



# Indo-US

## Workshop on

### Strengthening Supply Chain Security in the Pharmaceutical and Contract Chemical Synthesis Industries **2019**



July 15-16, 2019

CSIR-Indian Institute of Chemical Technology, Hyderabad



Gujarat Forensic  
Sciences University  
Knowledge | Wisdom | Excellence



Gujarat University  
Ahmedabad



In association with

Gujarat University, Ahmedabad  
CSIR-Indian Institute of Chemical Technology, Hyderabad

and

Pacific Northwest National Laboratory (PNNL), Richland, WA, USA  
U.S. Department of State's Chemical Security Program (CSP), Washington DC, USA

A B S T R A C T S





सत्यमेव जयते

डॉ. शेखर चि. मांडे

एफएनए, एफएएससी, एफएनएएससी

सचिव

भारत सरकार

वैज्ञानिक और औद्योगिक अनुसंधान विभाग

एवं महानिदेशक

**Dr. Shekhar C. Mande**

FNA, FASc, FNASc

Secretary

Government of India

Department of Scientific & Industrial Research

and Director General



वैज्ञानिक तथा औद्योगिक अनुसंधान परिषद

वैज्ञानिक और औद्योगिक अनुसंधान विभाग

(विज्ञान और प्रौद्योगिकी मंत्रालय)

अनुसंधान भवन, 2, रफी मार्ग, नई दिल्ली-110001

**COUNCIL OF SCIENTIFIC & INDUSTRIAL RESEARCH.**

Department of Scientific & Industrial Research

(Ministry of Science and Technology)

Anusandhan Bhawan, 2 Rafi Marg, New Delhi-110001



### Message

I am delighted to learn that CSIR-IICT, in its Platinum Jubilee Year, is conducting 4<sup>th</sup> Indo-US Workshop on "Chemical Security" on 15-16 July 2019 in association with Pacific Northwest National Laboratory (PNNL, US Department of Energy (DoE), USA and US Department of State Chemical Security Program (CSP), USA.

This workshop is indeed reflecting the relevance of the topic to the core objectives of the Government of India, with a special reference to the Chemical Sector, which plays a key role in the human and environmental health. With the ever increasing problems associated with the utilization of chemicals for destructive purposes, the supply chain management (SCM) becomes a central topic for all the stake holders, like vendors, manufacturers and buyers, besides the people those who manage them at different locations and specifically during transportation.

I am very glad to notice that, US organizers have long term plans to expand the horizon to conduct series of such joint workshops every year, not only in India, but in other Asian countries also, to highlight the problems associated with the use of Chemicals that have Dual-purpose and enlighten the community, to safeguard the global population.

I wish all the success for the Indo-US Workshop 2019.

New Delhi  
July 9, 2019

[ Shekhar C. Mande ]





PLATINUM JUBILEE



सी.एस.आई.आर - भारतीय रासायनिक प्रौद्योगिकी संस्थान  
CSIR - Indian Institute of Chemical Technology

(वैज्ञानिक तथा औद्योगिक अनुसंधान परिषद / Council of Scientific & Industrial Research)

CSIR - IICT (विज्ञान और प्रौद्योगिकी मंत्रालय, भारत सरकार / Ministry of Science & Technology, Govt. of India)

तारनाका Tarnaka, हैदराबाद Hyderabad - 500 007, T.S, भारत India

Tel : (O) +91-40-27193030, +91-40-27193234, Fax : +91-40-27160387

Email : director@iict.res.in / srivaric@iict.res.in | Website : www.iictindia.org



RIGHT TO INFORMATION

डॉ. एस. चंद्रशेखर, निदेशक

**Dr. S. Chandrasekhar**, FNASc, FASc, FNA  
Director

July 8, 2019

### Message

I am very glad to learn that the 4<sup>th</sup> Indo-US Workshop on “Chemical Security” is being organized in July 2019, both in Ahmedabad (Gujrat) and Hyderabad (Telangana). I feel honoured to be associated with this series of workshops since the 1<sup>st</sup> such event conducted by CSIR-Indian Institute of Chemical Technology in 2016, being sponsored by Pacific Northwest National Laboratory (PNNL), of US Department of Energy (DOE), USA and US Department of State Chemical Security Program (CSP), USA.

