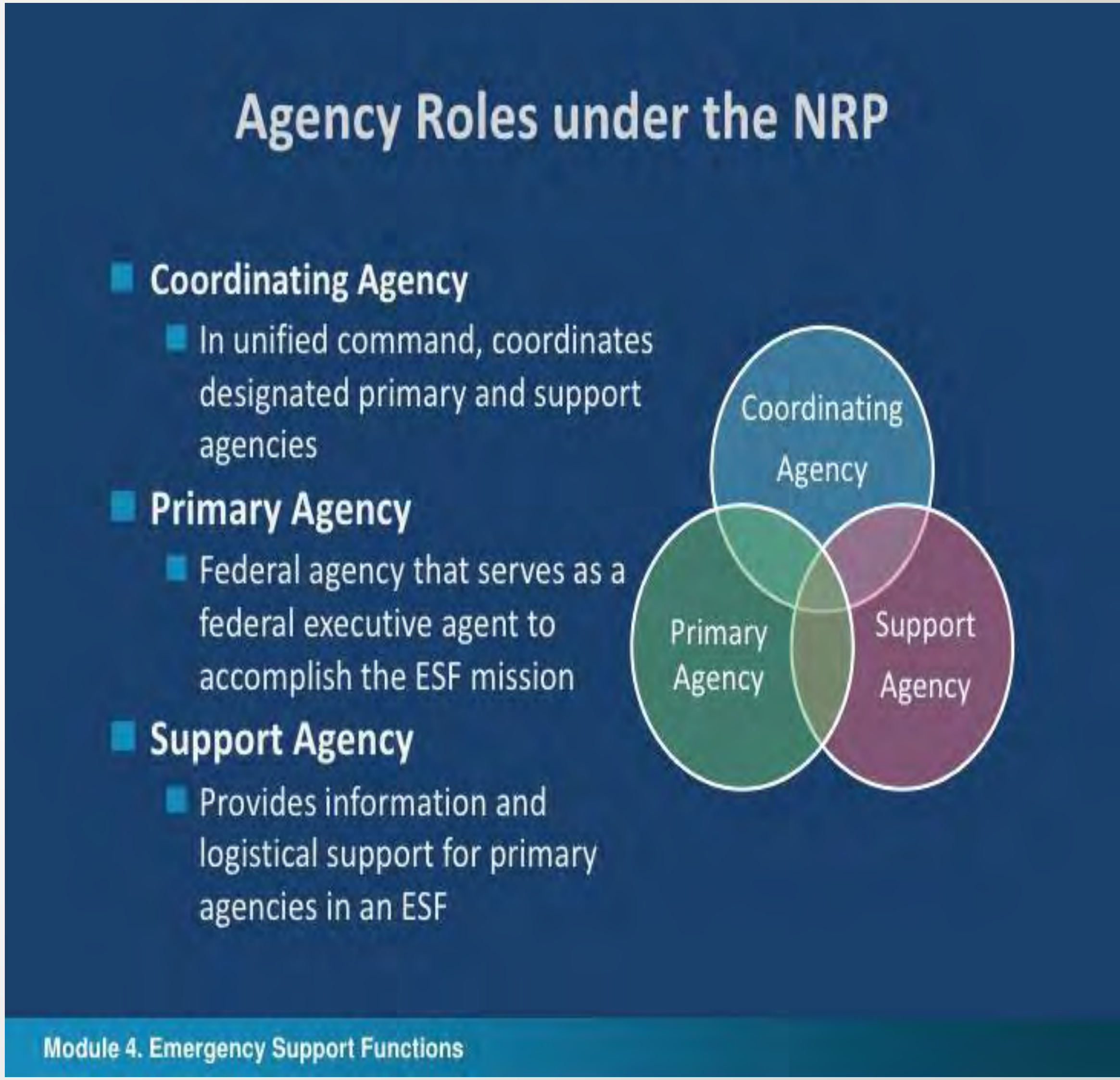


Critical Infrastructure
National Response Plan and Emergency Support Functions



FEDERAL ESFs

ESF #1	Transportation
ESF #2	Communications
ESF #3	Public Works + Engineering
ESF #4	Firefighting
ESF #5	Emergency Management
ESF #6	Mass Care, Emergency Assistance, Housing + Human Services
ESF #7	Logistics Management + Resource Support
ESF #8	Public Health + Medical Services
ESF #9	Search + Rescue
ESF #10	Oil + Hazardous Materials Response
ESF #11	Agriculture + Natural Resources
ESF #12	Energy
ESF #13	Public Safety + Security
ESF #14	Long-Term Community Recovery
ESF #15	External Affairs

