Continuous Diagnostics and Mitigation Estimating Risk Using Analytics

Managing Cyber Risk Through Improved Data Collection and Analytics

Cybersecurity and Communications
Federal Network Resilience Division
Cybersecurity Performance Management Branch

Cyber Threats: Large and Growing

Bloomberg Businessweek

Yes, the Chinese Army is Spying On You.

The Washin

Pentagon Poi

Chinese Ar ks

Computer

A Department of De says that Chin government

infiltrating, and coul

Iranian Hackers Penetrated US Navy Marine Corps Internet for Four Months

EET JOURNAL.

New York Times

Tw

ma er plants infected

via USB

Investigator

Hack

Depart

During a cyberattack on

personal data of employees a

classified data is leaked.

SECURITY

Windows rabilities doubled IE's Flash male iggest loser

PCWorld

A perfect storm' of cyber attacks

I'd be Fab in your team, eh?

It was so cheesy to fall for my dancer P10

TIME

CYBER WAR

The U.S. rushes to turn computers into tomorrow's weapons of destruction. But how vulnerable is the home front?

BREACHES CAN RESULT IN HUGE COSTS

DIRECTORS MUST WAKE UP TO CYBER THREATS

UK spy chief warns of global cyber threat

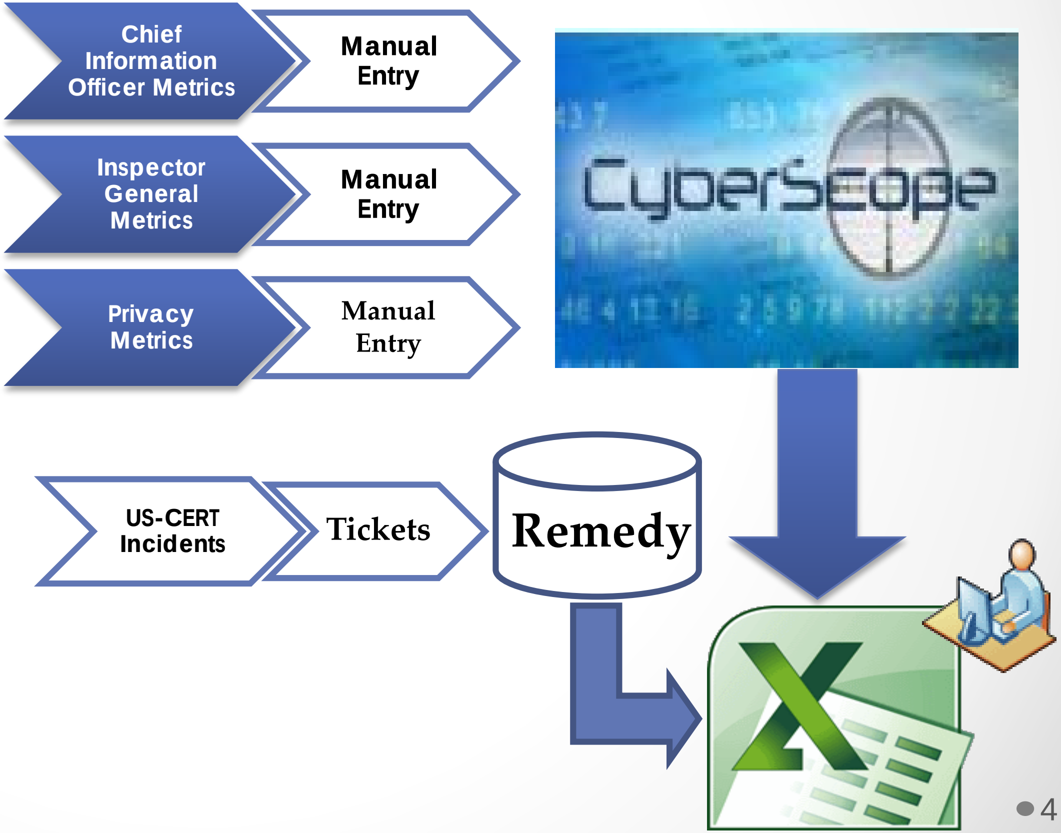
RISK MANAGERS CAN MITIGATE SOFTWARE GLITCHES

CYBER ATTACKS JUST AHEAD

The Theme

- Effectiveness of techniques for collecting, analyzing, and sharing risk factor data enabling us to estimate present and future information security risk levels, at the asset, system, agency/organization and federated level, for the purpose of hardening system defenses thereby improving Federal cyber security postures.