I am delighted to note that two day Indo-US Workshop 2019 on “**Strengthening Supply Chain Security in the Pharmaceutical and Contract Chemical Synthesis Industries**”, are being conducted by Gujarat University, Ahmedabad, Gujarat (India) on July 10-11, 2019 and CSIR-Indian Institute of Chemical Technology, Hyderabad (Telangana, India) on July 15-16, 2019 jointly by Pacific Northwest National Laboratory (PNNL), of US Department of Energy (DOE), USA and US Department of State Chemical Security Program (CSP), USA. As the Supply Chain Management occupies the central space for the manufacturing, with Make in India, Smart Cities and other new initiatives taken up by the Government of India, the two workshops on SCM acquire utmost importance with a special reference to the Chemical Industry, as it is the single that takes care of Human Well-being. With the globalization, ever-changing dynamics on the focus for the manufacturing in different regions of the Globe, development of effective and efficient strategies for SCM become nerve centre for any kind of manufacturing. The appropriately selected workshop syllabus to address the concerns of the stake holders, and faculty chosen both from India and USA, the experienced experts and the participants both from the academics and industry, would undoubtedly be able to impart requisite insights. I am sure, at the end of workshop, you all be going back new and relevant data. All my best wishes for a great success for the two noble endeavors at Ahmedabad and Hyderabad.

(S. Chandrasekhar)





## MESSAGE

For more than 50 years, the Pacific Northwest National Laboratory (PNNL) has advanced the frontiers of science and engineering in the service of humanity. We make fundamental scientific discoveries that illuminate the mysteries of our planet and the universe. We apply our scientific expertise to tackle some of the most challenging problems in energy, the environment, and security. We are honoured to represent the U.S. Department of State's Chemical Security Program in their efforts to enhance supply chain security and customer vetting in the pharmaceutical and specialty chemical sectors. In particular, our concern is the protection of dual-use chemicals; however, but the information provided in this workshop will also benefit other supply chain security objectives.

It is a privilege to combine forces in presenting this workshop with our distinguished partners from the Indian Institute of Chemical Technology, Gujarat University, Gujarat Forensics Science University, and other institutions and organizations. We look forward to continuing this engagement with our Indian and Bangladeshi colleagues -- to work together to improve chemical security around the world.

On behalf of Dr. Steven Ashby (Director of PNNL) and Jack Dishner (U.S. Department of State's Chemical Security Program), I warmly welcome you to this workshop.

**Clifford S. Glantz**

Chemical Security Project Director and Senior Staff Scientist  
Pacific Northwest National Laboratory





# **Indo-US Workshop on Strengthening Supply Chain Security in the Pharmaceutical and Contract Chemical Synthesis Industries**

**July 15-16, 2019**

**CSIR-Indian Institute of Chemical Technology [IICT]  
Hyderabad – 500 007**

## **Theme of the Workshop**

We are pleased to announce the presentation of Indo-US workshops at two locations (Ahmedabad – Gujarat and Hyderabad - Telangana, India) to strengthen chemical security awareness, to improve supply chain security, and enhance customer vetting in pharmaceutical and contract chemical synthesis industries.