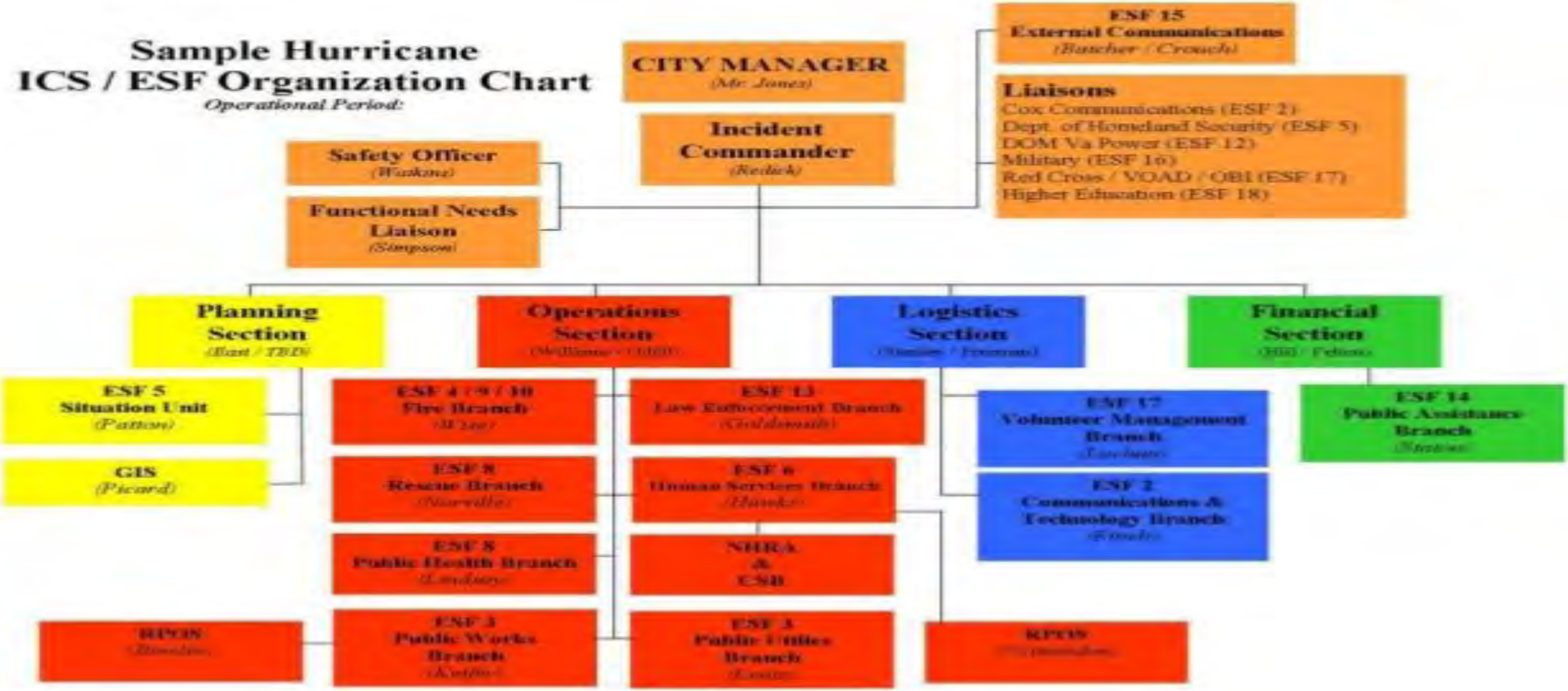


Agency Roles under the NRP

- **Coordinating Agency**
  - In unified command, coordinates designated primary and support agencies
- **Primary Agency**
  - Federal agency that serves as a federal executive agent to accomplish the ESF mission
- **Support Agency**
  - Provides information and logistical support for primary agencies in an ESF

