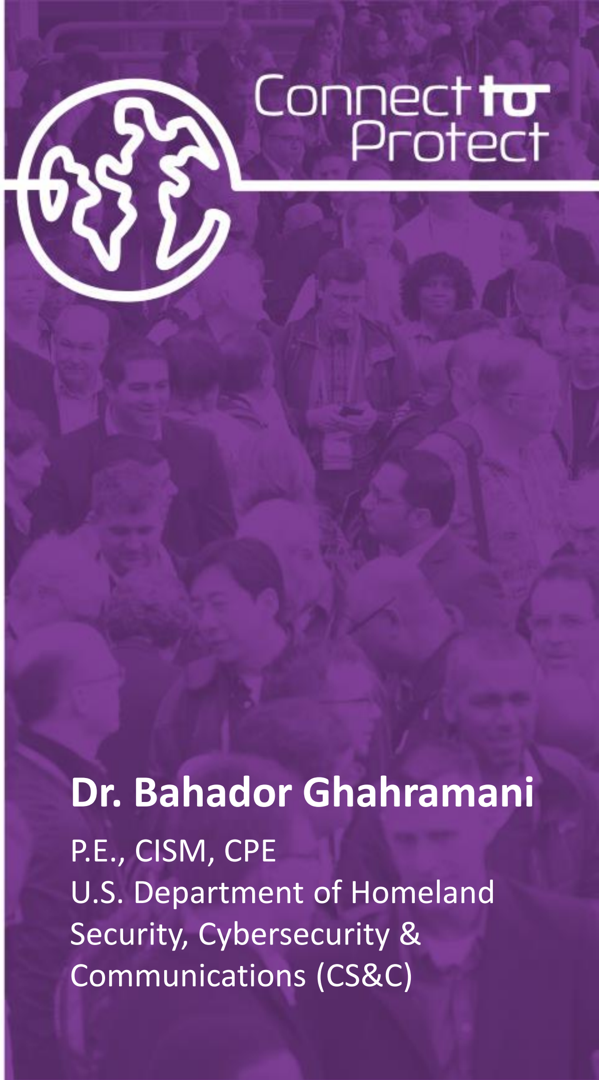
RSA®Conference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID:

National Cybersecurity for Transport Networks (NCTNs)

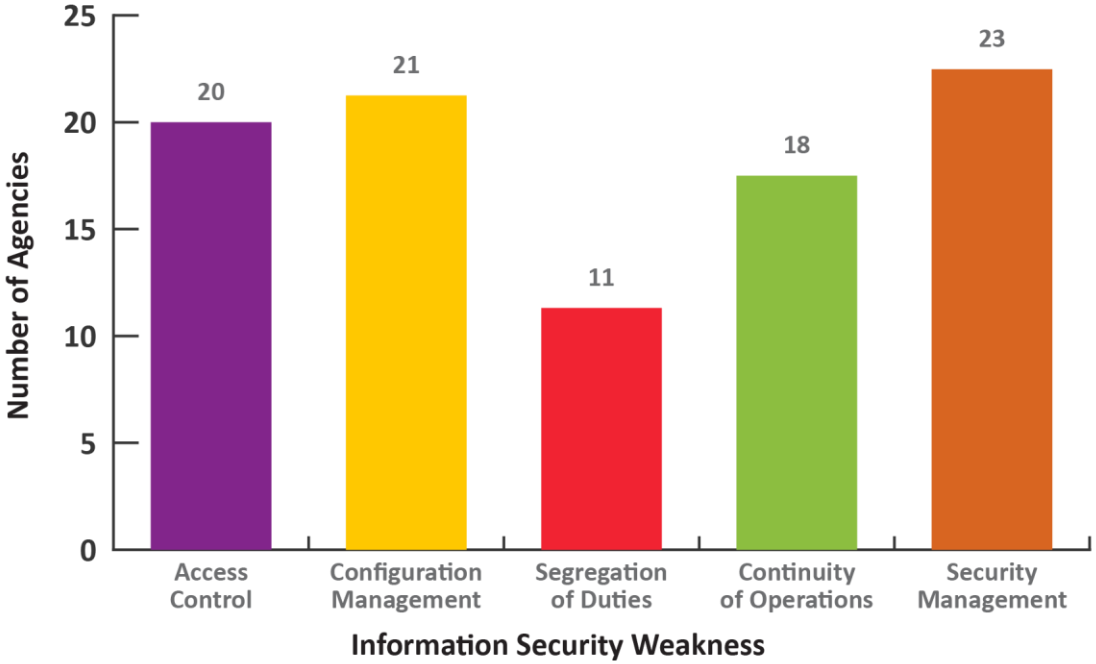


Dr. Bahador Ghahramani

P.E., CISM, CPE
U.S. Department of Homeland Security, Cybersecurity & Communications (CS&C)

#RSAC

U.S. Federal Agencies Vulnerability Categories



(Source: GAO Reports for fiscal year 2014)

Our commitment

*"In the realm of the 21st century cloud technology and dynamic world of Cyberspace, **what transcends in DHS, above all, is its solemn commitment to protect the United States Government and civilian infrastructures from Cyberespionage and Cyberthreats**."*

*"In the arena of Cyberespionage and Cyberthreats, **what resonates with the United States citizens is the protection of their personal freedom, wellbeing, property, and identity** from those who are adamant to harm them."*

Bahador

Introduction

This presentation encompasses a scientific DHS Model that effectively mitigates National Cybersecurity for Transport Networks (NCTNs) risks and vulnerabilities

DHS Components

DHS Components Supporting U.S. Cybersecurity Initiatives		
National Protection and Program Directorate (NPPD)	Federal Law Enforcement Training Center (FLETC)	Domestic Nuclear Protection Office
United States Citizenship and Immigration Services (USCIS)	United States Immigration and Customs Enforcement (ICE)	Office of Health Affairs (OHA)
United States Customs and Border Protection (CBP)	United States Secret Service (USSS)	Office of Intelligence and Analysis
United States Coast Guard (USCG)	Directorate for Management	Office of Operations Coordination
Federal Emergency Management Agency (FEMA)	Science and Technology Directorate	Office of Policy

Source: http://www.dhs.gov/components-directorates-and-offices

NCTNs Definition

NCTNs are:

- The essential focus of the DHS's initiatives to protect global transport infrastructures
- The inseparable part of DHS's mission critical, social interaction, and sensitive cyber transport systems

Model's Goals

- To support supply chain components: PSTNs, CCCT), NGN, and GSMs
- To provide clear distinction between risks and vulnerabilities and how to manage them
- To prevent threats to the Nation's Sixteen Critical Sectors
- To facilitate transports' insurance and privacy legislations, policies, standards, etc.

