Cyber Security and Critical Infrastructure

The Practice, Profession, and Problem Space

About me…

- Broad Background
  - Lived in a little hacker compound as a kid
  - Started with Open Source development (Rubicon03)
  - MSSP:IDS, Data Viz, Anomaly Detection Designer
  - Enterprise Security Architecture
  - ICS-CERT (INL)
  - Fed with Nationally-scoped cyber responsibilities
- Now
  - Non-profit Community Builder & Facilitator
  - Focus on Electric Sector

Why Define Cyber Security?

- B-SidesDC and Liquid Matrix
- The hackathon “Boring” problem
- Deluge of Debates and Discussion
  - Media Hype, Political Wedge, Money Fountain, Actual Problem
  - No Culturally Accepted Vision
- Laws & Mandates on Books, but poorly understood
  - Have you ever tried to READ any of it?
  - Even the people doing it don’t always get it
- Language Problems Cause Serious Barriers
  - Grab bag of security ideas, no structure
  - Players not always informed of “State of Play”
  - Different culture groups (“Product Developers” – Gene Kim)
- Opportunity
  - To cause more problems or…to stop losing
  - Will be lost without wide engagement and forward motion
- NOTE: “Observed Perspectives” vs “Official Truth”

Why should you care?

- It could be fun
  - –You get to learn a new problem space
  - –Cyber Security (IMO) is only distantly related to "computer security" as we know it
  - –Doesn't mean hacking isn't involved
  - –It just means we have to think bigger
- This will effect us
  - –Even if not explicitly: Culturally & Scope Creep

What does cyber security appear to be?

Part I: The Role of Language

Poor Labels, Poor Understanding

- Labels of Convenience: Other names for security
  - Info, Data, Computer, Hacking, Cloud, Bleh
  - Mean...what? to whom? Marketing or Lazy
- Functional Labels: Based on activity/skills
  - Reversing, Monitoring, Coding, Engineering, Blah
  - Better, not not great: No start/stop points

"Object Oriented Policy Making"

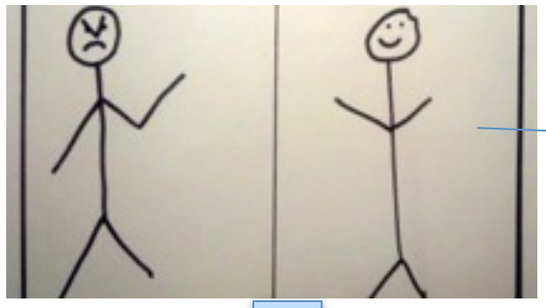
- Poor labeling leads to scoping and policy issues
  - Grab Bag Problem: Good ideas scattered everywhere – neither related nor consistently relatable
  - Sloppy code...err..policy..is buggy and unmaintainable
- We need object oriented policy-making!
  - Structure
  - Classes & Objects
  - Inputs/Outputs
  - Etc

“Security” has natural parenthetical Scopes

Boss Bob

I want to steal hazardous materials!

EVIL GOOD!

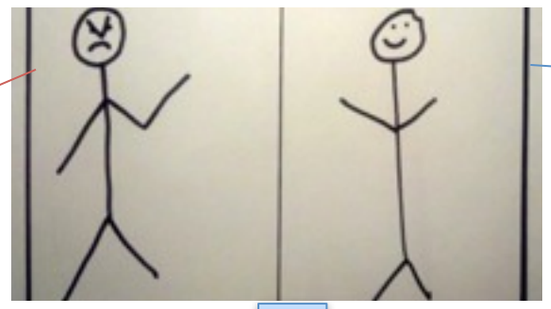


CEO Jim

I want to keep making $123 a day!

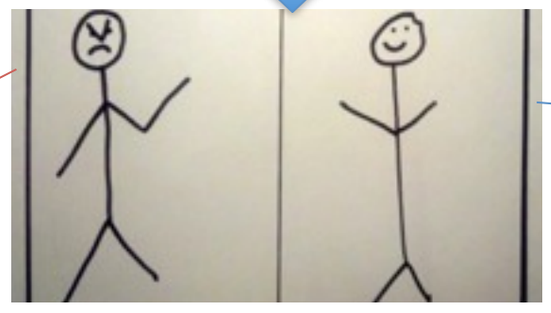
Cyber Planning Bob

Ok, we’ll attack Traffic Light Controls and make trucks stop!



IT Architect Jim

Let’s make sure IT enables $123/day



Hacker Bob

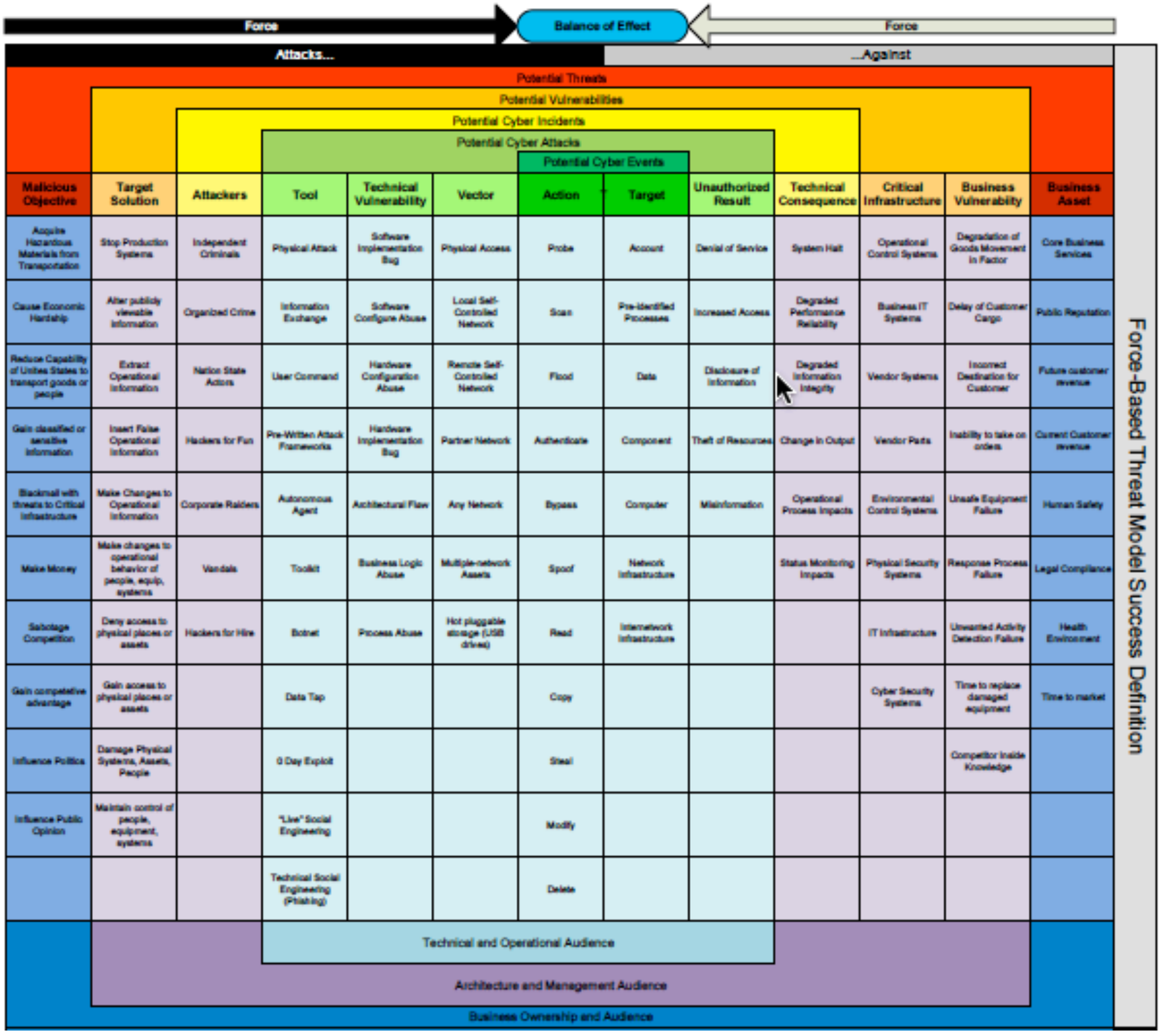
Metasploit to the rescue!