Module 4. Emergency Support Functions

Incident Command System
Emergency Support Functions



Northern Alabama Critical Infrastructure

Nuclear

Space

Interstate

Airport

Cyber

Water

Defense

Dams

Railways

Chemical

Energy

Healthcare

Emergency Services

Always remember….Incidents are managed at the local level

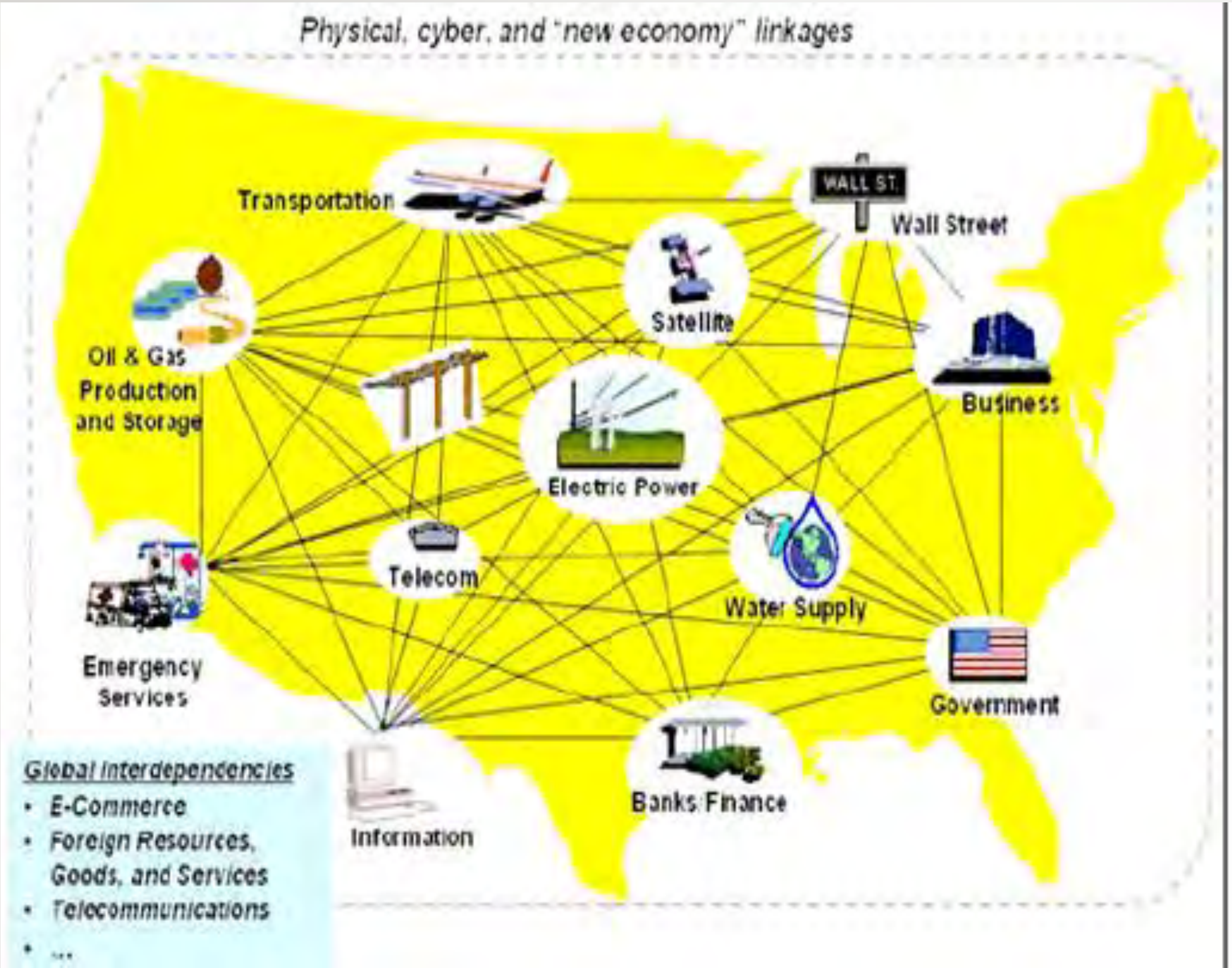
Banking/Finance

Education

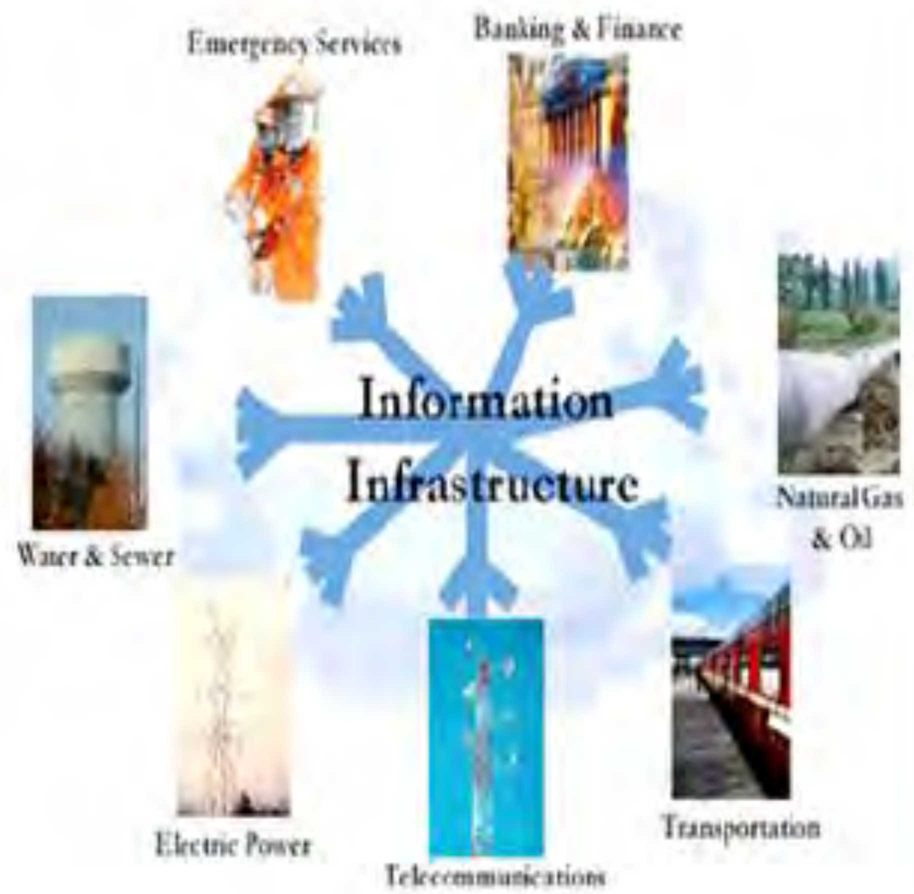
Manufacturing

Commercial

Critical Infrastructure
How They Connect



Global Interdependencies
- E-Commerce
- Foreign Resources, Goods, and Services
- Telecommunications
- ...