Model’s Mission

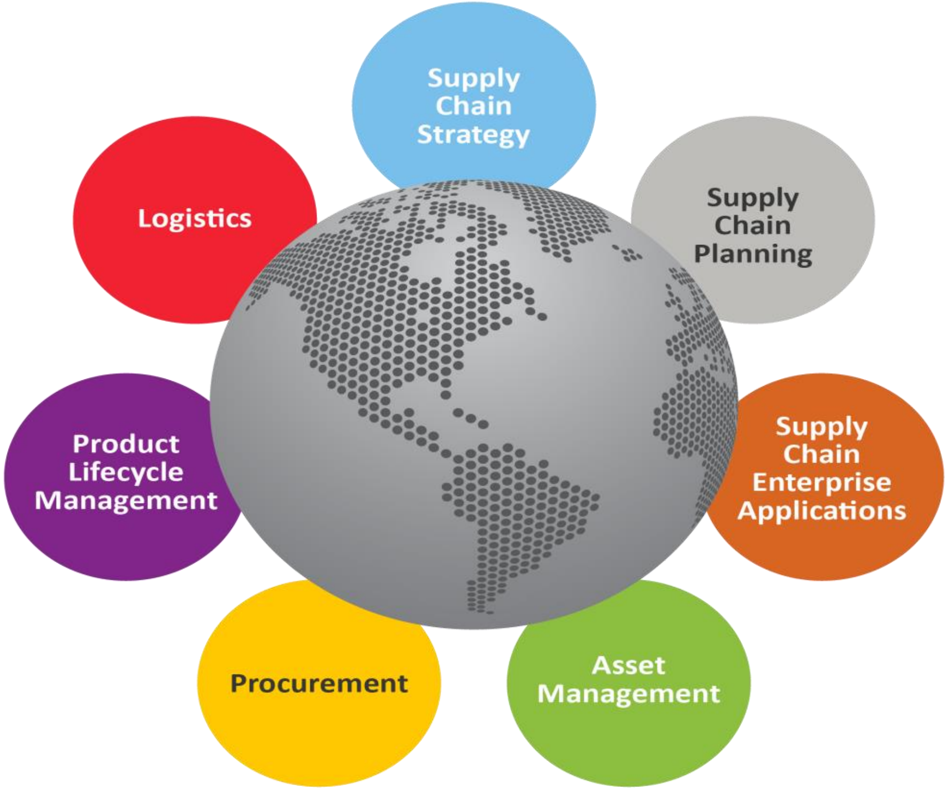
- Continuous mitigation of the real time interconnected GSMs transport interlinks
- Continuous facilitation of the global transport design and development systems

Model’s Technology

Addresses:

- Global transport’s inherent risks and vulnerabilities
- The drivers of the 21st century Cybersecurity transport thrust process

Model’s Global Topology



Model Shall

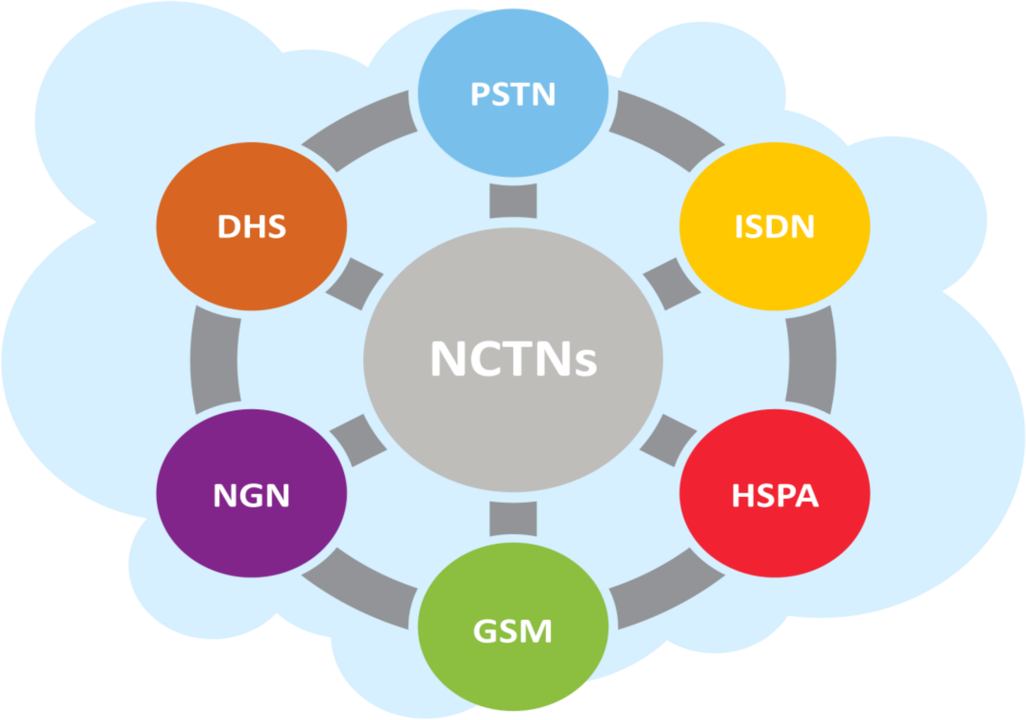
- Interconnect vital segments of today's NCTNs with global Cellular Cloud Computing Technology (CCCT)
- Facilitate voice and data transport systems through Integrated Services Digital Networks (ISDNs), dial-up, and related legacy and modern technologies
- Support implementation of the global transport networks including microwave transmission links and fiber optic capabilities.