Chemical security may be lax with poor security awareness; inadequate regulations; and little appreciation of how to identify, select, and implement risk-based, cost-effective security controls. Around the world, there is an immediate need for the decision makers (senior leaders, facility managers) and security personnel, emergency planning and response personnel to use appropriate tools to deter and mitigate potential security threats against facilities that manufacture, use, or store significant quantities of hazardous or weaponizable chemicals. Specifically, the pharmaceutical sector in the Asian region (e.g. India, Bangladesh, Indonesia, Malaysia etc.) faces substantial security risk from the theft or diversion of weaponizable chemicals and terror attacks. This risk is increasing as the region becomes a major world center for “end-to-end” drug discovery, manufacture, and distribution. The rapid growth in this industry has led to the proliferation of firms up and down the supply chain who routinely synthesize or distribute significant quantities of hazardous or weaponizable chemicals.

This workshop will build chemical security awareness and provide cost-effective techniques for implementing customer vetting and other supply chain security best practices for the pharmaceutical and contract chemical synthesis industries. In particular, the workshops propose to promote awareness and education in technical communities, support the adoption of customer-vetting programs in the chemical sector, and enhance security coordination and communication.

## Who Should Attend?

The target audience for the workshop includes personnel from pharmaceutical or speciality chemical firms and their suppliers and distributors. This includes firms that span a broad spectrum of sizes - from large firms to those firms who produces products with quantities in the range of 1 to 100 kg. In particular, the workshops invite attendees who are:

- Industry decision makers and facility managers
- Company safety and security personnel
- Facility emergency planners
- Managing the transportation or distribution of weaponizable chemicals
- Government security officials and law enforcement authorities
- Academicians who train people who are working in the pharmaceutical and specialty chemical sector or potential future sector employees.

## Workshop Syllabus

The tentative syllabus for the workshop covers the following topics:

- Raising security awareness throughout the product lifecycle.
- Identifying security weaknesses in the industry's supply chain management.
- Identifying high-value and cost-effective security controls that can improve security within the supply chain (e.g., security in product and process design, role and responsibility assignments, selection of suppliers and vendors, product procurement, workforce management and security training, inventory management, theft prevention, security monitoring, transportation, product disposal).
- Improving incident response and security event reporting.
- Characterizing potential terrorist capabilities to divert or steal pharmaceutical chemicals, intermediates, and/or end products.
- Understanding threats to public safety and security from a potential terrorist attack involving the use of weaponizable chemicals obtained from the pharmaceutical and contract chemical industry or from the associated supply chain.

Each workshop will be run as a residential event to encourage intense interactions amongst the participants.

---

# Indo-US

Workshops on

2019

Strengthening Supply Chain Security in the Pharmaceutical and Contract Chemical Synthesis Industries

## The Workshop Organizers

The U.S. partner at the workshop is Pacific Northwest National Laboratory (PNNL) and their work is sponsored by the U.S. Department of State's Chemical Security Program (CSP). The Indian workshop partners include the CSIR-Indian Institute of Chemical Technology, Gujarat University and GFSU, Gandhinagar, Gujarat. This workshop is a follow-up to the chemical security vulnerability assessment workshops conducted in Hyderabad, Chandigarh and Visakhapatnam in 2018 and Hyderabad in 2016; and the agrochemical security workshops conducted in 2017 in New Delhi, Ahmedabad, and Hyderabad.

## Patrons, Advisory and Organizing Committees

### Patrons

**Dr. Shekar Mande**, Director General, CSIR, New Delhi, India  
**Dr. S. Chandrasekhar**, Director, CSIR-IICT, Hyderabad, India  
**Dr. J. M. Vyas**, Director General, GFSU, Gandhinagar, India  
**Prof. H. A. Pandya**, Vice-Chancellor, Gujarat University, Ahmedabad, India  
**Mr. Jack Dishner**, Chemical Security Program, Department of State, Washington D.C., USA

### Advisory Committee

**Dr. Clifford S. Glantz**, PNNL, Richland, WA, USA  
**Dr. Radha Kishan Motkuri**, PNNL, Richland, WA, USA  
**Dr. P. Radhakrishna**, CSIR-IICT, Hyderabad, India  
**Dr. B. Jagadeesh**, CSIR-IICT, Hyderabad, India