Current Cyber Risk Collection Model for FISMA



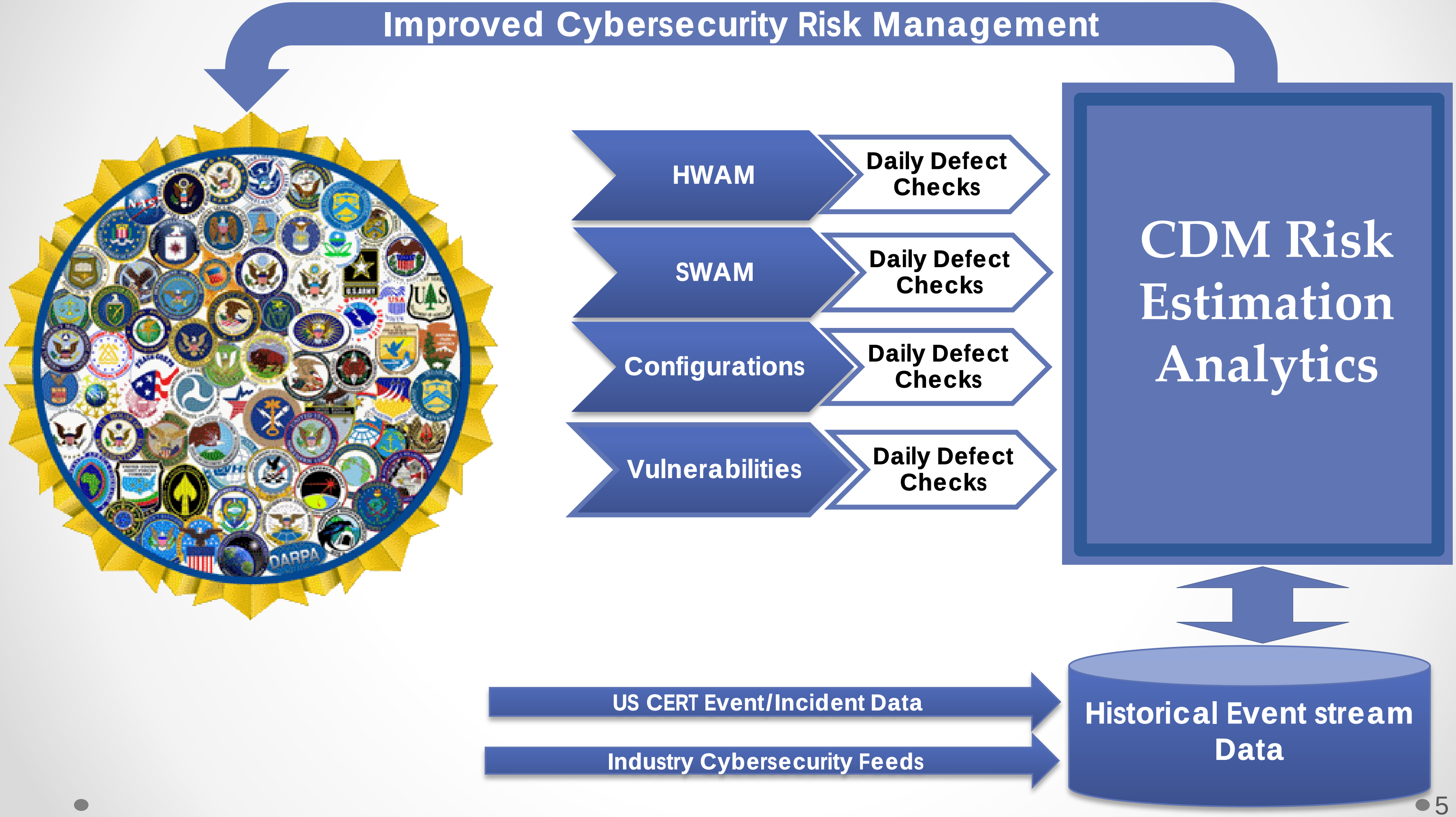
Chief Information Officer Metrics → Manual Entry