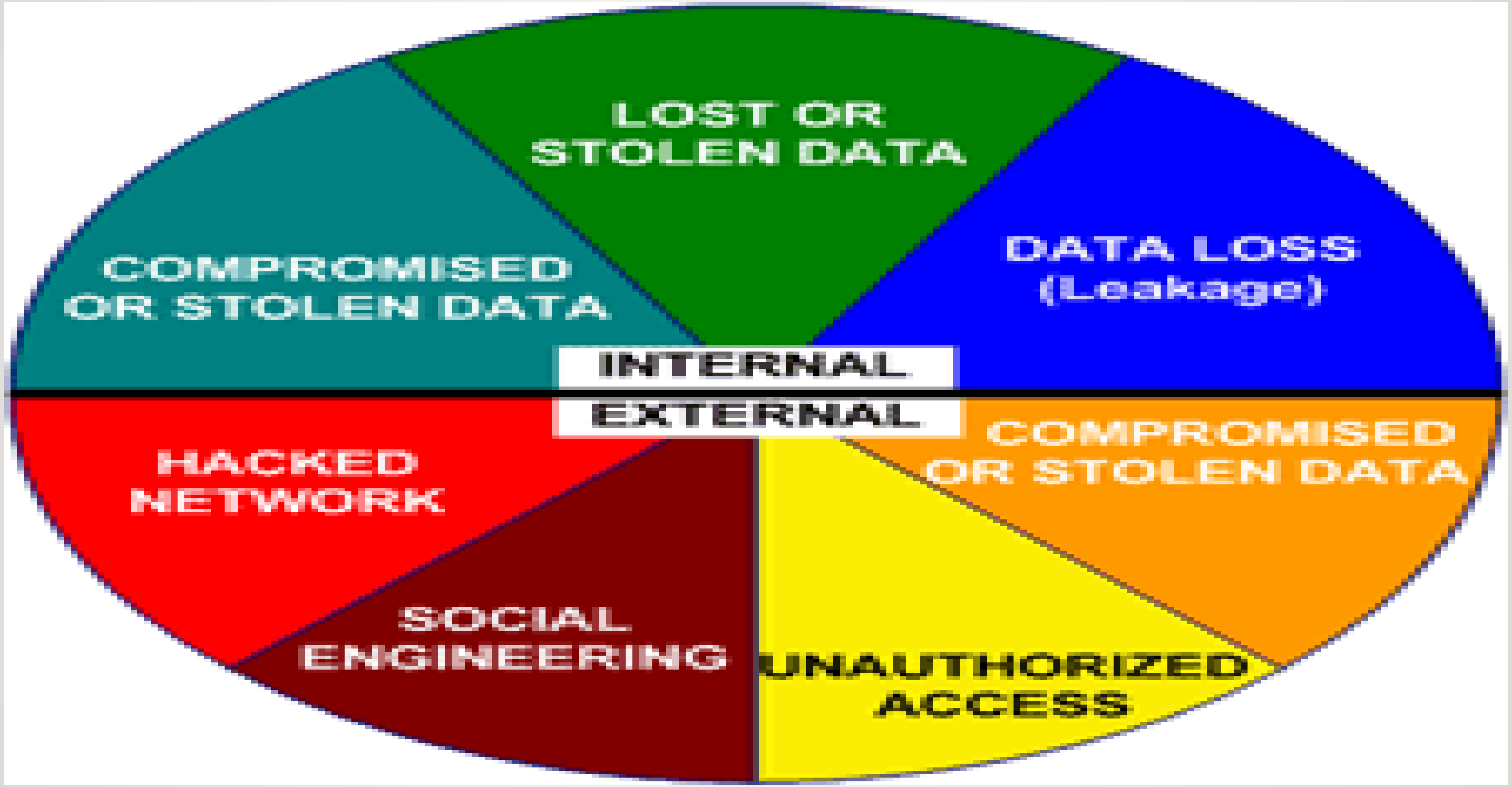


Disaster Categories

- **Natural** – A disaster caused by events other than man or technology.
- **Manmade** - A disastrous event caused directly and principally by one or more identifiable deliberate or negligent human actions. Also called human-**made disaster.** Examples include fires, transport accidents, industrial accidents, oil spills, and nuclear explosions/radiation. War and deliberate attacks may also be put in this category.
- **Technological disaster** - is a catastrophic event that is caused by either human error in controlling technology or a malfunction of a technology system**.** Technology based disasters are as serious as natural disasters.

Threats to Critical Infrastructure
Internal/External

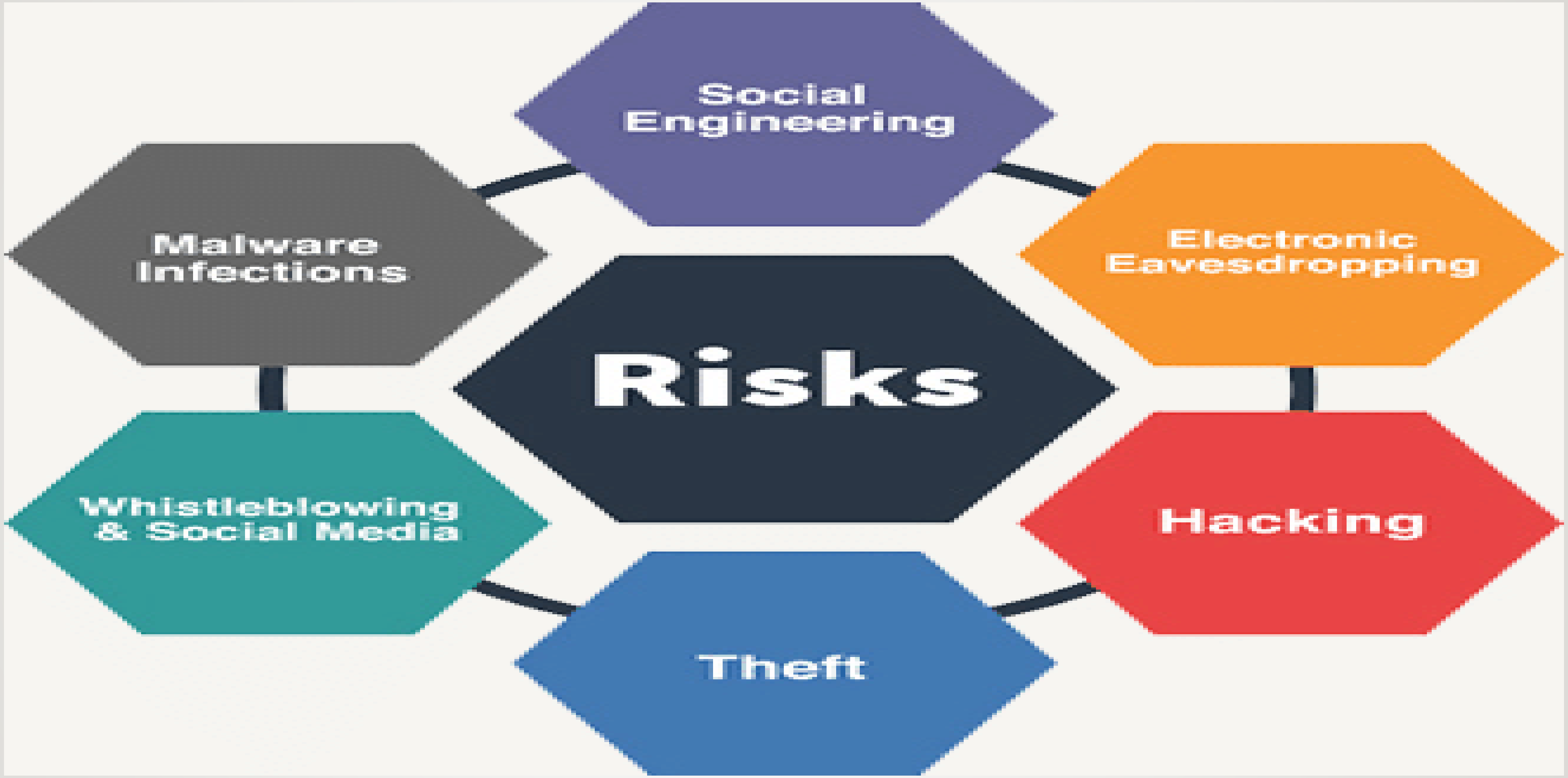
-



Theft in multiple cases losing millions of employee records, customers and citizens