Model Provides

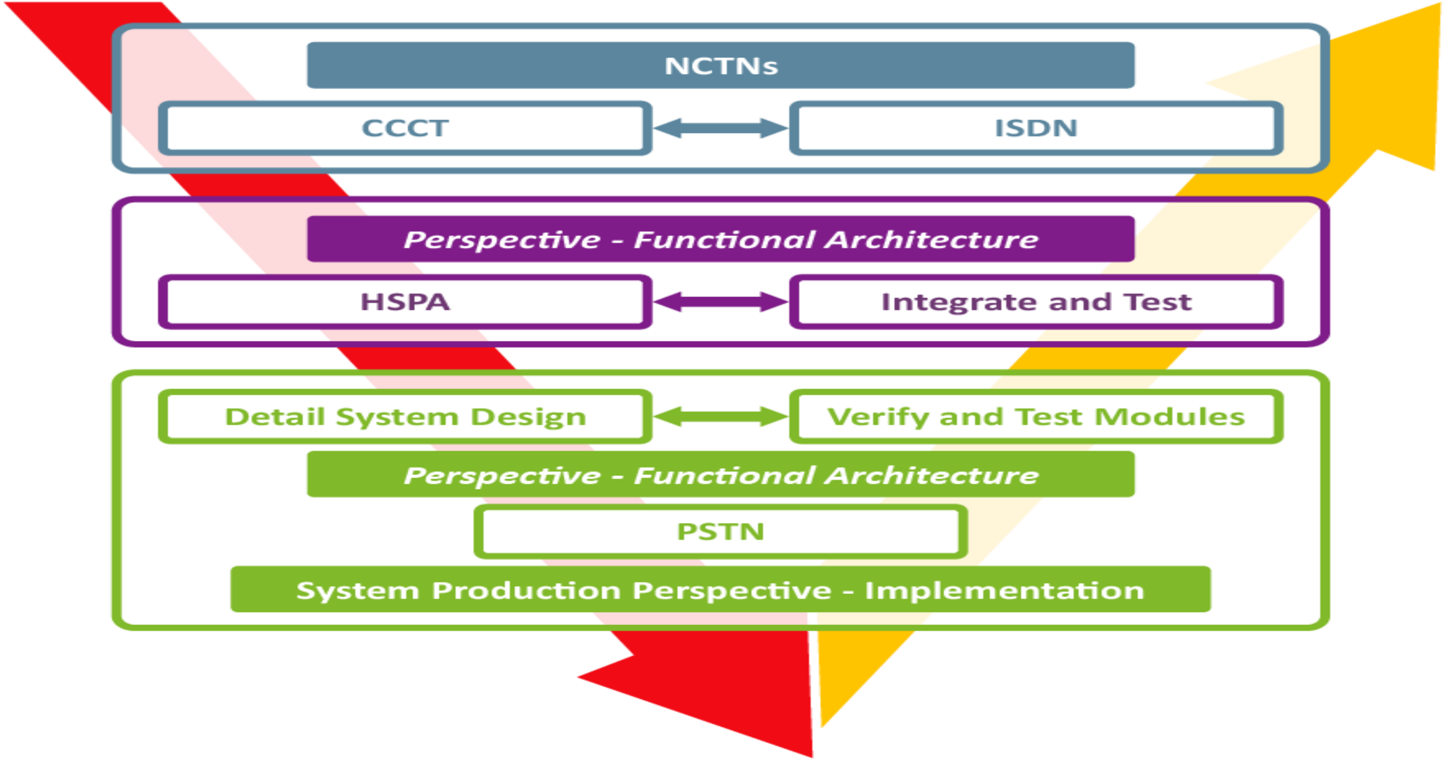
- A continuous mitigation of the global transport’s lifecycle systems
- A secured and effective global architectural Transport Validation and Verification System (TV&VS)

Model’s Support

Cellular Cloud Computing Technology



Model's Systems



NCTNs

CCCT ↔ ISDN

Perspective - Functional Architecture

HSPA ↔ Integrate and Test

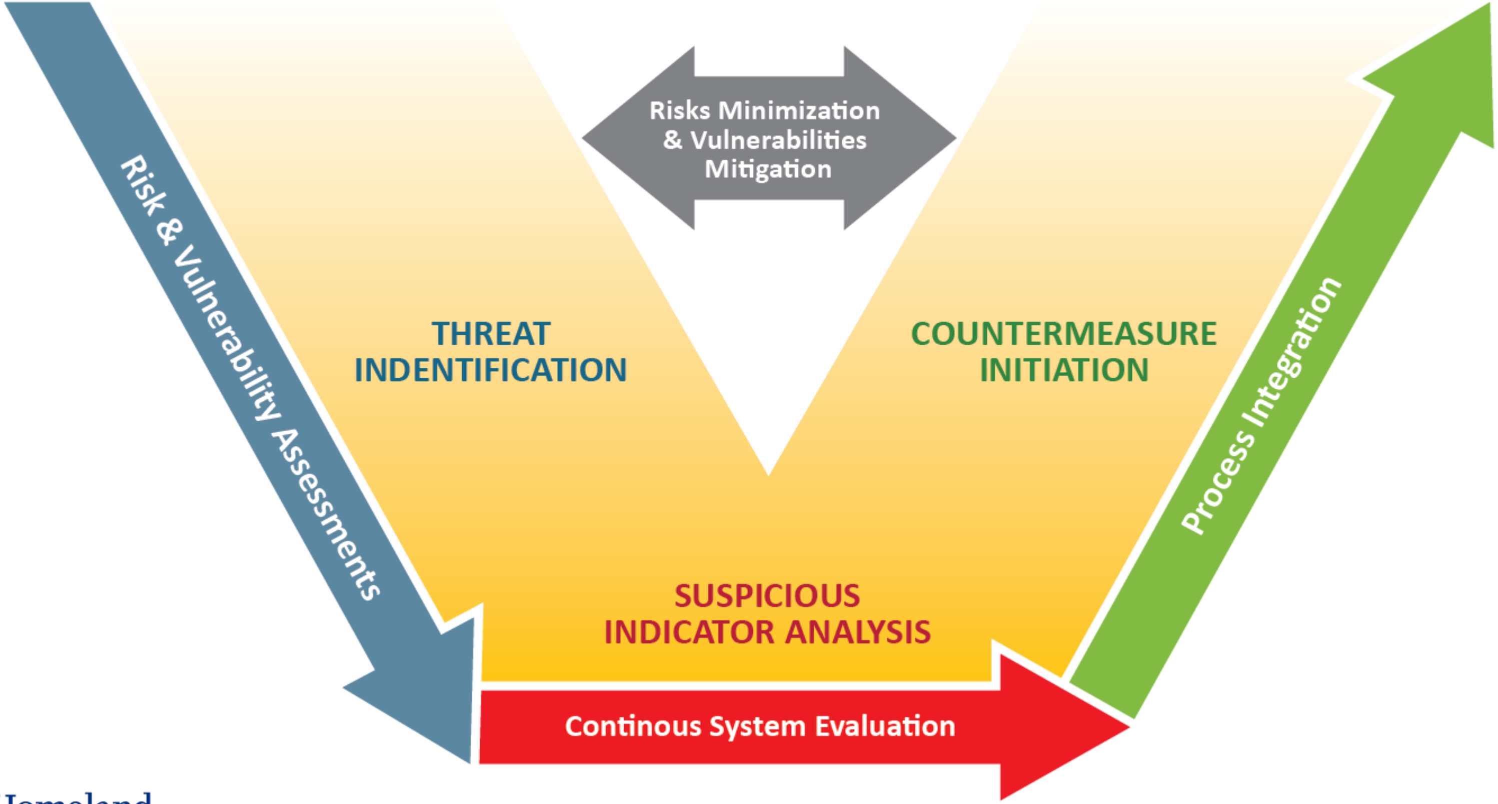
Detail System Design ↔ Verify and Test Modules

Perspective - Functional Architecture

PSTN

System Production Perspective - Implementation

Model's Management Process



Risk & Vulnerability Assessments

THREAT INDENTIFICATION

Risks Minimization & Vulnerabilities Mitigation

COUNTERMEASURE INITIATION

Process Integration

SUSPICIOUS INDICATOR ANALYSIS

Continous System Evaluation

Model's Lifecycle Process – Use Case

Instantaneously after a probable harmful intrusions, the system simultaneously activates its Risks and Vulnerabilities Prevention Methods:

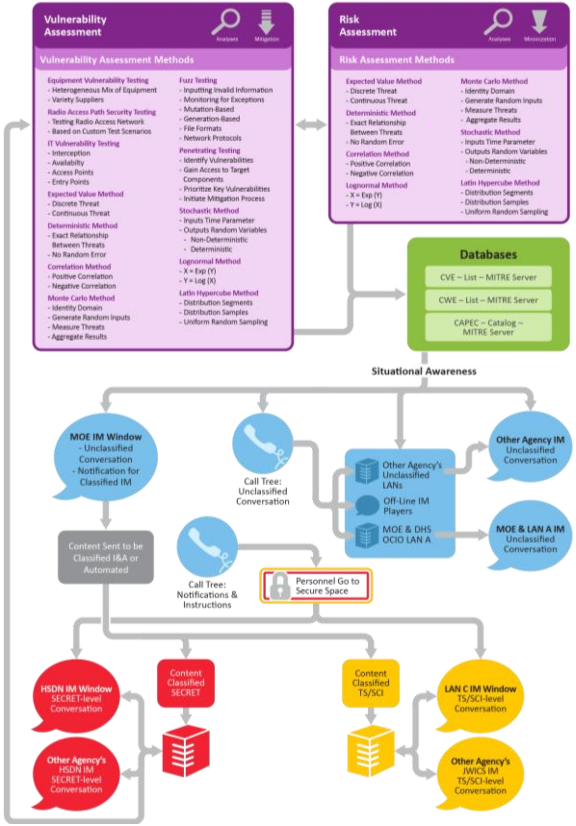
1. Identifies and blocks threat and abnormality before it can harm a DHS NCTNs.
2. It is bridged to MITRE's CVE, CWE, and CAPEC databases to be further analyzed and determined whether any "similar" information exists within these servers.
3. If there is a remedy within MITRE databases, the appropriate "fix action" is activated to prevent the threat and abnormality from harming the NCTNs; then it notifies other Government agencies, private industry, and civilian stakeholders of the incident, remedy, and all other relevant information.
4. If there is no remedy within the MITRE databases, the system continues to block the threat and abnormality until a "fix action" remedy is found by DHS SMEs. As soon as the remedy is found, it is included in the MITRE databases, for future references, and all of the relevant information is circulated to the appropriate Government agencies, industry, and civilian stakeholders as a warning.

Note: Following diagrams will illustrate the above process

Model’s Lifecycle Assessment Diagram

Provides:

- Risk Minimization Assessment Methods
- Vulnerability Mitigation Assessment Methods
- Risk and Vulnerability Auditing Methods



Vulnerability Assessment

Analyses

Mitigation

Vulnerability Assessment Methods

Equipment Vulnerability Testing
- Heterogeneous Mix of Equipment
- Variety Suppliers

Radio Access Path Security Testing
- Testing Radio Access Network
- Based on Custom Test Scenarios

IT Vulnerability Testing
- Interception
- Availabilty
- Access Points
- Entry Points

Expected Value Method
- Discrete Threat
- Continuous Threat

Deterministic Method
- Exact Relationship Between Threats
- No Random Error

Correlation Method
- Positive Correlation
- Negative Correlation

Monte Carlo Method
- Identity Domain
- Generate Random Inputs
- Measure Threats
- Aggregate Results

Fuzz Testing
- Inputting Invalid Information
- Monitoring for Exceptions
- Mutation-Based
- Generation-Based
- File Formats
- Network Protocols

Penetrating Testing
- Identify Vulnerabilities
- Gain Access to Target Components
- Prioritize Key Vulnerabilities
- Initiate Mitigation Process

Stochastic Method
- Inputs Time Parameter
- Outputs Random Variables
  - Non-Deterministic
  - Deterministic

Lognormal Method
- X = Exp (Y)
- Y = Log (X)

Latin Hypercube Method
- Distribution Segments
- Distribution Samples
- Uniform Random Sampling

Risk Assessment

Analyses

Minimization

Risk Assessment Methods

Expected Value Method
- Discrete Threat
- Continuous Threat

Deterministic Method
- Exact Relationship Between Threats
- No Random Error

Correlation Method
- Positive Correlation
- Negative Correlation

Lognormal Method
- X = Exp (Y)
- Y = Log (X)

Monte Carlo Method
- Identity Domain
- Generate Random Inputs
- Measure Threats
- Aggregate Results

Stochastic Method
- Inputs Time Parameter
- Outputs Random Variables
  - Non-Deterministic
  - Deterministic

Latin Hypercube Method
- Distribution Segments
- Distribution Samples
- Uniform Random Sampling