Inspector General Metrics → Manual Entry

Privacy Metrics → Manual Entry

US-CERT Incidents → Tickets → Remedy

Future of Federal Risk Analysis



Improved Cybersecurity Risk Management

HWAM

Daily Defect Checks

SWAM

Daily Defect Checks

Configurations

Daily Defect Checks

Vulnerabilities

Daily Defect Checks

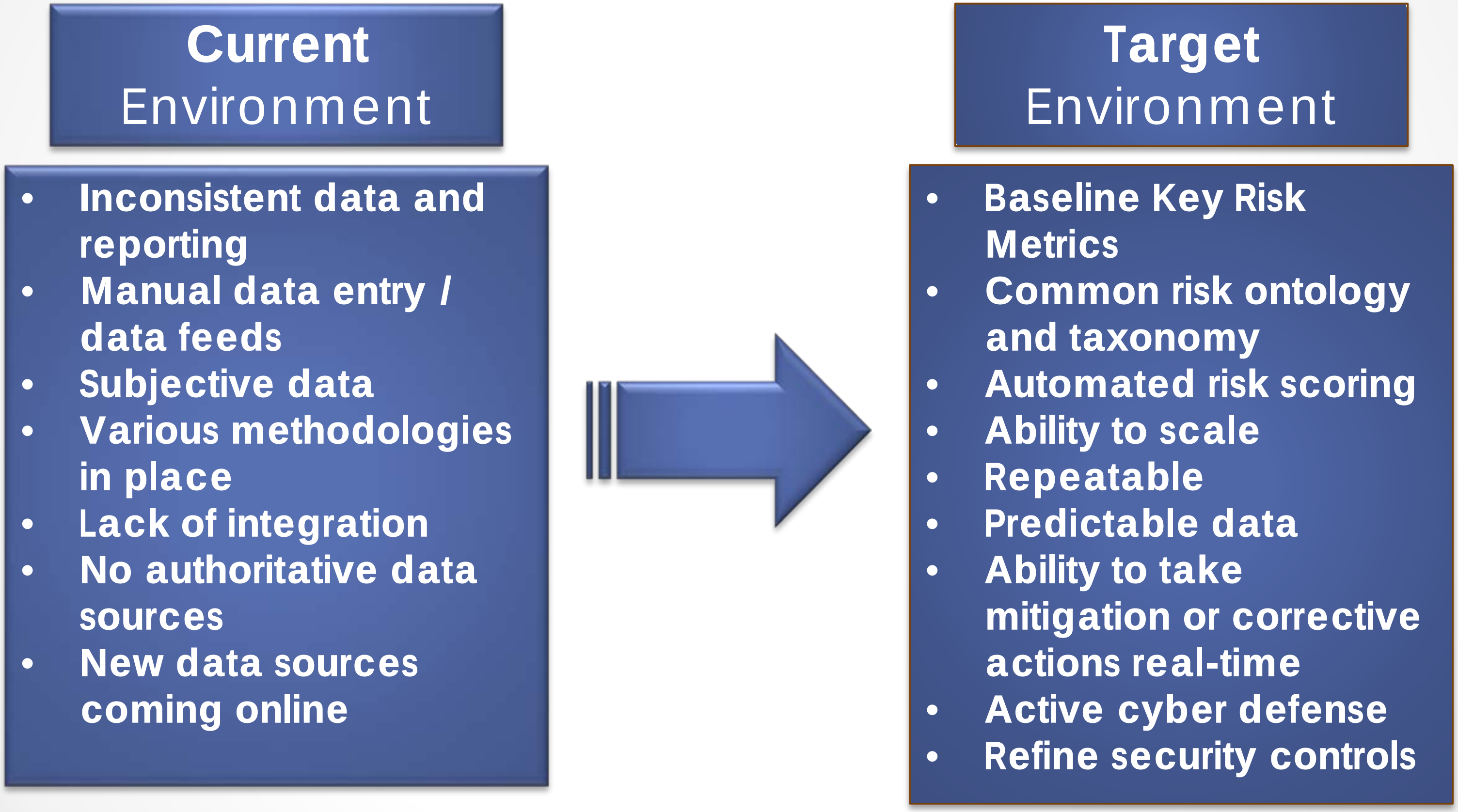
CDM Risk Estimation Analytics

US CERT Event/Incident Data

Industry Cybersecurity Feeds

Historical Event stream Data

Operationalizing Risk – Roadmap



Current Environment