Security Jim

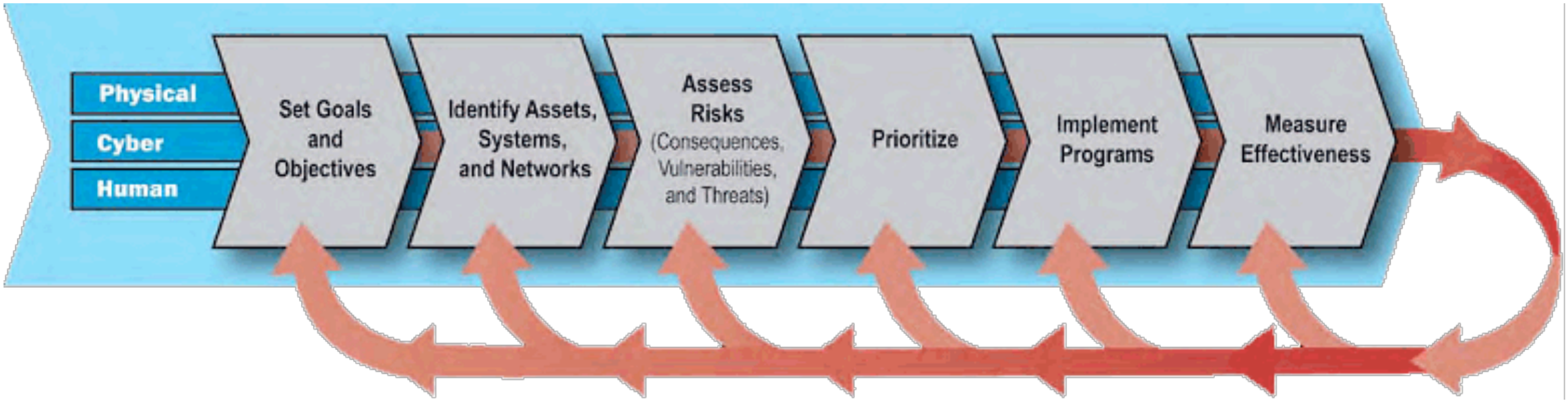
IDS to the Rescue!

“Tech

Maybe too detailed? Start smaller.



Simple Risk Management

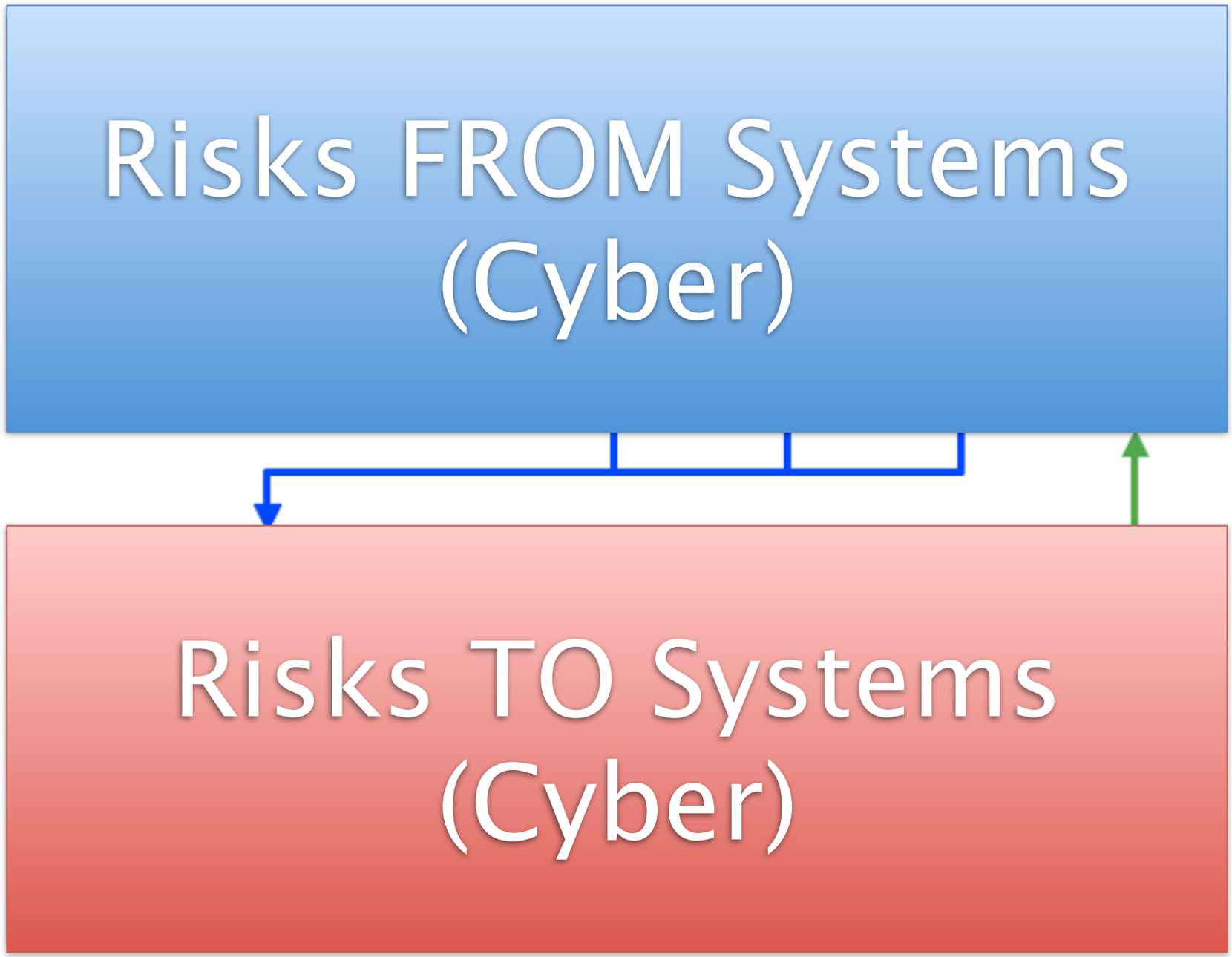


Scoping is not defined.

This is a mistake, even at a high level.