Threats To Critical Infrastructure

Cyber



Internal/External

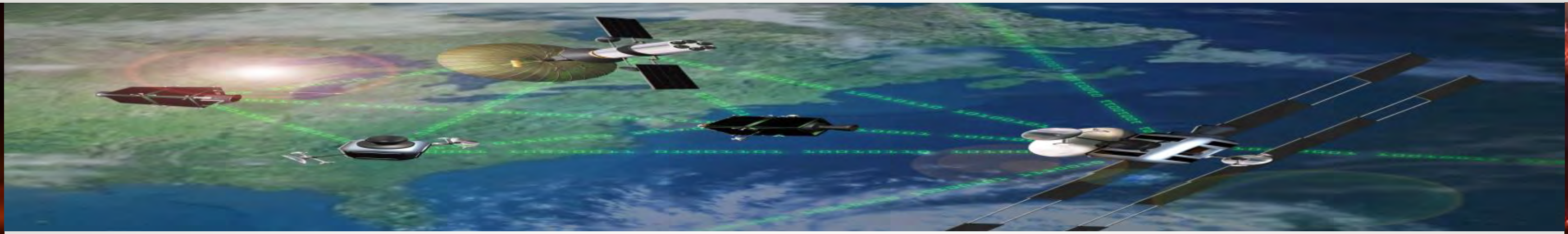
Easier to hack from afar than in person
Ransomware found in 39% of cases where malware was identified
Computer chips and controlling ships?

Threats To Critical Infrastructure
Cyber

- U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations (Jun, 2018).
- Mattis - Russian GRU caught hacking, vows cyber support to allies (Aug, 2018).
- Cyber-attack (e.g., Ukraine Blackout of 2015).
- White House National Security Adviser confirms **China** carried out the cyber attack on the Office of Personnel Management and stole 20 million records (Sept, 2018).
- Allegations of Chinese cyber spies had used a U.S.-based tech firm to secretly embed tiny computer chips into electronic devices purchased and used by almost 30 different companies (Oct, 2018).
- China may be copying Facebook to build an intelligence weapon (Oct 2018).
- U.S. infrastructure vulnerable to cyberattacks designed to suppress voter turnout (Oct, 2018).

Threats To Critical Infrastructure

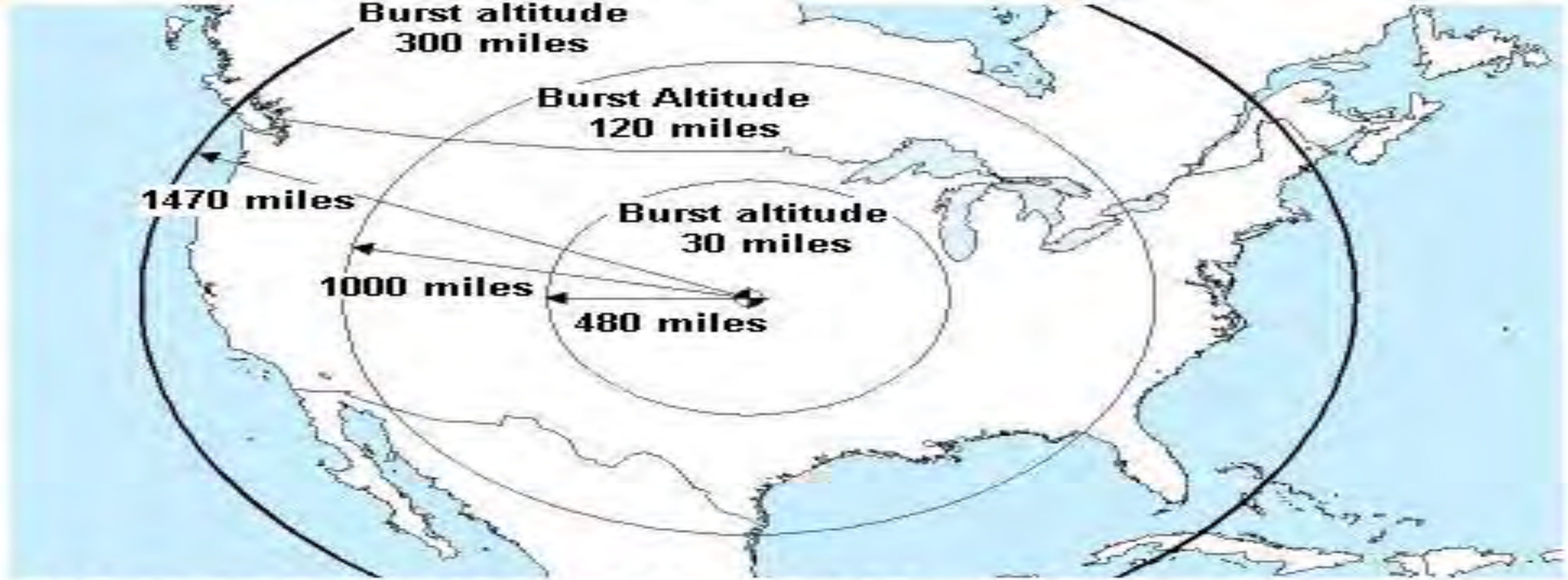
Terrorism



- No longer requires a nation state or military to cause major disruption to life, economy, or critical infrastructure
- Metcalf sniper attack on a Pacific gas and Electric Company’s Metcalf Transmission Substation located in Coyote, California (2013). Snipers fired on 17 electrical transformers