- Inconsistent data and reporting
- Manual data entry / data feeds
- Subjective data
- Various methodologies in place
- Lack of integration
- No authoritative data sources
- New data sources coming online

Target Environment

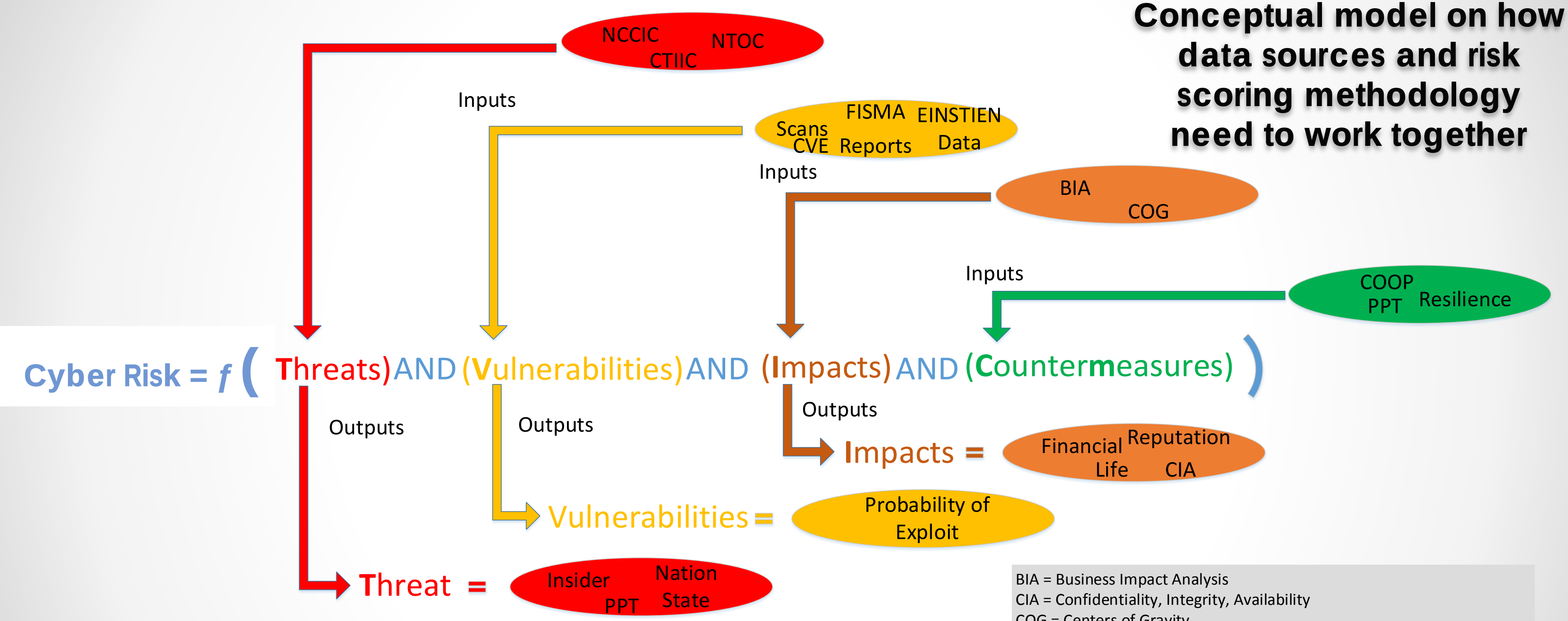
- Baseline Key Risk Metrics
- Common risk ontology and taxonomy
- Automated risk scoring
- Ability to scale
- Repeatable
- Predictable data
- Ability to take mitigation or corrective actions real-time
- Active cyber defense
- Refine security controls