(Yes, this is/was in use nationally ☹)

More helpful: Linked Life-cycles



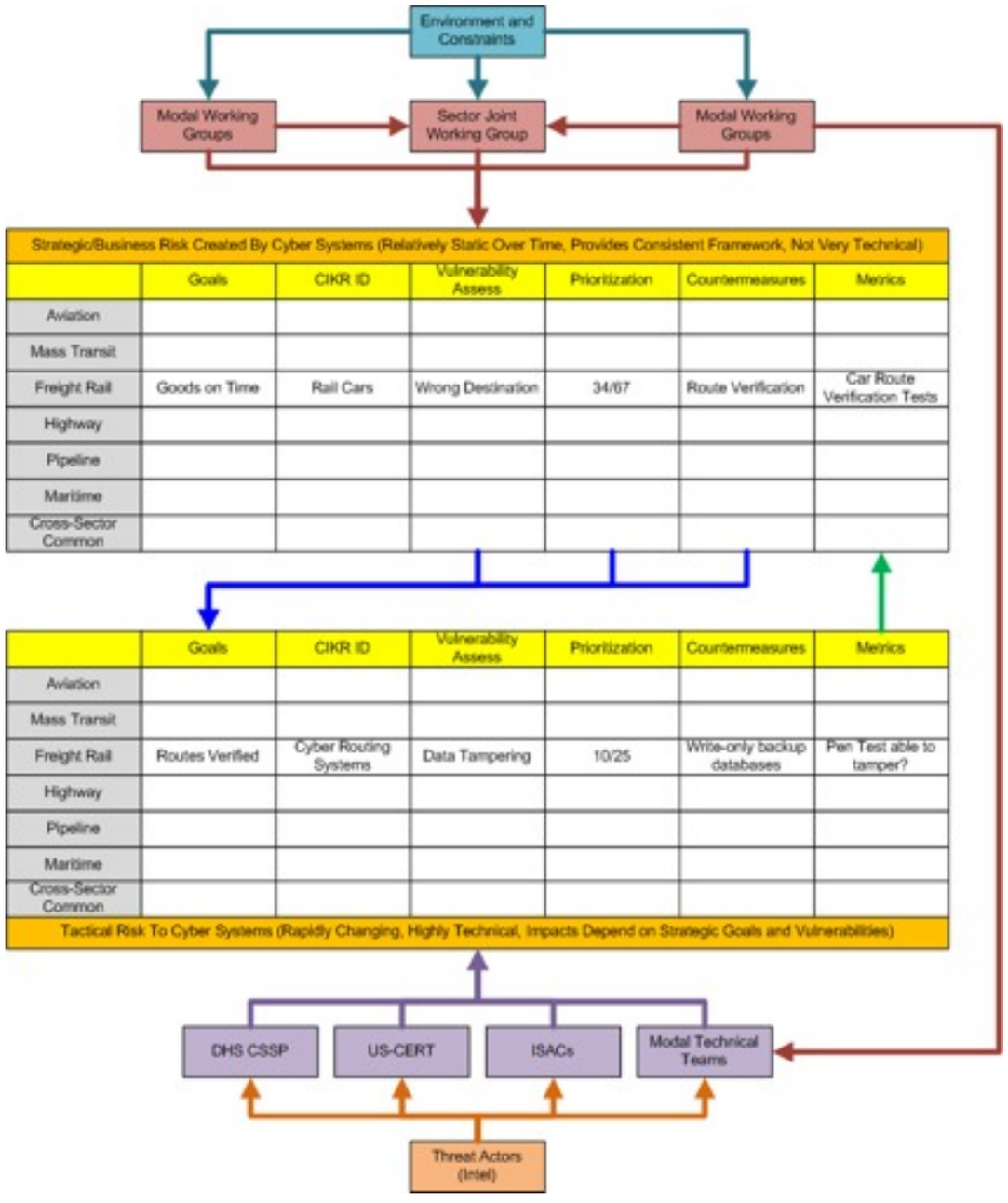
Risks From Cyber / Risks To Cyber

- "Risks from"
  - Business & Non-Cyber
  - Long view
  - Evaluated regularly
  - Frames "Risks to" and makes actionable

- "Risks to"
  - Technical & Implementation
  - Dynamic, Rapidly Changing
  - Should be reevaluated often
  - Context provided by "Risks From"

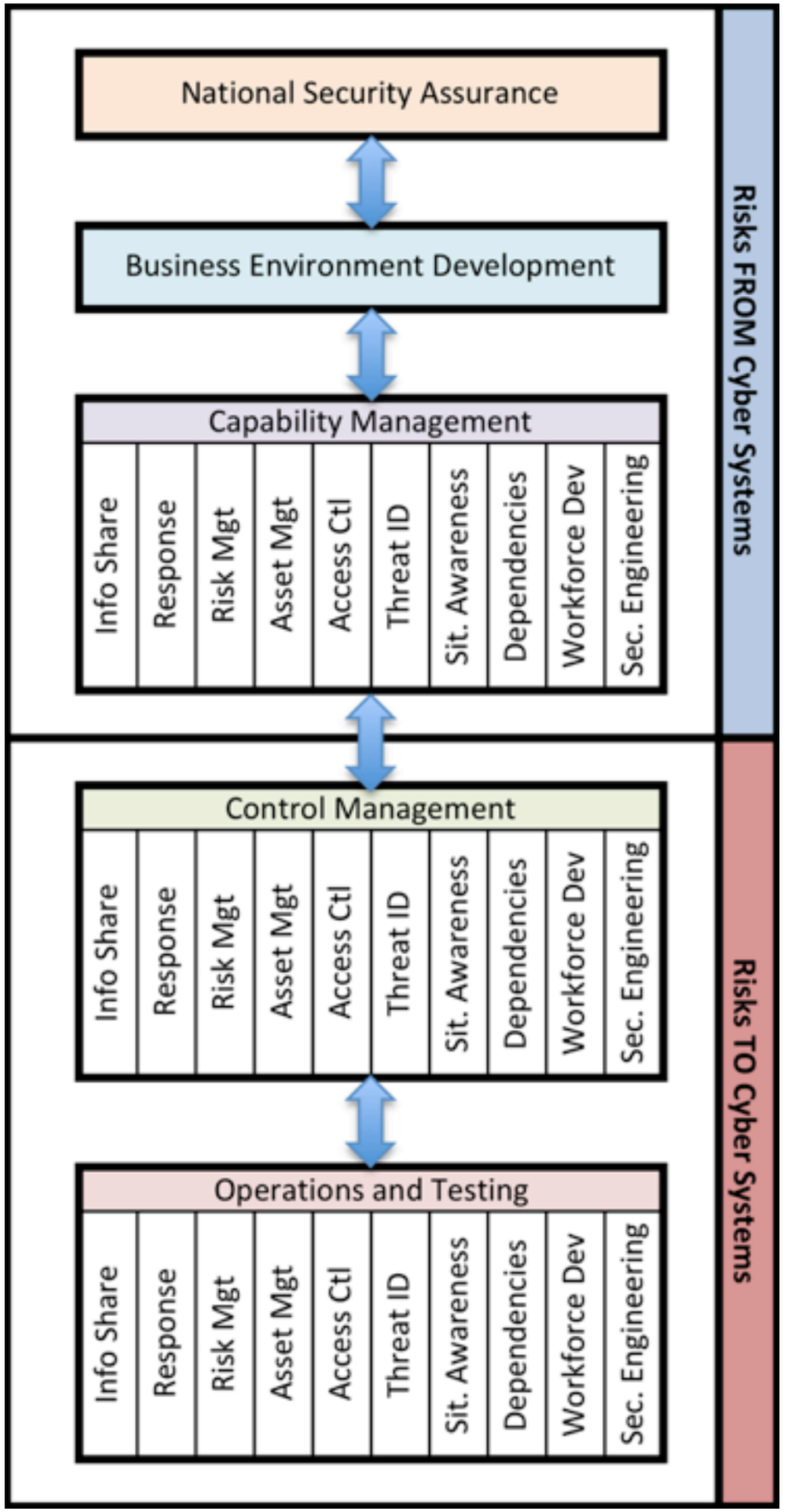
- Linked Life-cycles allow alignment of strategy and tactics while de-conflicting perspectives
- Allows strategy to influence ground action and, where pertinent, vice versa