Databases

CVE – List – MITRE Server

CWE – List – MITRE Server

CAPEC – Catalog – MITRE Server

Situational Awareness

MOE IM Window
- Unclassified Conversation
- Notification for Classified IM

Call Tree: Unclassified Conversation

Other Agency’s Unclassified LANs

Off-Line IM Players

MOE & DHS OCIO LAN A

Other Agency IM Unclassified Conversation

MOE & LAN A IM Unclassified Conversation

Content Sent to be Classified I&A or Automated

Call Tree: Notifications & Instructions

Personnel Go to Secure Space

HSDN IM Window SECRET-level Conversation

Other Agency’s HSDN IM SECRET-level Conversation

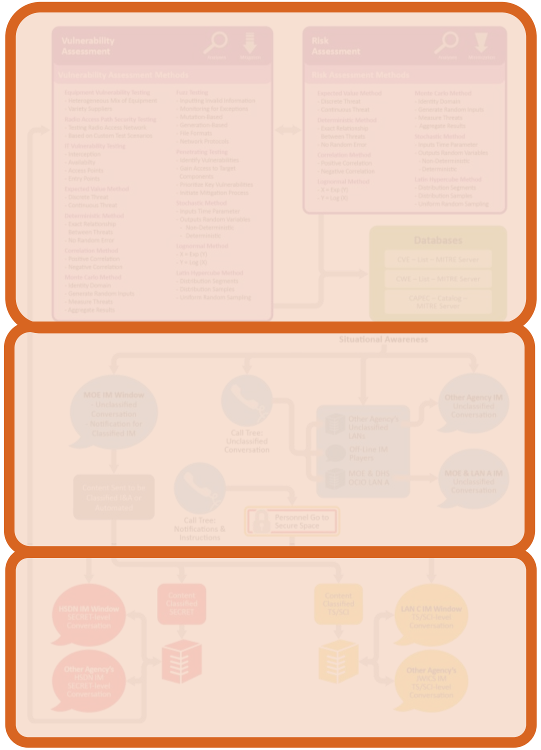
Content Classified SECRET

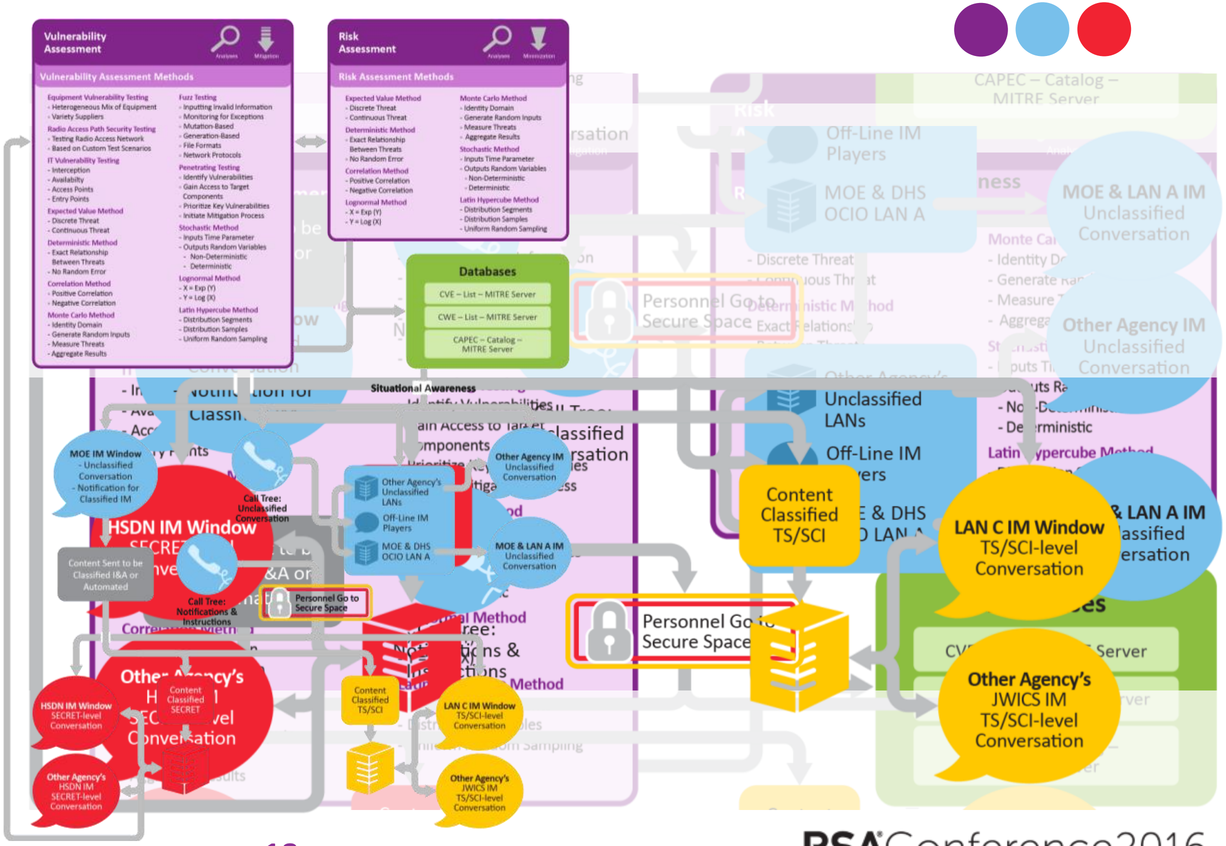
Content Classified TS/SCI

LAN C IM Window TS/SCI-level Conversation

Other Agency’s JWICS IM TS/SCI-level Conversation

Model's Lifecycle Assessment Diagram





Vulnerability Assessment

Vulnerability Assessment Methods

Equipment Vulnerability Testing
- Heterogeneous Mix of Equipment
- Variety Suppliers

Radio Access Path Security Testing
- Testing Radio Access Network
- Based on Custom Test Scenarios

IT Vulnerability Testing
- Interception
- Availabity
- Access Points
- Entry Points

Expected Value Method
- Discrete Threat
- Continuous Threat

Deterministic Method
- Exact Relationship Between Threats
- No Random Error

Correlation Method
- Positive Correlation
- Negative Correlation

Monte Carlo Method
- Identity Domain
- Generate Random Inputs
- Measure Threats
- Aggregate Results

Fuzz Testing
- Inputting Invalid Information
- Monitoring for Exceptions
- Mutation-Based
- Generation-Based
- File Formats
- Network Protocols

Penetrating Testing
- Identify Vulnerabilities
- Gain Access to Target Components
- Prioritize Key Vulnerabilities
- Initiate Mitigation Process

Stochastic Method
- Inputs Time Parameter
- Outputs Random Variables
  - Non-Deterministic
  - Deterministic

Lognormal Method
- X = Exp (Y)
- Y = Log (X)

Latin Hypercube Method
- Distribution Segments
- Distribution Samples
- Uniform Random Sampling

Risk Assessment

Risk Assessment Methods

Expected Value Method
- Discrete Threat
- Continuous Threat

Deterministic Method
- Exact Relationship Between Threats
- No Random Error

Correlation Method
- Positive Correlation
- Negative Correlation

Lognormal Method
- X = Exp (Y)
- Y = Log (X)

Monte Carlo Method
- Identity Domain
- Generate Random Inputs
- Measure Threats
- Aggregate Results

Stochastic Method
- Inputs Time Parameter
- Outputs Random Variables
  - Non-Deterministic
  - Deterministic

Latin Hypercube Method
- Distribution Segments
- Distribution Samples
- Uniform Random Sampling

Databases
- CVE – List – MITRE Server
- CWE – List – MITRE Server
- CAPEC – Catalog – MITRE Server