Data of Interest

1. Data Sources
   - **Defect check results** (defects identified within hardware asset management, software asset management, configuration setting management and software vulnerability defense capabilities. CDM suite of products will provide data.
   - Types and sources of **Threat** and **Attack** data will be coming from a variety of sources (Einstein, US-CERT, Industry - e.g., Mandiant, Symantec).
   - To be useful for analysis purposes, the above data will need to be available at the granular (e.g., physical and virtual hardware object) level. This will be a phased approach, as the data collection systems are only being built now.
2. Data Access Restrictions.
   - Agency data is tightly controlled. Significant incentive NOT to share (FOUO). Not public.
3. How data access restrictions could be overcome to appeal to a wider community
   - Business requirements for sharing (what can be shared, how to share it widely) still being identified with the goal of sharing data *without* attribution to specific systems/assets/organizations.

Operationalizing Risk – Data Interaction

Conceptual model on how data sources and risk scoring methodology need to work together



BIA = Business Impact Analysis
CIA = Confidentiality, Integrity, Availability
COG = Centers of Gravity
COOP = Continuity Of Operations Planning
CTIIC = Cyber Threat Intelligence Integration Center
CVE = Common Vulnerability Enumeration
FISMA = Federal Information Security Management Act
NCCIC = National Cybersecurity and Communications Integration Center
NTOC = NSA / CSS Threat Operations Center
PPT = People, Process, Technology

Specific Tasks

- Task description
  1. Verify accuracy of defect check data.
  2. Verify completeness of defect check data.
  3. Evaluate correlations among defects, attacks, and time.
  4. Estimate relative risk of attack from each unmitigated defect
- Metrics to be collected to quantify task performance.
  1. Estimate accuracy percentage, completeness percentage, with confidence intervals.
  2. Typical regression analysis or factor analysis, percentage of variation explained by factors. Dependent variable: occurrence of attack. Independent variables: defects, however defined.
- Method to ground-truth performance metrics.
  1. Modeling Simulations.
  2. Artificial environment.

Challenges

- Verifiable Data Quality
- Resistance to Change
- Scope Creep
- Increased Transparency
- Data Sensitivity
- Inconsistent Risk Scoring