Helpful to understand government's activity
(Even if they don't always)



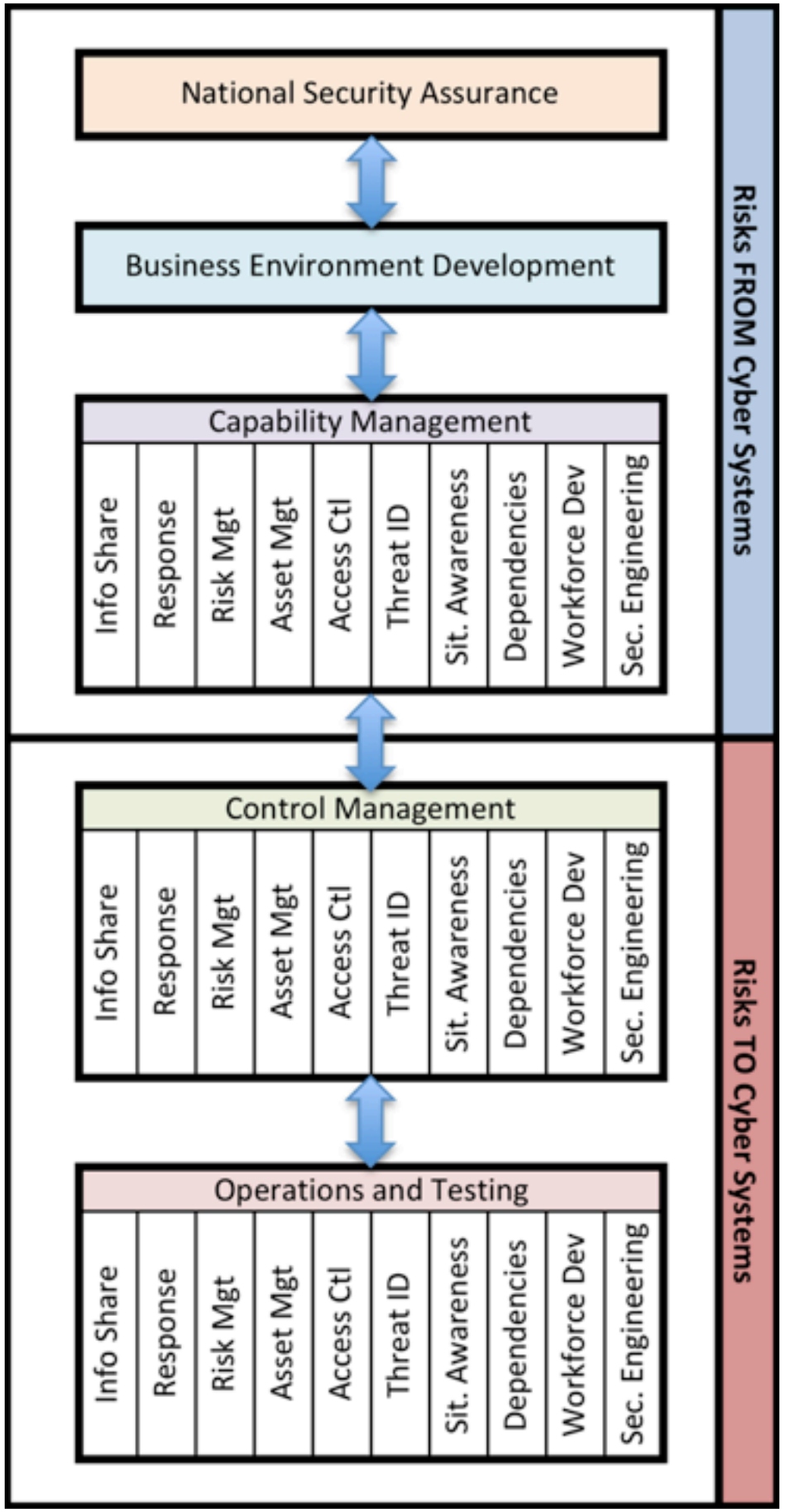
A Cyber Management Protocol Stack

- All layers depend on the ones above and below for success
- Provides common terms
- Structures & Enables discussion
- Allows narrow focus in problem areas
- Highlights completeness
- Will use this later



A Cyber Management Protocol Stack

- National Security Assurance
  - Assure Nation will continue; Diplomacy; Military
- Business Environment
  - Define Common Business Outcome Goals for Cyber security; Describe Environment; Create Common Lexicon
- Capability Management
  - Evaluate capabilities against organizational goals; prioritize resources and investments; adjust capabilities in response to ops data
- Control Management
  - Evaluate conceptual application of best practices, standards,
- Operations & Testing
  - Compare conceptual control placement to actual configurations and threats



Looking at Labels again..

- Lots of different *skills* at top, middle, bottom
- Closer to bottom, more *skills* align with *roles*
- Not-so-much at top for security
- So we have a gap that needs filling...
- Which, by coincidence, is:
  - Where a lot of the references to “cyber security” occur in real life...

So what happens at the top of this stack?

First, defining critical infrastructure...

Critical Infrastructure

What is it...officially?

Primary Documents: HSPD-7/NIPP

- "Homeland Security Presidential Directive-7"
  - Bush. Builds on earlier directive from Clinton
  - Assigns Critical Infrastructure Protection to DHS
- National Infrastructure Protection Plan (NIPP)
  - DHS Plan for Implementation of HSPD-7
- "All" Critical Infrastructure, not just Cyber
  - Most of the people traditionally involved are *not* cyber
  - **This isn't entirely wrong, but causes public disconnect**
- They do require cyber-specific actions from DHS
  - Confusing. One of the reasons for the EO

- http://www.dhs.gov/homeland-security-presidential-directive-7
- http://www.dhs.gov/national-infrastructure-protection-plan

HSPD-7 Policy Statement

"It is the policy of the United States to enhance the protection of our Nation's critical infrastructure and key resources against terrorist acts that could:

- Cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction;
- Impair Federal departments and agencies' abilities to perform essential missions, or to ensure the public's health and safety;
- Undermine State and local government capacities to maintain order and to deliver minimum essential public services;
- Damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services;
- Have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources; or
- Undermine the public's morale and confidence in our national economic and political institutions."

HSPD-7 Policy Statement

RealSpeak Summary:

The U.S. will protect the infrastructure supporting National Cohesion" in Partnership with Industry

Experience says:

- "Protect" doesn't have to be active
- "Protect" really means "Assure Security"
- "Assurance" starts with measuring and only continues to protecting *if* the measurements fail
- Industry: Hint. Hint. Hint.