Situational Awareness

MOE IM Window
- Unclassified Conversation
- Notification for Classified IM

Call Tree: Unclassified Conversation

Other Agency's Unclassified LANs

Off-Line IM Players

MOE & DHS OCIO LAN A

Other Agency IM Unclassified Conversation

MOE & LAN A IM Unclassified Conversation

HSDN IM Window SECRET-level Conversation

Content Sent to be Classified I&A or Automated

Call Tree: Notifications & Instructions

Personnel Go to Secure Space

Other Agency's HSDN IM SECRET-level Conversation

Content Classified SECRET

Content Classified TS/SCI

LAN C IM Window TS/SCI-level Conversation

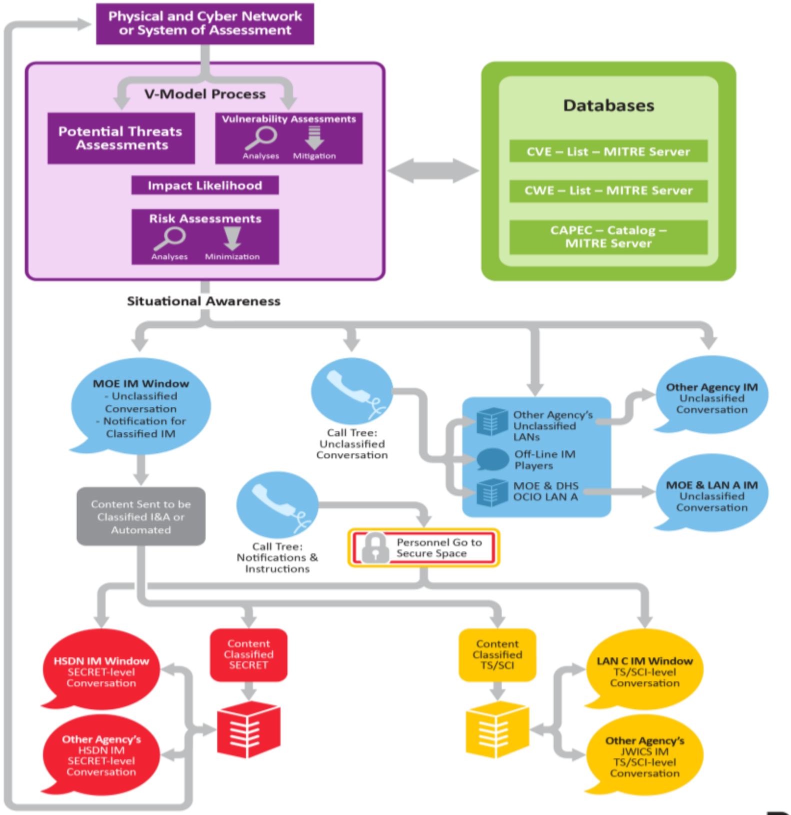
Other Agency's JWICS IM TS/SCI-level Conversation

CAPEC – Catalog – MITRE Server
Off-Line IM Players
MOE & DHS OCIO LAN A
MOE & LAN A IM Unclassified Conversation
Other Agency IM Unclassified Conversation
Personnel Go to Secure Space
Content Classified TS/SCI
LAN C IM Window TS/SCI-level Conversation
Other Agency's JWICS IM TS/SCI-level Conversation
Unclassified LANs
Off-Line IM Players
Other Agency's HSDN IM SECRET-level Conversation
HSDN IM Window SECRET-level Conversation

Model's Lifecycle Components

Supports:

- Physical and Cyber Networks
- Cybersecurity Architectures
- Cellular Cloud Computing Technologies



Physical and Cyber Network or System of Assessment

V-Model Process

Potential Threats Assessments

Vulnerability Assessments

Analyses

Mitigation

Impact Likelihood

Risk Assessments

Analyses

Minimization

Databases

CVE – List – MITRE Server

CWE – List – MITRE Server

CAPEC – Catalog – MITRE Server

Situational Awareness

MOE IM Window
- Unclassified Conversation
- Notification for Classified IM

Call Tree: Unclassified Conversation

Other Agency's Unclassified LANs

Off-Line IM Players

MOE & DHS OCIO LAN A

Other Agency IM Unclassified Conversation

MOE & LAN A IM Unclassified Conversation

Content Sent to be Classified I&A or Automated

Call Tree: Notifications & Instructions

Personnel Go to Secure Space

HSDN IM Window SECRET-level Conversation

Content Classified SECRET

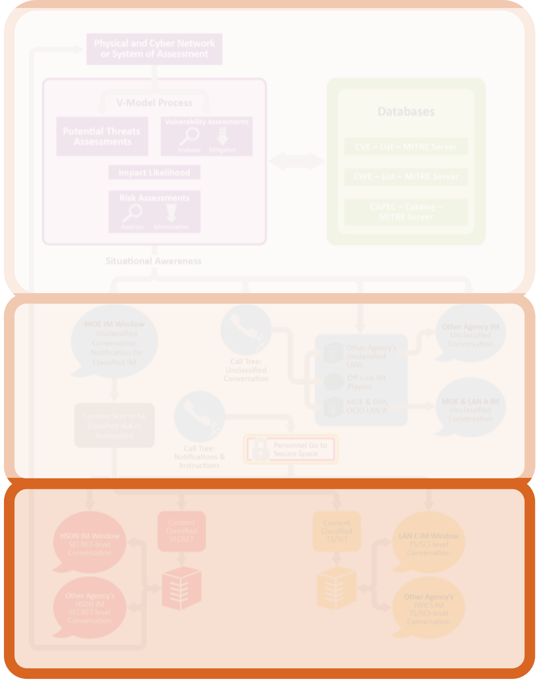
Other Agency's HSDN IM SECRET-level Conversation