Threats To Critical Infrastructure

Electromagnetic Pulse

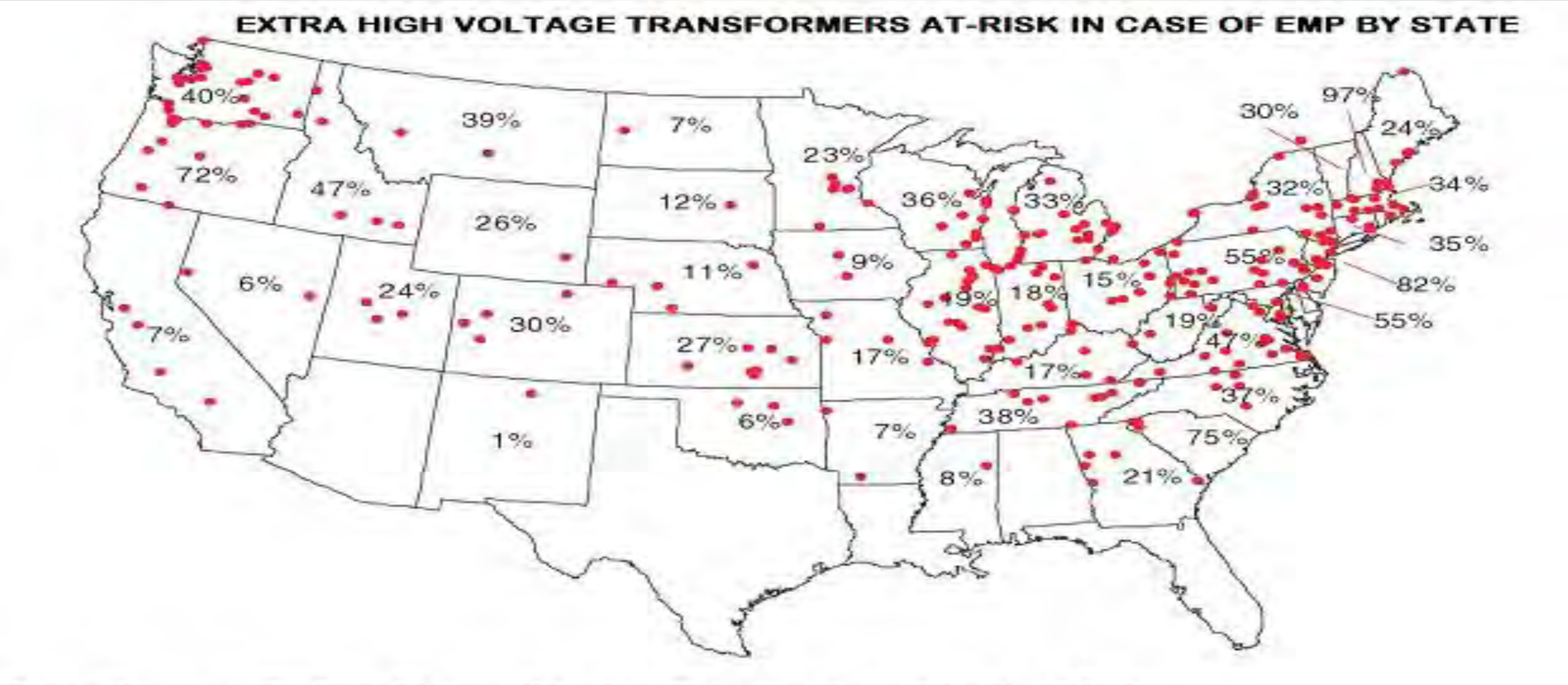


EMP AREA BY BURSTS AT 30, 120 and 300 MILES

Gary Smith, "Electromagnetic Pulse Threats", testimony to House National Security Committee on July 16, 1997

An intense pulse of electromagnetic radiation, especially one generated by a nuclear explosion and occurring high above the earth’s surface

Threats To Critical Infrastructure Electromagnetic Pulse



EXTRA HIGH VOLTAGE TRANSFORMERS AT-RISK IN CASE OF EMP BY STATE

Source: J.Kappenman - "The Future: Solutions or Vulnerabilities?", space weather workshop, May 23, 2008

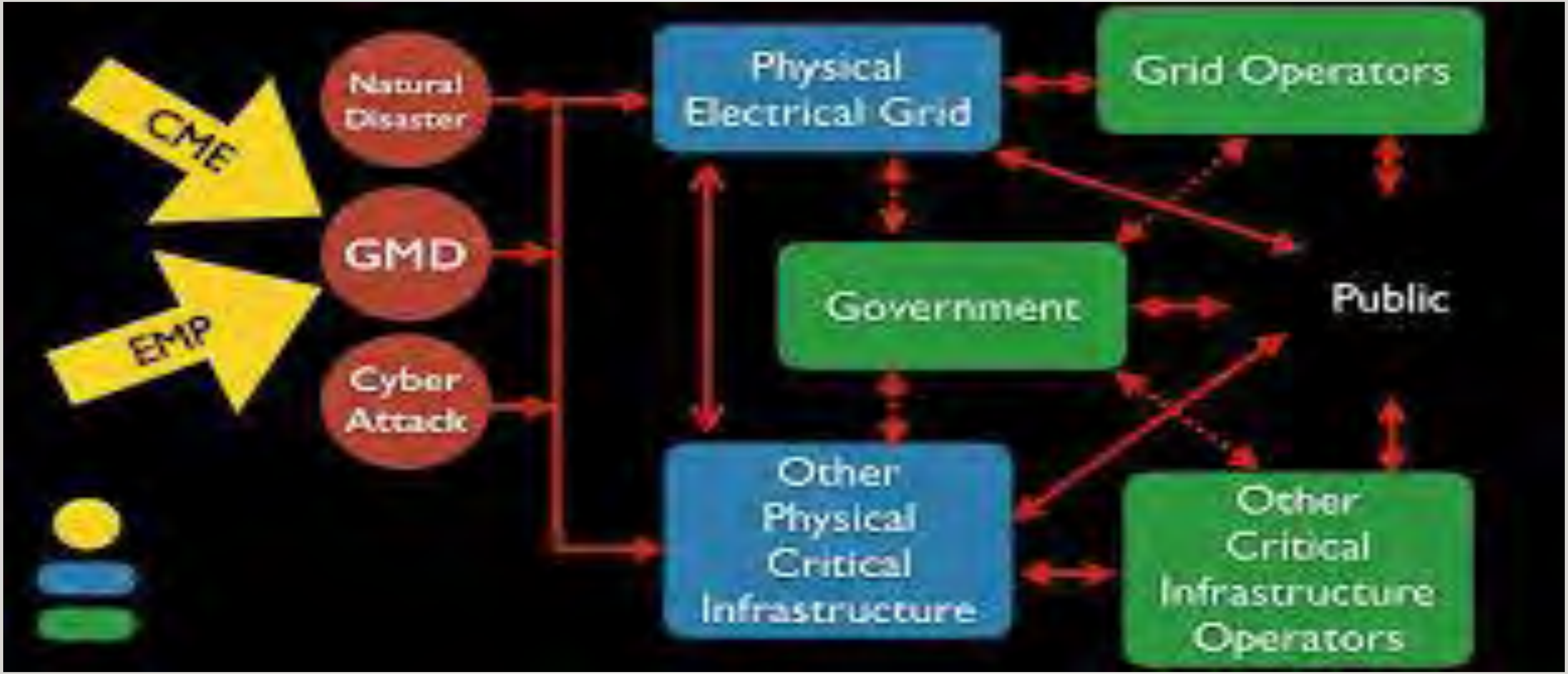
Threats To Critical Infrastructure
Electromagnetic Pulse (EMP)