Primary HSPD-7/NIPP Goals

- Identify Critical Infrastructure
- Prioritize Infrastructure
- Protect
- Report on Progress

- This means: Create specific plans to, in voluntary cooperation with industry, implement the NIPP Risk Management Lifecycle and report annually

Dividing Ownership

- US Government (HSPD-7/NIPP) splits Critical Infrastructure responsibilities into 16 “Sectors”
- Each “Sector” is assigned a “Sector Specific Agency” (“SSA”)
- Assignments are done at a a Department level
  - Some departments assign SSA responsibilities to sub-organizations (e.g. DHS assigning Transportation to TSA)

Chemical: DHS	Financial Services: Treasury
Commercial Facilities: DHS	Food and Agriculture:Agg/HHS
Communications: DHS	Government Facilities: DHS/GSA
Critical Manufacturing: DHS	Healthcare and Public Health: HHS
Dams: DHS	Information Technology: DHS
Defense Industrial Base: DOD	Nuclear: DHS
Emergency Services: DHS	Transportation Systems: TSA/DOT
Energy: DOE	Water and Wastewater Systems:

Sector Specific Agency Responsibilities

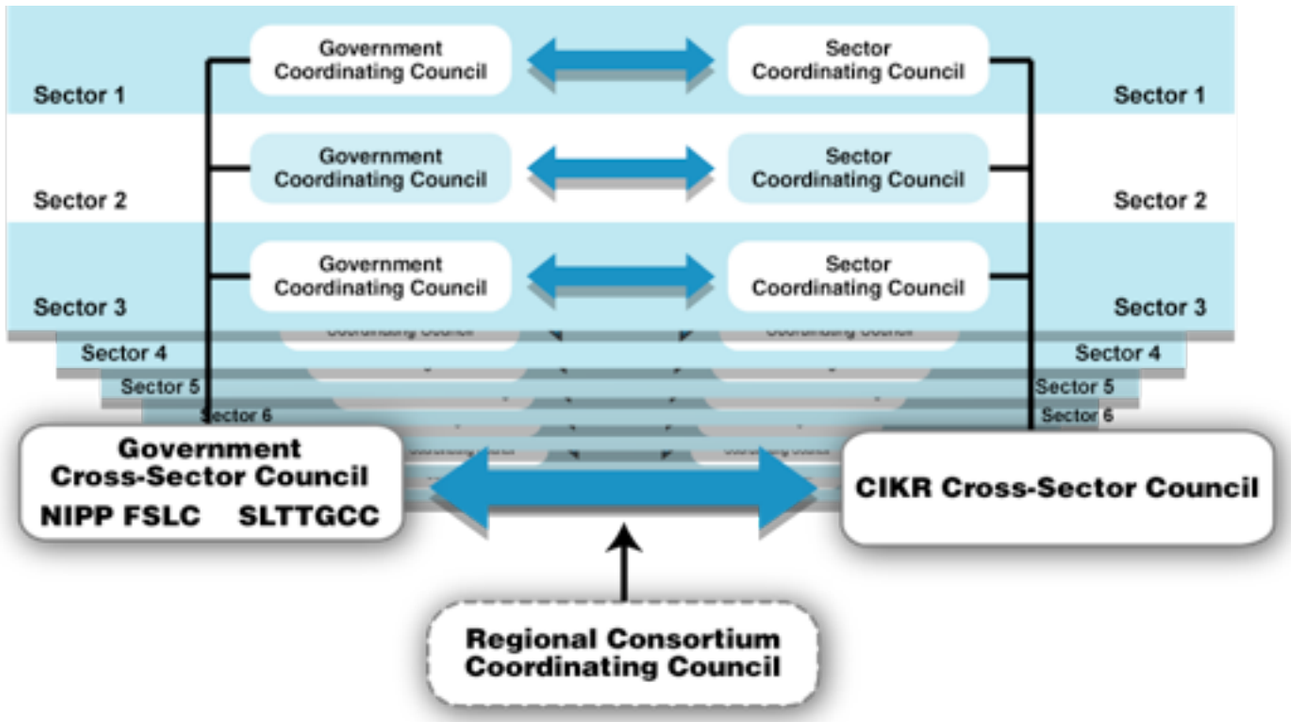
Encourage organizations with information to share with those who need it and **encourage development** of **sector information sharing programs** and mechanisms
Promote education, training, and awareness within the sector in coordination with other government and private sector partners
Identify, prioritize, coordinate federal CCIP activities in sector
Appraise congress of sector's current status and progress in **reducing risk** and **implementing the NIPP**
Increase integration of cyber security efforts with other all hazards protection and response programs
Develop and implement sector risk management program and framework and use to **determine risk priorities of sector** and **coordinate** risk assessment and management **programs**
Support Ad-Hoc DHS data calls
Promote cyber awareness of owners and operators and **program level guidance** for CIKR protection

The DHS “Infrastructure Protection” (IP) organization is responsible for coordinating all of the sectors and assuring the NIPP is being implemented. (This can and has been problematic)

“Public/Private Partnership”

- Formal Term, Formal Constructs
  - Used in many contexts
- Foundation of Critical Infrastructure Protection in the US
- “Voluntary”, “Public”
  - (Limited? Trust issues)
- Alternative is/has been Regulation
- “Weight of Government Burnout” problems
- This is important

HSPD-7/NIPP Partnership Model



- The primary organizational structure for coordinating critical infrastructure efforts and activities.
- Facilitates integration of all partners into planning & ops activities
- Ensure a collaborative approach to critical infrastructure protection.
- The SCCs and corresponding GCCs work in tandem to create a coordinated national framework for Critical Infrastructure protection and resiliency within and across sectors.

Sector Coordinating Councils (SCC's)

- The principal entities for CIKR owners and operators within a sector to coordinate with the government
- Include a broad base of owners, operators, associations, and other entities
- Principal private sector policy coordination and planning entities
- Participate in planning efforts related to reporting for the NIPP
- For information sharing and response, often rely on ISACs and other non-SSA entities
- **Problem: This is probably the first time you're hearing this (also: industry vs citizens)**

Government Coordinating Councils (GCC's)

- The government counterpart for each SCC to enable interagency and cross-jurisdictional coordination within a sector
- Includes representatives from various levels of government (Federal, State, local, or tribal) as appropriate
- Co-chaired by a representative from the designated SSA and DHS IP (**This causes some issues**)
- Coordinates with and supports the efforts of the SCC to plan, implement, and execute the Nation's CIKR protection mission.
- Provides interagency strategic communications, discussion, and coordination at the sector level
- Participates in NIPP planning efforts

What is “CIPAC”?