### Organizing Committee

**Dr. V. K. Jain**, Gujarat University (Co-ordinator, Ahmedabad)  
**Prof. S. K. Mehta**, Panjab University, Chandigarh  
**Dr. K. Ravindranath**, Chief Scientist, CSIR-IICT (Co-ordinator, Hyderabad)  
**Dr. S. Prabhakar**, Principal Scientist, CSIR-IICT (Convenor, Hyderabad)  
**Dr. K. Srinivas**, Principal Scientist, CSIR-IICT, Hyderabad  
**Dr. B. V. Subba Reddy**, Chief Scientist, CSIR-IICT, Hyderabad  
**Dr. G. V. M. Sharma**, Chief Scientist (Rtd.), CSIR-IICT, Hyderabad  
**Dr. D. Krishna Rao**, CSIR-IICT (Office Secretary, Hyderabad)

For further information, please contact one of the following USA / India representatives:

### India

**Prof. V.K. Jain**

Gujarat University, Ahmedabad  
Tel: +91-79-26300969  
drvkjain@hotmail.com

**Dr. Manthan Panchal**

Gujarat University, Ahmedabad  
Tel: +91-9033238633  
Panchal\_manthan@gmail.com

**Prof. S.O. Junare**

GFSU, Gandhinagar  
Tel: +91-7923977144  
dir\_fs@gfsu.edu.in

**Dr. K. Ravindranath**

CSIR-IICT, Hyderabad  
Tel: +91 944 080 2808  
kajjam@iict.res.in

**Dr. S. Prabhakar**

CSIR-IICT, Hyderabad  
Tel: +91 944 107 0036  
prabhakar@iict.res.in

### USA

**Dr. K. Srinivas**

CSIR-IICT, Hyderabad  
Tel: +91 917 759 7871  
kantevari@gmail.com

**Dr. G.V.M. Sharma**

CSIR-IICT, Hyderabad  
Tel: +91-9440802785  
sharmagvm@gmail.com

**Dr. Clifford Glantz**

PNNL, Richland  
Tel: +1 509-375-2166  
cliff.glantz@pnnl.gov

**Dr. Radha Kishan Motkuri**

PNNL, Richland  
Tel: +1 509-371-6484  
radhakishan.motkuri@pnnl.gov

**Dr. John Cort**

PNNL, Richland  
Tel: +1 509-371-6334  
John.Cort@pnnl.gov

# Indo-US

## Workshops on

Strengthening Supply Chain Security in the Pharmaceutical and Contract Chemical Synthesis Industries

### Technical Program

**Day - 1**

**Program - July 15, 2019**

09h00 - 09h30: **Registration**

09h30 - 10h00: **Opening Ceremony**

- Welcome Remarks and Greetings
- Introduction of US and Indian Invitees
- Purpose and Goals of the Workshop
- Opening address
- Introduction of Instructors and Participants

10h00 - 10h30: **High Tea**

**Chairman: Dr. P. G. Rao (L1 and L2)**

#### Technical Session - 1

10h30 - 11h00:  
**30 min**

**L1**

**Dr. S. Prabhakar / Dr. K. Srinivas, CSIR-IICT, India**  
**Perspective on the Security of Dual-Use Chemicals**

#### Technical Session - 2

11h00 - 11h20:  
**20 min**

**L2**

**Dr. Clifford Glantz, PNNL, USA**  
**Examples of Security Risks in Supply Chain and Customer Vetting**

- Security risks associated with sabotage, loss of intellectual property, failure to vet customers
- Real Worlds Incidents: German steel mill, Ukraine Grid, Saudi petrochemical facility, and others

**Chairman: Dr. B. Gopalan (L3, L4 and L5)**

#### Technical Session - 3

11h20 - 11h45:  
**25 min**

**L3**

**Dr. Clifford Glantz, PNNL, USA**  
**Threats and Consequences**

- Insiders, criminals, terrorists, nation states, and other external threats
- Types of attacks physical, cyber, and blended
- Design basis threats and consequences (Confidentiality, Availability, and Integrity Impacts)
- Ways to enhance security: Predict, Prevent, Detect, and Respond to attacks

11h45 - 12h30:  
**45 min**

**L4**

**Dr. Radha Kishan Motkuri, PNNL, USA**  
**Exercise-A**

- Given the characteristics of an example chemical company and the capabilities of an identified adversary -- identify security problems.