- In 1962, the US conducted a test named *Starfish Prime* by detonating a 1.4 megaton thermonuclear bomb 20 miles above Johnston Atoll in the Pacific. In space, six American, British, and Soviet satellites suffered damage, and 800 miles away in Hawaii, burglar alarms sounded, street lights blinked out, and phones, radios, and televisions went dead.
- 2001-2017 EMP Commission Study to assess the threat to the US from EMP attack.
- In 2004 and 2008, the EMP Commission testified to the Armed Service Committee that the U.S. society and economy are so critically independent upon the availability of electricity that a significant collapse of the grid precipitated by a major natural or man-made event, or EMP, could result in catastrophic civilian casualties.
- In 2016, DoE efforts to improve EMP resilience: Methodology to assess high-altitude electromagnetic pulse (HEMP) impact on the Electric Grid (Oak Ridge National Laboratory), EMP/GMD Impacts Study (Los Alamos National Laboratory), Report on Vulnerability of and Impact to Grid from an EMP (Idaho National Laboratory), Joint Electromagnetic Pulse Resilience Strategy (DoE, EPR, ICF) and US Department of Energy Electromagnetic Pulse Resilience. (Idaho National Laboratory).
- In 2016 Congress approved the Critical Infrastructure Protection Act (CIPA) by inserting it in to the National Defense Authorization Act. Passage means that millions of emergency planners and first responders across the nation will become part of the solution to the existential threat that is EMP.
- Numerous studies and books: Dr. Vincent Pry, Dr William Fortschen, Jonathon Hollerman……..
- Continuity of Government (COG) and Continuity of operations (COOP).

Threats To Critical Infrastructure
Electromagnetic Pulse (EMP)

- North Korean KMS-3 and KMS-4 satellites orbiting over the US 24/7 South to North path.
- Speculation vs ability to test facts or statements, US Government/Private Industry failure to identify and resolve.
- Former CIA Director Woolsey states "North Korea possesses EMP capability" (2017). Equally, Russia and China threat to the homeland and DoD.
- Russian Sukhoi Su -24 with the newest jamming complex paralyzed in the Black Sea the most modern American combat management system "Aegis" installed on the destroyer "USS Donald Cook" (April, 2014).
- Russia's new Alabuga EMP weapons program. "This EMP would create an ultra high frequency (UHF) field of approximately 3.5 kilometers, not only disabling computers, radars, communications systems and precision weapons, but also making them unusable by damaging their electronic components." (Dec, 2017).
- China's new microwave weapon can disable missiles and paralyze tanks (Jan, 2017).
- Pandemic (listed by Federal Energy Regulatory Commission and Department of Energy as a threat to the power grid).
- DOE conspired with industry's private electric power research institute to produce a "junk science" study that argued that a nuclear EMP attack would not destroy electric grid transformer or cause a protracted nationwide blackout. (2012-2016)
- Oct 2017, Congressional hearing….90% death of citizens in first year after EMP.
- **Estimated price tag to fix domestic grid and protect from EMP** ……3 billion dollars (Jun, 2017).

Threats To Critical Infrastructure
Space Weather



Solar Flare or Geomagnetic disturbance (e.g., Quebec blackout of 1989).
Two CMEs missed hitting the United States by one week in 2016. Events minutes apart . Speculation NASA or Government missed the threat and/or failed to notify populace.

Requirements to Identify Critical Infrastructure

- Three strategic imperatives to drive the Federal approach to strengthen critical infrastructure security and resilience:
  - *Refine* and *clarify* functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience:
  - *Enable* effective *information exchange* by identifying baseline data and systems requirements for the Federal Government; and,
  - *Implement* an *integration* and *analysis* function to inform *planning* and *operations* decisions regarding critical infrastructure.
- Federal departments and agencies shall implement this directive in a manner consistent with applicable law, Presidential directives, and Federal regulations, including those protecting privacy and civil liberties.