- DHS Construct: Critical Infrastructure Partnership Advisory Council
- Provides a legal framework for SCC and GCC members to engage in joint CIKR protection-related activities
- Operational mechanism of National Infrastructure Protection Plan (NIPP)
- Provides membership to agencies across all levels of government and the private sector, including membership representing almost 50 percent of the Gross National Product of the United States.
- Allows members of Sector Coordinating Councils (SCC) and Government Coordinating Councils (GCC) to engage in cross-Sector, cross-government coordination.
- Key activities of the CIPAC include information sharing, national planning, and program implementation

CIPAC: Good & Bad

- Good
  - –No FACA, Not owned by government
  - –Managed Engagement
  - –**Must** Have SCC co-chair
- Bad
  - –Control issues (SSA's don't always like it)
  - –Trust Issues (Northwest Rail story)

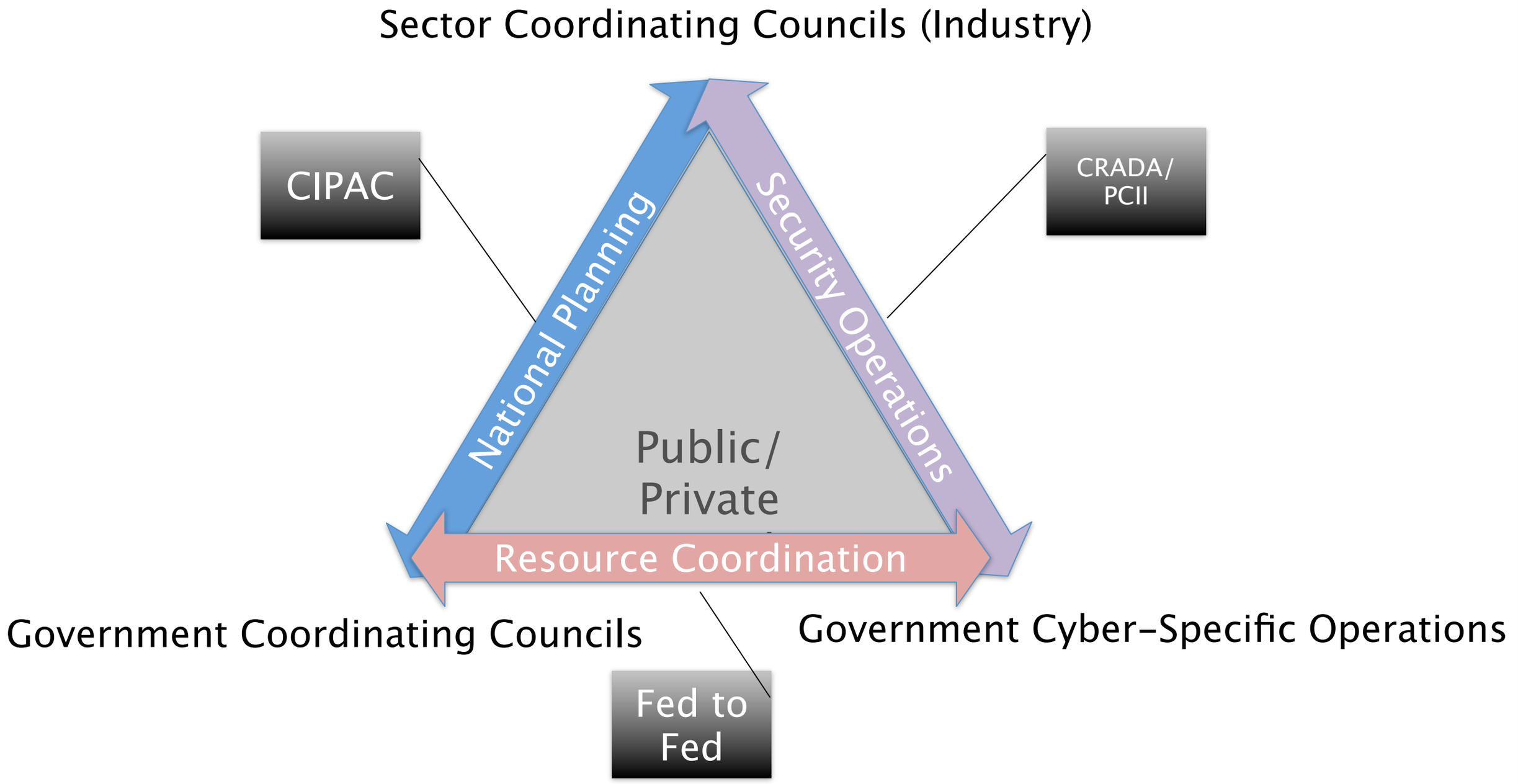
CIPAC Examples

- Industrial Control Systems Joint Working Group (ICSJWG)
- Cross Sector Cyber Security Working Group (CSCSWG)
- Transportation Systems Sector Cybersecurity Working Group (TSSCWG)

What about “real” security?

- NCCIC
- ICS-CERT
- CISCP
- NLE/Cyberstorm
- US-CERT
- ISACs

HSPD-7 & NIPP Environment



New Policies

- Cyber Executive Order:
  - **Aimed at Gov, Not You: Mom reigning in kids**
  - Cyber was already supposed to have been being handled (as we've seen)
  - Attempts to rectify these barriers while keeping in tact most of the fundamental structures already in place.
  - **Heavy focus on "Harmonizing Cyber Efforts"**
    ← Awesome
- Presidential Policy Directive (PPD-21)
  - Not Cyber specific – update to HSPD-7
  - Important
- CISPA
  - Very narrowly focused on information sharing

PPD-21

Three strategic imperatives shall drive the Federal approach to strengthen critical infrastructure security and resilience:

1) Refine and clarify functional relationships across the Federal Government

- Federal functions related to critical infrastructure security and resilience shall be clarified
- There shall be two national critical infrastructure centers operated by DHS – one for physical infrastructure and another for cyber infrastructure.

2) Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government; and

- Enable efficient information exchange through the identification of requirements for data and information formats and accessibility, system interoperability, and redundant systems and alternate capabilities should there be a disruption in the primary systems.

3) Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.

White House Cyber Executive Order

Main Thrusts:

- Improve Information Sharing
- Use business-function driven risk analysis to determine priorities
- Create a framework of standards for reducing risks from cyber security issues to critical infrastructure
- Engage industry to the greatest extent possible, and assure privacy and civil liberties are embedded in the entire process.

DHS/SSA's White House

Executive Order: Section Analysis

1.- 3. Fluff
4. Cybersecurity Information Sharing
5. Privacy and Civil Liberties Protections
6. Consultative Process
7. Baseline Framework to Reduce Cyber Risk to Critical Infrastructure
8. Voluntary Critical Infrastructure Cybersecurity Program
9. Identification of Critical Infrastructure at Greatest Risk
10. Adoption of Framework (Read: Potential Regulation)

Executive Order: Concerns

- Could this infringe on individual freedoms?
  - "Not any more than before"
- Do we have any guarantee of transparency?
  - So far: Chaotic Good
- The government wants my data?
  - Yes. Because they need your data to make theirs actionable for you. But that's not "the point"
- Why so obtuse?
  - Right ideas. Poor Messaging.
  - Married Couple Analogy
- I don't want the government in my space
  - They just need to "assure" their mission
  - It is possible for industry to keep interference to a minimum
- No faith in government agility to get it right
  - Crickets. Real Problem. Will impact success.
- Should it have been so broad?
  - Built into the EO is a process to focus it. It's actually at the right level
- Isn't this just a political goad?
  - Not just. Smart people have worked on it. Useful (Possibly).
- This preempts legislation or ignored existing work
  - No
- Why is this a DHS issue?
  - National cohesion IS DHS's mission – cyber just a part. There is no "singularly cyber" mission. Others have other takes on cyber mission
- What about regulation?
  - This situation might have gotten a little better, more dynamic

Executive Order: NIST Framework

This is so amorphous yet so crucial,
I'm mostly just going to talk to y'all about it

"Framework to Achieve DHS specified Performance Goals"

Industry Driven

"All Inclusive"

Standards vs Standards

Some Vision

Lost in Translation

EO Performance Goals

Balance Rails, Quality Assurance, Soylent Cyber is People!