#### Technical Session - 4

12h30 - 13.00:

**30 min**

**L5**

**Dr. John Cort, PNNL, USA**

#### **Supply Chain Security and Customer Vetting Background Information**

- What is Supply Chain Security and Supply Chain Management?
- Introduction to customer vetting
- The difference between defense and resilience

13h00 - 14h00:

#### **Lunch**

**Chairman: Prof. V. K. Jain (L6 and L7)**

14h00 - 14h45:

**45 min**

**L6**

**Dr. Radha Kishan Motkuri, PNNL, USA**

#### **Exercise -B**

- For the problematic facility in the previous exercise, identify potential security and resilience practices that can be adopted to better secure the supply chain

#### Technical Session - 5

14h45 - 15h15:

**30 min**

**L7**

**Dr. M. Surianarayanan, CSIR-CLRI, India**

#### **Security Vulnerabilities in the Indian Supply Chain**

- Vulnerabilities may exist throughout all the links in the supply chain and product lifecycle
- Review some of the key supply chain vulnerabilities, with an emphasis on those that may be of the most concern in India and neighboring countries.

15h15 - 15h30:

#### **High Tea**

**Chairman: Prof. S. K. Mehta (L8 and L9)**

15h30 - 16h15:

**45 min**

**L8**

**Dr. Radha Kishan Motkuri, PNNL, USA**

#### **Exercise -C**

- For the problematic facility in the previous exercises, discuss and identify potential vulnerabilities in the supply chain

#### Technical Session - 6

16h15 - 17h00:

**45 min**

**L9**

**Dr. John Cort, PNNL, USA**

#### **Security Engineering**

- Supply chains can be securely engineered to prevent abuse and crime.
- Approaches to reduce the risks of threats and vulnerabilities can be strategic, tactical, or both.
- Layered defences, Building security into equipment, Incident response, and event reporting.

## **Day - 2**

## **Program - July 16, 2019**

**Chairman: Mr. K. Ravindranath (L10 and L11)**

#### Technical Session - 7

09h15 - 10h00:

**45 min**

**L10**

**Dr. John Cort, PNNL, USA**

#### **Supply Chain Security and Customer Vetting Best Practices**

- Addressing People, Processes, and Equipment New technologies (e.g., RFID chips, digital monitoring, block chain)

10h00 - 10h45: <b>45 min</b>	<b>L11</b>	<b>Dr. Radha Kishan Motkuri</b> , PNNL, USA <b>Exercise-D</b> <ul style="list-style-type: none"> <li>● Discuss the pluses and minuses of various supply chain security and customer vetting best practices for the chemical sector.</li> </ul>
---------------------------------	------------	--

**10h45 - 11h00: High Tea**

**Chairman: Dr. G. V. M. Sharma (L12, L13 and L14)**

**Technical Session - 8**

11h00 - 11h45: <b>45 min</b>	<b>L12</b>	<b>Dr. C. Sudhakar</b> , CSIR-IICT / <b>Mr. V. V. Sasi Kumar</b> , Govt. of Telangana and <b>Dr. John Cort</b> , PNNL, USA <b>International and Regional Security Standards</b> <ul style="list-style-type: none"> <li>● Applicable standards in India and Bangladesh</li> <li>● ISO/PAS 28000:2007 -- Specification for security management systems for the supply chain</li> <li>● International standards (e.g., International Ship and Port Facility Security Code, Global Container Control Programme)</li> <li>● US Standards Chemical Facility Anti-Terrorism Standards (CFATS), Customs Trade Partnership against Terrorism (C-TPAT), Container Security Initiative (CSI).</li> </ul>
---------------------------------	------------	---