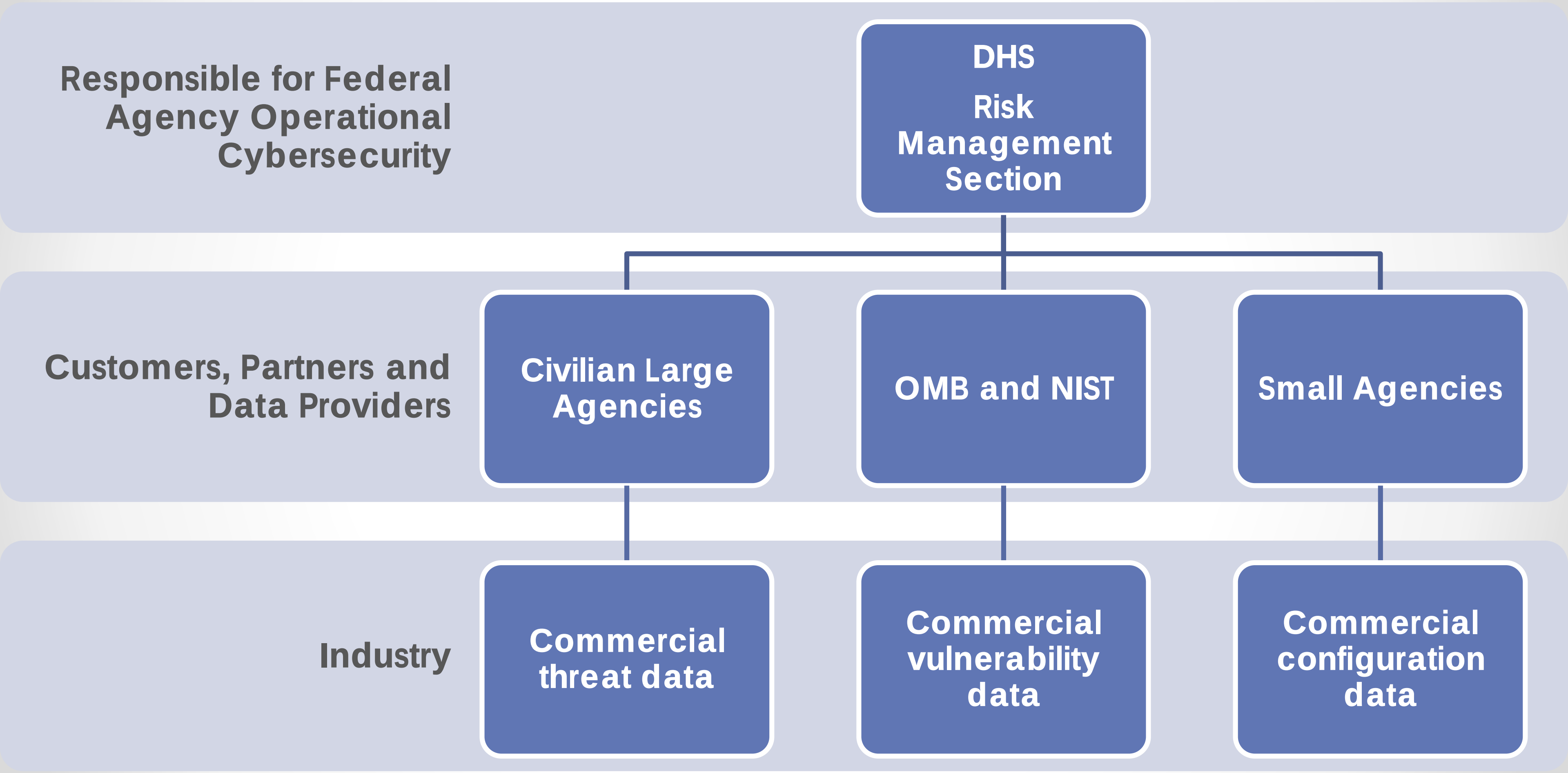
Potential Participants

- Targeted community for participants
  - For source data: individual federal agencies (identity must be protected).
  - Actuarial scientists
  - Cybersecurity researchers
  - Data scientists
- What kind of participation is desired?
  - Independent review (of methods, research design, methods)
  - Data access (for data contributors)
- What do we need/expect from NIST?
  - Don’t know yet.
- Recruitment techniques to:
  - Obtain new participants. Outreach
  - Maintain participation.

Track Organizing Committee

- Co-chairs – Craig Chase and Paul Eavy
  - Program Managers leading research, outreach, data analysis, reporting
- Participants - Jason Carrier Jeannette Cockrell,
  - Section Chiefs responsible for overseeing Risk Management and FISMA implementation
- Data Analysts – Rick LoGalbo and Viet Le
  - Subject matter experts in data collection, analysis and reporting
- Other DHS Organizations – Technical Expertise
  - DHS NCCIC, DHS NSD, DHS S&T
- Customers, Partners and Data Providers
  - OMB, CIO Council, ISIMC
  - NIST
  - Civilian Large Agencies, Small Agencies

Organizations



Responsible for Federal Agency Operational Cybersecurity

DHS

Risk Management Section

Customers, Partners and Data Providers

Civilian Large Agencies

OMB and NIST

Small Agencies

Industry

Commercial threat data

Commercial vulnerability data

Commercial configuration data

Questions

Paul Eavy, Program Manager & DSE Co-Lead
paul.eavy@hq.dhs.gov

Craig Chase, Program Manager & DSE Co-Lead
craig.chase@hq.dhs.gov

Jason Carrier, Risk Management Section Chief
jason.carrier@hq.dhs.gov

Jeannette Cockrell, FISMA Section Chief
jeannette.cockrell@hq.dhs.gov

Rick LoGalbo, DSE Subject Matter Expert
rick.logalbo@hq.dhs.gov

Viet Le, DSE Subject Matter Expert
viet.le@hq.dhs.gov