CISPA

- An executive order cannot change already legislative assigned federal responsibilities

- CISPA handles legal aspects of:
  - Remove legal barriers to information sharing
  - Addressing specific problems associated with industry cybersecurity needing to intersect with the intelligence community.

- My experience as a Fed was that barriers CISPA attempts to do away with were ones often cited by Industry Reps as what they needed.

- **Intent legit, but details?** …

What does cyber security appear to be?

Part II

Cyber Security is (?)...

- Those activities and job roles which synthesize multiple disciplines – both technical and non-technical – to sustainably improve the *environment* for other more technical or tactical security activities, particularly at an industry or national scale and in the context of government laws, policies, mandates, and regulations.

Example Technical Knowledge:

- Threat Landscape
- Attack Architecture
- Defense Architecture
- Experience with operations
- Hacker Mentality
- Basic Principles of your Non-Core tech

Example Non-Technical Knowledge:

- Communication & Facilitation
- Legal/Policy realities
- Business & Industry
- Modeling
- INCIDENT RESPONSE MANAGEMENT
- Self Presentation
- Strategic Thinking

Critical Infrastructure & Cyber Security:

Example Problem Spaces & Initiatives

Example 1: Tools

- **CARMA:** A Risk Management Approach
- **CRR:** A Cyber Resiliency Model
- **CSET:** A Cyber Evaluation Tool
- **ES-C2M2:** A Maturity Model
- **RMP:** A Risk Management Approach
- **NIST Cyber Framework:** Standards
- **Executive Order:** Better Cybersecurity

Example 1: Tools

This year I had the following discussion with a critical infrastructure sector:

Them: “which one of those should industry use or get involved with.”

Me: “All of them”

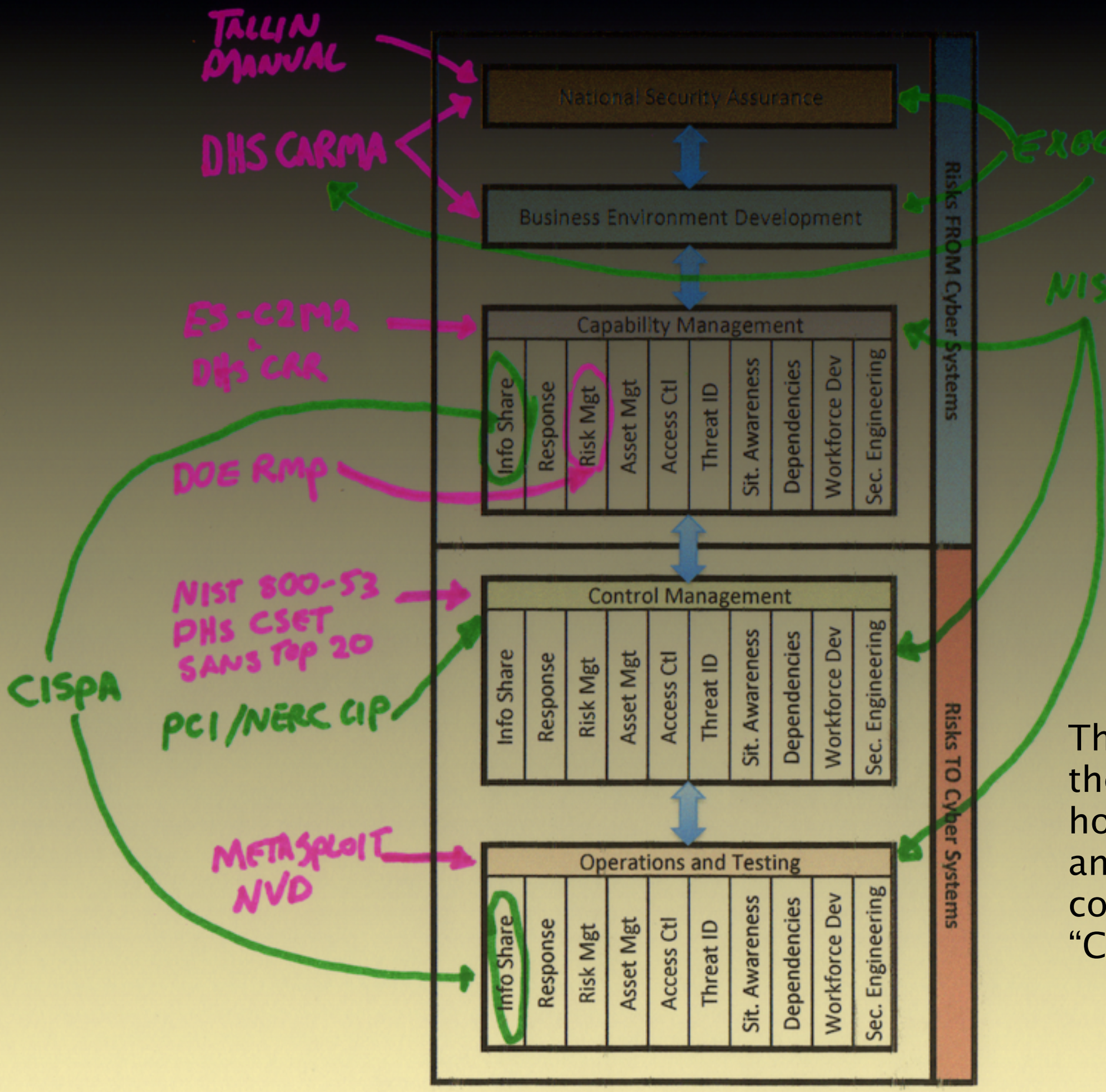
Them: “But we don’t have time, what's the best?”

Me: “But they do different things!”

Them: “It doesn’t look like it…”

What. The. Hell.

Wait! We have a protocol stack…



Clearly, the question made no sense when you look at a structured perspective – they all suit different needs.

The model showed the types of needs, how they fit together, and provided a common reference for "Cyber Security"

Example 1: Tools

- **A bit about these tools for reference…**
- CARMA
  - DHS Cybersecurity And Risk Management Approach
  - Sector-wide model of business-function and value chain driven risks
  - Ties business models and cyber infrastructure
  - No individual business details
  - **Being used in Executive Order process to determine performance goals for NIST Framework**
- ES-C2M2/CRR
  - Electric Sector Capability Maturity Model / DHS Cybersecurity Resilience Model
  - Both look evaluate business maturity and progression in capability domains
  - Neither provides performance goals or context
  - Management link between strategy and execution
- RMP
  - DOE Risk Management Process
  - Slots both into the risk management domain and overlaps everything
- DHS CSET
  - DHS Control Systems Evaluation Tool: Control Catalogue Application Evaluation
- Tallinn Manual
  - Not a gov doc – academic even if NATO – but speaks to international law