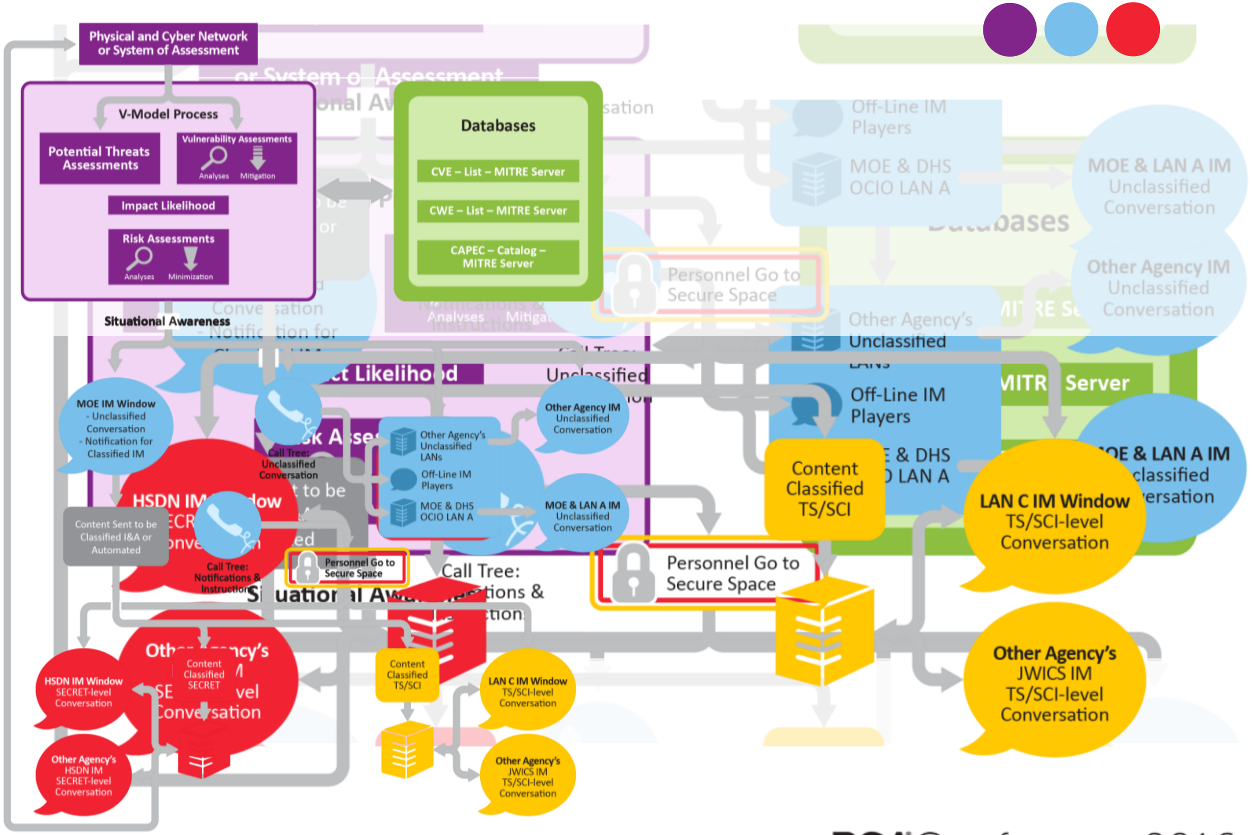
Content Classified TS/SCI

LAN C IM Window TS/SCI-level Conversation

Other Agency's JWICS IM TS/SCI-level Conversation

Model's Lifecycle Components

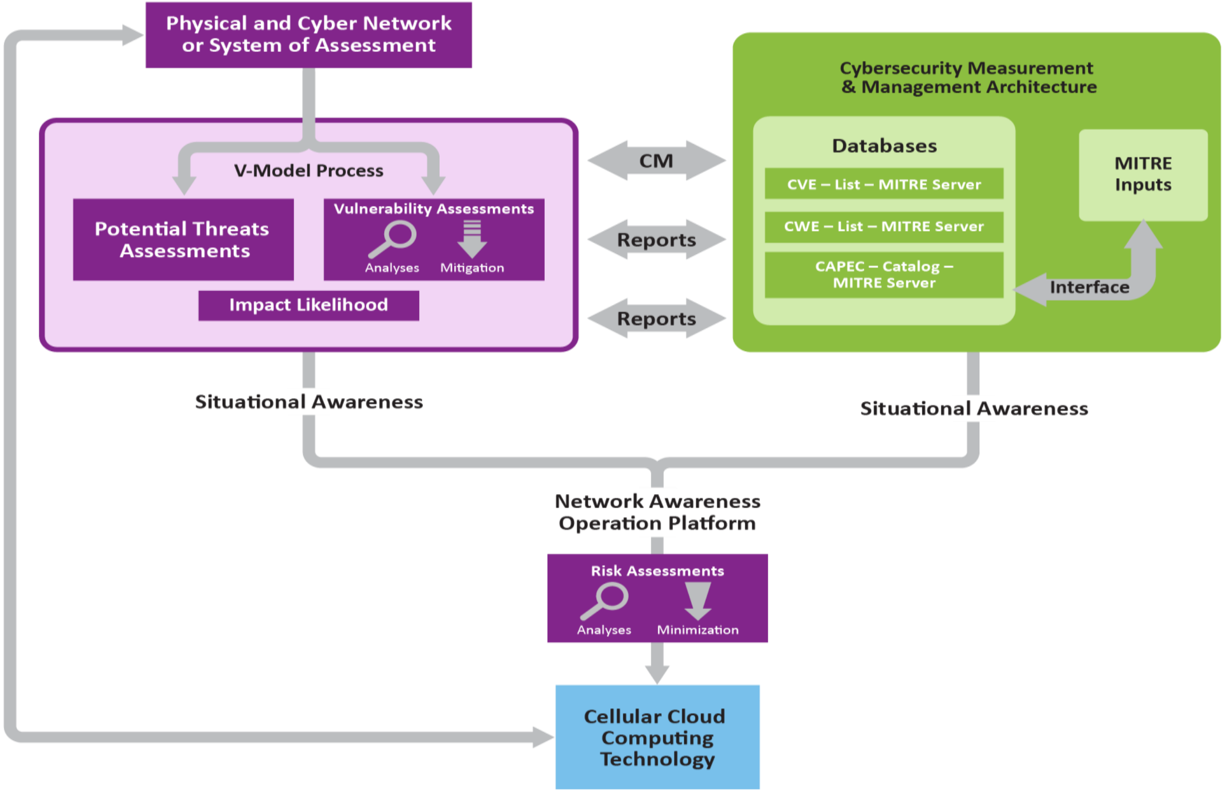



Physical and Cyber Network or System of Assessment
V-Model Process
Potential Threats Assessments
Vulnerability Assessments
Analyses
Mitigation
Impact Likelihood
Risk Assessments
Analyses
Minimization
Situational Awareness
Databases
CVE – List – MITRE Server
CWE – List – MITRE Server
CAPEC – Catalog – MITRE Server
MOE IM Window - Unclassified Conversation - Notification for Classified IM
Call Tree: Unclassified Conversation
Other Agency's Unclassified LANs
Off-Line IM Players
MOE & DHS OCIO LAN A
Other Agency IM Unclassified Conversation
MOE & LAN A IM Unclassified Conversation
Content Sent to be Classified I&A or Automated
Call Tree: Notifications & Instructions
Personnel Go to Secure Space
HSDN IM Window SECRET-level Conversation
Content Classified SECRET
Other Agency's HSDN IM SECRET-level Conversation
Content Classified TS/SCI
LAN C IM Window TS/SCI-level Conversation
Other Agency's JWICS IM TS/SCI-level Conversation