Requirements to Identify Critical Infrastructure
Innovation, Research and Development

- The Secretary of Homeland Security, in coordination with the Office of Science and Technology Policy, the Sector Specific Agency's, Department of Commerce, and other Federal departments and agencies, shall provide input to align those Federal and Federally-funded research and development (R&D) activities that seek to strengthen the security and resilience of the Nation's critical infrastructure, including:
    - Promoting R&D
    - Enhancing modeling capabilities
    - Facilitating initiatives to promote cybersecurity investments and adaptation of designs to strengthen all-hazards security and resilience; and
    - Prioritization of efforts to support strategic guidance issued by the Secretary of Homeland Security

Critical Infrastructure Protection
Starts With Hometown Security

- Just as incidents are managed at the local level, Homeland Security starts with hometown security.
- ***Hometown security*** – pre-planning and preparation can often prevent the event and also provides for a faster recovery from most potential events. Apply these four steps:
  - **Connect, plan, train** and **report** in advance of an incident or attack to help better prepare businesses and their employees to proactively think about the role they play in the safety and security of their businesses and communities
- ***Protective Security Advisors (PSA)*** – are trained in critical infrastructure security and resilience and vulnerability mitigation.
- ***Homeland Security Information Network – Critical Infrastructure (HSIN-CI)*** – is the trusted network for homeland security mission operations to share Sensitive but Unclassified (SBU) information. This is the primary system through which private sector owners and operators, DHS, and other federal, state, and local government agencies collaborate to protect the nation's critical infrastructure.
- ***Suspicious Activity Reporting Tool*** - This HSIN-CI Suspicious Activity Reporting tool allows non-uniformed, law enforcement private sector members to submit formalized suspicious activity reports to appropriate law enforcement officials and to facilitate efficient information sharing and responsiveness.

Critical Infrastructure Protection
Starts With Hometown Security (cont'd)

- ***Active Shooter Preparedness*** – resources include various trainings and human resources personnel can mitigate the risk of and appropriately react in the event of an active shooter situation.
- ***Bombing Prevention*** – rare, but should always be taken seriously. How quickly and safely you react to a bomb threat could save lives, including your own.
- ***Unmanned Aircraft Systems*** – commonly known as unmanned aerial vehicles (UAV) or drones and the ownership and usage increases daily. Used by both ***responders and adversaries***, UAVs can often evade detection and create challenges for the critical infrastructure community.
- ***Ready.gov*** – a national public service advertising campaign designed to educate and empower Americans to prepare for and respond to natural and man-made incidents. The goal is to get the public involved and ultimately to increase the level of basic preparedness across the nation.
- ***Training.FEMA.GOV*** – a great learning tool through FEMA to not only obtain a certificate upon successful testing on the chosen topic, this is a great tool to learn "what does FEMA do" during disasters and pre-disaster preparedness. Many citizens find it easier to blame FEMA than to learn what FEMA is responsible for and it's limitations.

Critical Infrastructure Protection
Starts With Hometown Security (cont’d)

- ***Business Continuity Planning Suite*** – consists of three main components: BCP training and disaster recovery plan tool, and exercises for an implemented BCP. The suite and training are free and available to all.
- ***The Infrastructure Development and Recovery Program*** – coordinates a suite of resources and methods to enhance infrastructure security and resilience to all natural and human hazards during planning, maintenance and recovery across the critical infrastructure community.
- ***Sector Specific Agencies*** – the primary federal entities responsible for coordinating critical infrastructure security and resilience efforts within individual sectors. DHS is the sector-specific agency for 10 of the 16 sectors.
- ***Sector-Specific Tabletop Exercise Program*** – this tool allows critical infrastructure partners to develop interactive, discussion-based exercises for their communities of interest, at the sector or a facility level. The program allows users to leverage pre-built exercise templates and tailor them to their programs, policies, and procedures within an incident management functional area. Contact the IP Exercise Team at SOPD.Exercise@hq.dhs.gov.

Incident Command Structure (ICS)

- https://training.fema.gov
- Complete the following four correspondence courses:
- IS 100 - https://training.fema.gov/is/courseoverview.aspx?code=IS-100.b
- IS 200 - https://training.fema.gov/is/courseoverview.aspx?code=IS-200.b
- IS 700 - https://training.fema.gov/is/courseoverview.aspx?code=IS-700.a
- IS 800 - https://training.fema.gov/is/courseoverview.aspx?code=IS-800.b
- Take In-Residence - IS 300 and IS 400 to obtain the NIMS certification
- Other important correspondence courses to support NIMS and EM:
- IS 546 a: Continuity of Operations Awareness Course - https://training.fema.gov/is/courseoverview.aspx?code=IS-546.a
- IS 547 a: Introduction to Continuity of Operations - https://training.fema.gov/is/courseoverview.aspx?code=IS-547.a
- IS 520 - Introduction to Continuity of Operations Planning for Pandemic Influenzas - https://training.fema.gov/programs/coop/level1.aspx

Critical Infrastructure Protection
Assessment Resources

- ***Infrastructure Visualization Platform (IVP)*** – data collection and presentation tool .
- ***Assist Visits*** – two-part voluntary program that includes security surveys and outreach. Protective Security Advisors conduct security surveys to assess the overall security posture of the Nation's most critical infrastructure sites and facilities.
- ***Regional Resiliency Assessment Program (PRAP)*** – evaluates critical infrastructure in specific geographic regions to examine vulnerabilities, threats, and potential consequences from an all-hazards perspective.
- ***National Counter-Improvised Explosive Device (IED) Capability Analysis*** – gathers comprehensive data on state and local first responders to assess readiness, equipment, training, and assets required for effective response to IED threats.
- ***Multi-Jurisdiction Improvised Explosive Device Security Planning*** – systematic process fuses counter-IED capability analysis, training, and planning to enhance urban area IED prevention, protection, mitigation, and response capabilities.
- ***Critical Infrastructure Cyber Community C3 Voluntary Program*** – coordinates with the federal government for critical infrastructure owners and operators interested in improving their cyber risk management.
- ***Cybersecurity Evaluation Program (CSEP)*** – voluntary cybersecurity assessments conducted across all 16 critical infrastructure sectors and within state governments and large urban areas.

FINAL THOUGHTS

- Most Valuable Resources: (People – I.T. – Infrastructure)
- Personal and Family Survival Priority One – Life Safety
- Risk Analysis: Threat vs Reality? VA-Mitigation
- Politics vs Reality
- Defense in Depth vs Citizen Support (InfraGard)
- Layers of Government vs Local Level Management (Integration, Training, Funding and Communications)
- Leadership vs Media (Trust, Sales Job, and Support)
- Doing Something vs Doing Nothing
- **$3 billion dollars!!!!**

Questions and Comments

Thank you