**Technical Session - 9**

11h45 - 12h15: <b>30 min</b>	<b>L13</b>	<b>Dr. Clifford Glantz</b> , PNNL, USA <b>Assessing Supply Chain Security</b> <ul style="list-style-type: none"> <li>● Security assessment models</li> <li>● Modeling the maturity of supply chain security programs.</li> </ul>
---------------------------------	------------	--

12h15 - 13h00: <b>45 min</b>	<b>L14</b>	<b>Dr. Radha Kishan Motkuri</b> , PNNL, USA <b>Exercise-E</b> <ul style="list-style-type: none"> <li>● Apply a simple maturity model to evaluate the supply chain security of a company</li> </ul>
---------------------------------	------------	--

**13h00 - 14h00: Lunch**

**Chairman: Dr. John Cort (L15 and L16)**

**Technical Session - 10**

14h00 - 14h30: <b>30 min</b>	<b>L15</b>	<b>Dr. Clifford Glantz</b> , PNNL, USA <b>Security Costs and Making Effective Security Decisions</b> <ul style="list-style-type: none"> <li>● Assessing supply chain security costs</li> <li>● Supply chain security must be cost-effective and can result in cost savings</li> <li>● Balancing risks and costs</li> <li>● Presenting results to decision makers</li> </ul>
---------------------------------	------------	---

14h30 - 15h20: <b>50 min</b>	<b>L16</b>	<b>Dr. Radha Kishan Motkuri</b> , PNNL, USA <b>Exercise-F</b> <ul style="list-style-type: none"> <li>● Make risk management decisions on supply chain security improvements given a set of identified vulnerabilities, potential security fixes and their costs, and a limited budget.</li> </ul>
---------------------------------	------------	---

**15h20 - 15h40: Closing Ceremony 20 min**

**Chairman: Dr. Clifford Glantz, PNNL, USA**

- Discussion on the two days deliberations
- Impressions of the participants
- Discussions on the Future Perspectives of Chemical Security

**ABSTRACTS /  
PRESENTATIONS**



## Biosketch of Dr. K. Srinivas

**Dr. Srinivas Kantevari**

**Principal Scientist & Associate Professor of AcSIR**

**Fluoro & Agrochemicals Division**

**CSIR-Indian Institute of Chemical Technology Hyderabad-500 007**

**E-mail: [ksrinivas@iict.res.in](mailto:ksrinivas@iict.res.in); [kantevari@gmail.com](mailto:kantevari@gmail.com)**



Dr. Srinivas Kantevari is affiliated to Fluoro & Agrochemicals Division, CSIR-Indian Institute of Chemical Technology. Dr. Srinivas Kantevari obtained his B.Sc. degree in chemistry (1989) from Andhra Loyola College, Vijayawada and Master degree in applied chemistry (1991) from National Institute of Technology (NIT) Warangal and Ph.D. organic Chemistry (1996) from Department of Chemistry, Indian Institute of Technology (IIT), New Delhi. He was research associate (1996-97) at National Institute of Immunology (NII) New Delhi. Later, he was a post-doctoral fellow (2001-2003) and research associate (2006-2008) with Prof. Graham Ellis-Davies, Department of Pharmacology and Physiology, Drexel University College of Medicine, Philadelphia, USA. He has been associated with CSIR-Indian Institute of Chemical Technology (IICT) since 1997 and presently he is Principal Scientist and Associate Professor of Academic of Scientific and Innovative Research, New Delhi. Dr. Kantevari is associated with several industries in process development of agrochemicals, APIs and their intermediates.