Model's Lifecycle Engineering Process

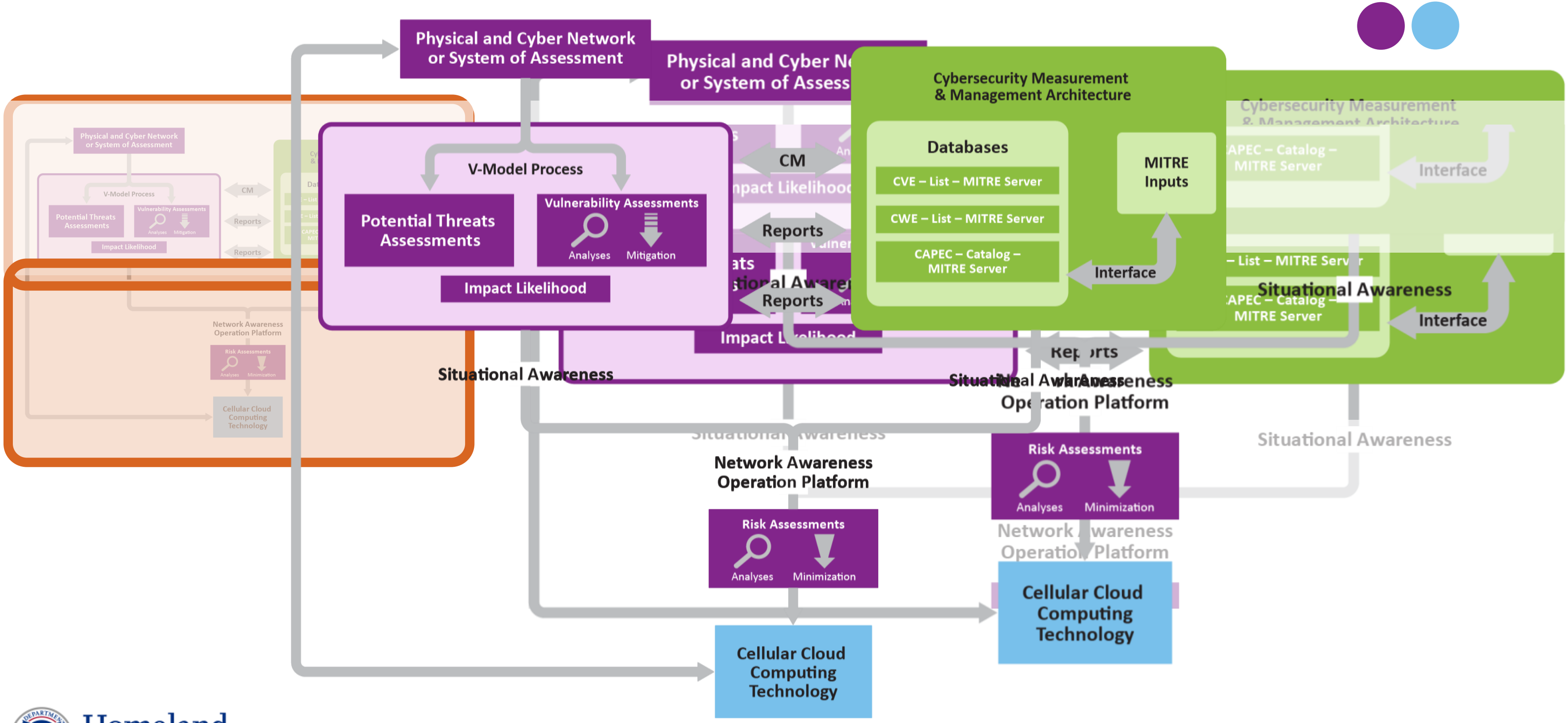
Facilitates:

- Strategy and Logistics
- Enterprise Application
- Asset Management
- Procurement Management
- Product Management


Physical and Cyber Network or System of Assessment
V-Model Process
Potential Threats Assessments
Vulnerability Assessments
Analyses
Mitigation
Impact Likelihood
CM
Reports
Reports
Cybersecurity Measurement & Management Architecture
Databases
CVE – List – MITRE Server
CWE – List – MITRE Server
CAPEC – Catalog – MITRE Server
MITRE Inputs
Interface
Situational Awareness
Situational Awareness
Network Awareness Operation Platform
Risk Assessments
Analyses
Minimization
Cellular Cloud Computing Technology

Homeland Security

Model’s Lifecycle Engineering Process


Physical and Cyber Network or System of Assessment
V-Model Process
Potential Threats Assessments
Vulnerability Assessments
Analyses
Mitigation
Impact Likelihood
Situational Awareness
CM
Reports
Reports
Physical and Cyber Ne
or System of Assess
Cybersecurity Measurement & Management Architecture
Databases
CVE – List – MITRE Server
CWE – List – MITRE Server
CAPEC – Catalog – MITRE Server
MITRE Inputs
Interface
Cybersecurity Measurement & Management Architecture
APEC – Catalog – MITRE Server
Interface
– List – MITRE Server
APEC – Catalog – MITRE Server
Situational Awareness
Interface
Reports
Situational Awareness
Operation Platform
Situational Awareness
Situational Awareness
Network Awareness Operation Platform
Risk Assessments
Analyses
Minimization
Cellular Cloud Computing Technology
Risk Assessments
Analyses
Minimization
Network Awareness Operation Platform
Cellular Cloud Computing Technology
Physical and Cyber Network or System of Assessment
V-Model Process
Potential Threats Assessments
Vulnerability Assessments
Analyses
Mitigation
Impact Likelihood
CM
Reports
Reports
Network Awareness Operation Platform
Risk Assessments
Analyses
Minimization
Cellular Cloud Computing Technology

Model’s Practical Applications

The Model’s practical applications entail:

- Establishing a National Platform for NCTNs supply chain security
- Improving secure trade flow of the most recent information, hardware, software, firmware, and interfaces
- Supporting the development and implementation of global telecommunication supply chain security measures by establishing a harmonious supply chain security initiative
- Stresses the Human Factors
- Encourages the definition and implementation of common NCTNs platform

Model‘s Transformation to Reality

- Model is developed and approved
- Related White Paper is circulated and staffed
- Budget in process
- Production timeline in process

DHS SMEs Support

A few of the Randomly Selected DHS SMEs Testimonials

Mike Roskind: The paper is well written and thoughtful. Supply chain management is critical to cyber and this offers ways to develop a model on known vulnerabilities which can be attributed and shared for risk management. Detecting unknown vulnerabilities is still the country's long pole.	Starks, George: "A telecommunication Supply Chain Model to Prevent Cyberspace Risks and Vulnerabilities" is a well-supported, well-structured and well-written white paper, which I believe lays a solid foundation that offers DHS the ability to better secure its telecommunication environment, and it was my pleasures to peer review it.	Tumbarello, Stephen: Your White Paper "A Telecommunications Supply Chain Model to Prevent Cyperspace Risks and Vulnerabilities" is Outstanding! I would easily give it an "A" grade!
Maxey, Serena: Keep up the great work. Your paper was pretty brilliant.	Woodhouse, Allen: It has a lot of promise and no doubt will have lots of senior level support as well.	Moore, Gerald: This is a very well written paper and I look forward to reading the final draft.

Closing Remarks

The Model provides:

- Service security
- Service availability
- Service Integrity
- Service interoperability
- Service privacy

Apply

Proactively supporting and participating in the DHS's Cybersecurity initiatives to the extend that it directly and indirectly impacts your organization's efforts by:

- Establishing a National Platform for NCTNs supply chain security
- Improving secure trade flow of the global transport information, hardware, software, firmware, and interfaces
- Facilitating the development, updating, and implementation of global transport supply chain security measures

Summary

The Model safeguards:

- Vital NCTNs systems 24x7x365 from cyber intrusions and espionage
- NCTNs components and infrastructures
- CDMA, PSTNs, GSMs, NGN, and other legacy circuit-switched and modern packet-based next generation transports systems

Q&A

Dr. Bahador Ghahramani, P.E., CISM, CPE

DHS National Protection & Programs Directorate (NPPD)

(o) 703.235.3056

(m) 202-253-7528

(f) 703.235.3060

http://www.dhs.gov/

bahador.ghahramani@hq.dhs.gov