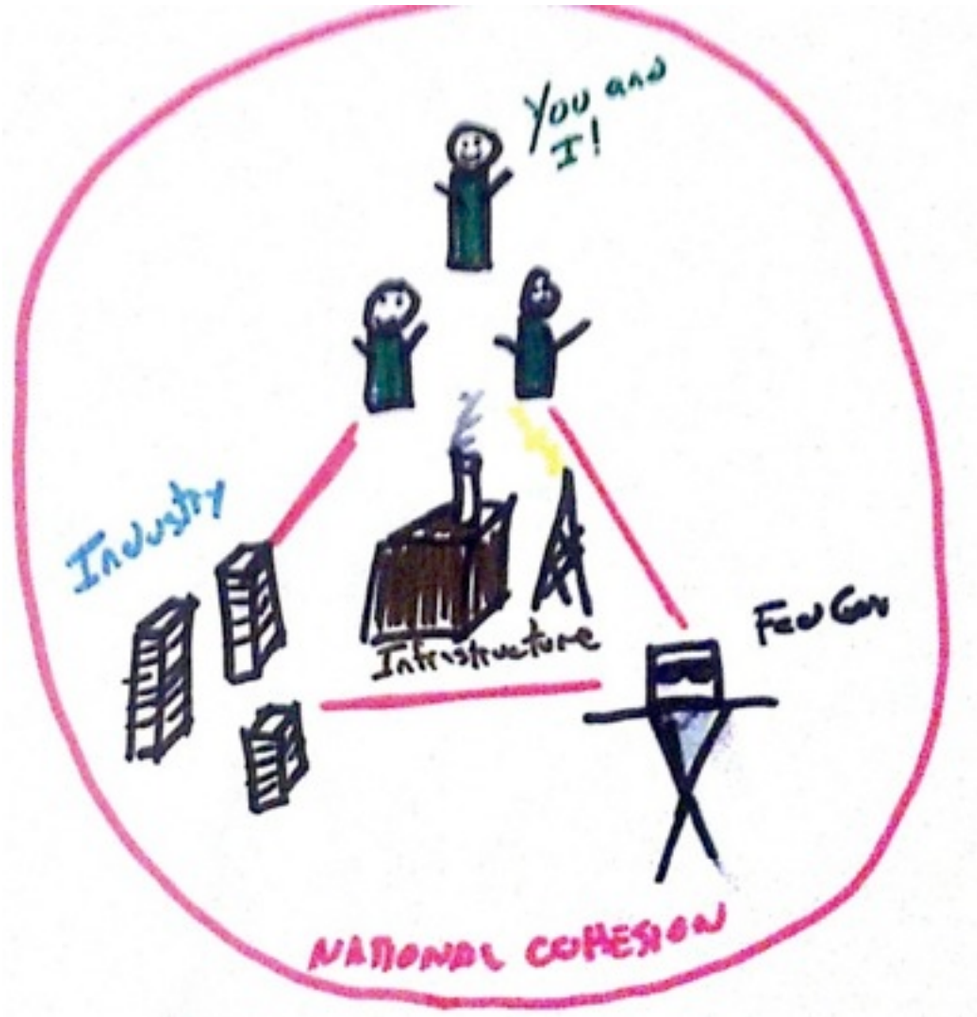
Example 2: Industry vs Gov Scope

- "Incident Response" organizations are often regarded as "Information Sharing" ones
  - Must not forget distinction
  - Missions may conflict and impact sharing
- FBI, Military, and the Intel Community also have potentially conflicting scopes
- **Most importantly: Private Industry vs. Government**

Example 2: Industry vs Gov Scope

CUSTOMERS OF
CYBER SECURITY:

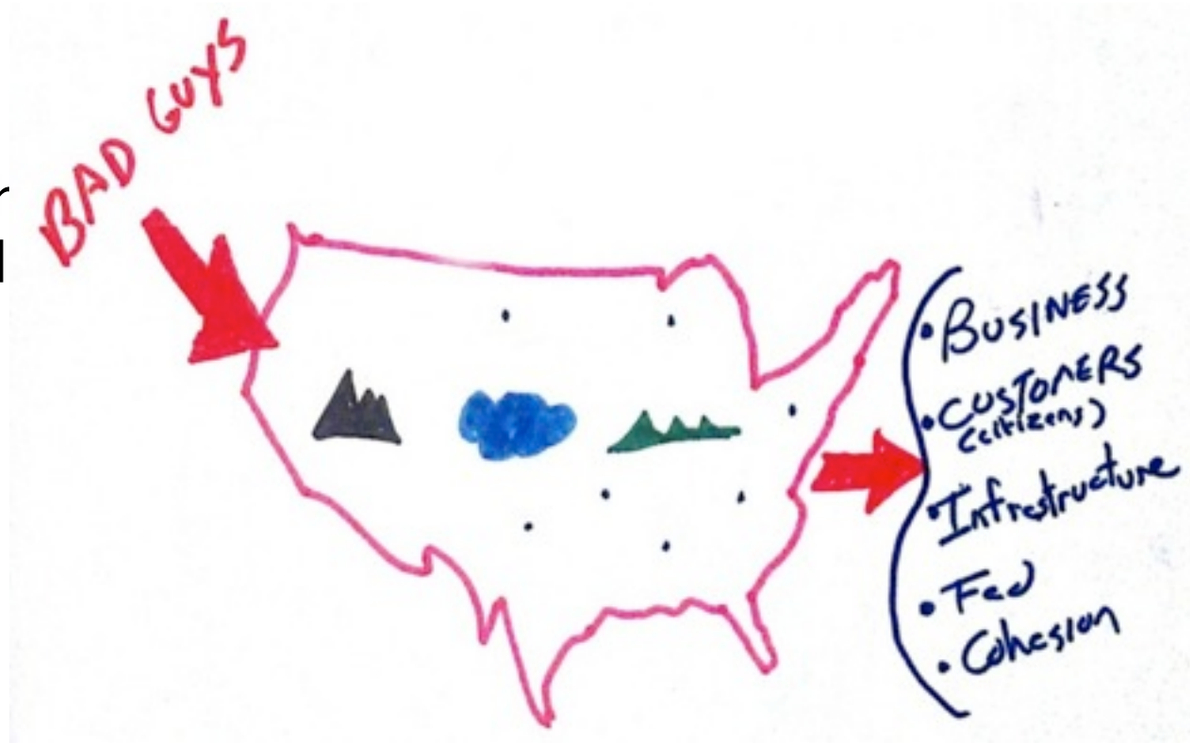
- Citizens
- Individual Businesses
- Industries
- National Infrastructure
- Government infrastructure
- National Cohesion



Overlap.

Example 2: Industry vs Gov Scope

- Contestable Threat Vectors (CTV):
  - Provide defendable space between “bad guys” and targets
  - Imply that there is a space that is *not* th target that must be traversed beforehand
  - “Domains” is used too often IMO
- Historically…
  - Earth
  - Air
  - Water
  - Space (for some value of historically)



Example 2: Industry vs Gov Scope

Government "Security" apparatus responsibilities heavily influenced by geography

- The military protects national sovereignty outside the U.S.
- DHS protects national cohesion; operates on U.S. as whole
- FBI specific aspects of internal U.S. interests
- State & Local government organizations

Example 2: Industry vs Gov Scope

"Along Came a Cyber!!!"

- "Cyberspace" comes along; screws things up
  - Cyber Assets: Targets AND part of a CTV
  - "Customers of Protection" now own a CTV
  - Geographic Protection Schemes break
  - Opaque by Default
- But can have consequences in other CTVs
  - So we can't ignore old physical policy mechanisms
  - "National Guard" example
- "Critical Infrastructure" here but can be used with a lens to provide other views

Other Examples

- Connectedness: Business Support Models (Telvent!)
- CARMA and SSA: Building Trust
- NIST Framework: Collaborative Framing
- Minimum Level of Monitoring: Sustainable Operations
- Corman's Cavalry: A little bit different...

The End!

- Jack Whitsitt
- sintixerr@gmail.com
- http://twitter.com/sintixerr