His core research interests are in organic chemistry, and able to successfully carry out extensive basic and applied research investigations in the chemistry of new molecules of biological relevance. He also developed several processes for APIs and drug molecules of interest and involved in transferring the technologies. Dr. Srinivas Kantevari has authored 98 peer-reviewed scientific papers in international journals of repute and >50 invited lectures at national and International conferences. He has five patents to his credit. He has supervised eight Ph.D. students and 28 M. Sc and M. Pharmacy students completed their project work. Currently six students are pursuing their Ph.D. five students are doing their project work. Dr. Srinivas Kantevari contributions have acclaimed recognition from honourable subject experts around the world. Dr. Srinivas Kantevari is actively associated with different societies and academies. Dr. Srinivas Kantevari academic career is decorated with several reputed awards and notable one is recipient of Indo-Australia biotechnology fund of DBT.

## Biosketch of Dr. S. Prabhakar

**Dr. S. Prabhakar**  
**Principal Scientist & Associate Professor of AcSIR**  
**Analytical Department**  
**CSIR-Indian Institute of Chemical Technology,**  
**Hyderabad-500 007**  
**E-mail: [prabhakar@iict.res.in](mailto:prabhakar@iict.res.in), [prabhakar.iict@gov.in](mailto:prabhakar.iict@gov.in)**



Dr. Sripadi Prabhakar obtained his B.Sc. degree in chemistry and biology (1989) and M.Sc. degree in organic chemistry (1992) from Osmania University, Hyderabad, India. He performed his doctoral work on the development of mass spectral techniques for stereochemical problems and received a Ph.D. degree in chemistry (1997). After completing his Ph.D., he joined as a Scientist at the National Centre for Mass Spectrometry, CSIR-Indian Institute of Chemical Technology, Hyderabad. He is continuing his research on the application of mass spectrometry in organic and biological chemistry including the special topic on analysis of chemical warfare agents and their degradation products in environmental samples. He achieved postdoctoral fellowship (2007–2009) at the Department of Chemistry, George Washington University, USA, and a postdoctoral fellowship (2001–2003) at Oxford Glycobiology Institute, University of Oxford, Oxford, UK. His research interests include detection and identification of chemical warfare agents and their degradation products in environmental samples, metabolite profiling of body fluids, shotgun metabolomics for clinical use, targeted metabolomics, study of isomeric compounds and gas-phase rearrangements, isolation and quantification of small molecules in biological fluids (pharmacokinetics). Right from inception, he has immense contributions to the Centre for Analysis of Chemical Toxins (CACT), CSIR-IICT, which is an ISO/IEC 17025 (NABL) accredited laboratory for the off-site analysis of chemicals related chemical weapons convention. The centre obtained OPCW designation status in 2008 and the team is regularly participating in official OPCW PTs to retain the designation status. He was awarded 'Eminent Mass Spectrometrist' award by ISMAS in 2013. He serves as a Life Member for the Indian society for mass spectrometry and the Indian Society for Analytical Scientists, and as a Fellow of the Telangana Academy of Sciences, Hyderabad. He is a member of editorial board for the Rapid Communications in Mass Spectrometry, Journal of Chemistry and Science Journal of Medicine. He has published 145 research papers in peer-reviewed international journals and supervised twelve Ph.D. students. He is a certified GLP inspector and technical assessor for NABL.

# Perspectives on the Security of Dual-Use Chemicals

**Dr. S. Prabhakar / Dr. K. Srinivas**

**CSIR-Indian Institute of Chemical Technology  
Hyderabad-500 007, Telangana State, INDIA  
prabhakar@iict.res.in, ksrinivas@iict.res.in**



## What chemicals are of most concern for diversion?

Common laboratory/industrial chemicals that would be targeted by someone for illegal reasons (chemical weapon/explosive/drug)

### Chemical Safety

To Prevent/protect against chemical laboratory accidents



### Chemical Security

To prevent/protect against the misuse of chemicals for non-peaceful purposes



Both ensure protection of:

Workers, Plant facility, Community, Environment, Economy

## Dual use chemicals?

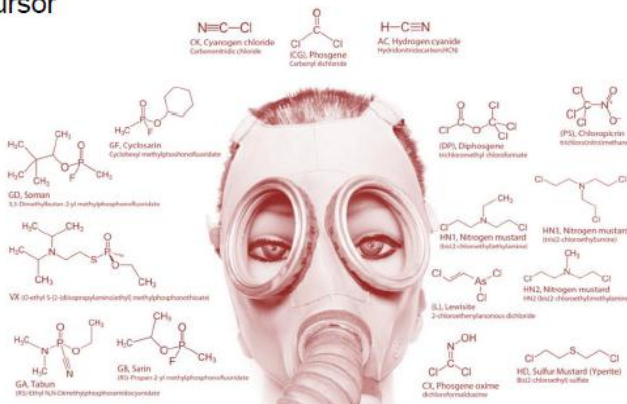
Chemicals used in industry or everyday life that can also be used in bad ways

Legal and Illegal use



How dual use chemicals can be used (bad ways)?

- Chemical weapon precursor
- Explosive precursor
- Drug precursor





## Many industrial chemicals have dual uses

- **Dimethyl methyl phosphonate (DMMP)**
  - Flame retardant for:
    - building materials, furnishings, transportation equipment, electrical industry, upholstery
  - Nerve agent precursor
- **Thiodiglycol**
  - Dye carrier, ink solvent, lubricant, cosmetics, anti-arthritis drugs, plastics, stabilizers, antioxidants, photographic, copying, antistatic agent, epoxides, coatings, metal plating
  - Mustard gas precursor
- **Arsenic Trichloride**
  - Catalyst in CFC manufacture, semiconductor precursor, intermediate for pharmaceuticals, insecticides
  - Lewisite precursor

## Dual-use chemical example Industrial chemical

### Sodium Azide ( $\text{NaN}_3$ )

- Used in agriculture (farming) for pest control
- Used in automobile airbags
- (Electrical charge convert to nitrogen gas inside the airbag)
- Chemical preservative in hospitals and labs. laboratories.
- Reacts explosively with metals
  - Biological laboratory drains have exploded from discarded waste solutions containing  $\text{NaN}_3$  as a preservative.
- When poured into a drain, release toxic gas (harm)  
Hydrazoic acid
- The most commonly reported health effect from azide exposure is hypotension (abnormal low blood pressure)
- Fatal doses occur with exposures of 700 mg (10 mg/kg).



## Dual-use chemical example Diversion of Industrial chemical 'Potassium Chlorate ( $KClO_3$ )'

- Herbicide
- Kill grasses and weeds non-agricultural sites
- '56' Active products containing sodium chlorate as an active ingredient



### Other agro chemicals:

Sodium chlorate  
Calcium chlorate  
Magnesium chlorate

### Bali bombing 2002

- One ton of potassium chlorate



A beautiful memorial for the victims of the tragic Bali bombings has been left to decay, leaning in one crystal clear pool stagnant green, as ornate stone carving covered in mud and one remaining figure barely held together with cracked wire.

### Van Bomb:

Potassium chlorate  
Aluminum powder

## Dual-use chemical example "Chlorine"

### Legal Use

Manufacturing of chlorinated compounds

- Organic chlorine compounds (PVC, ethylene chlorides)
- Inorganic chlorine compounds ( $HCl$ ,  $PCl_3$ )
- Disinfecting and bleaching products



### Illegal Use

Chlorine gas cylinders blown up (using explosives)

World War I as a chemical weapon

Syrian regime strikes targets in Hama with chlorine gas



aa.com.br/en/middle-east/syrian-regime-strikes-targets-in-hama-with-chlorine-gas/704204

## Dual-use chemical example Cyanide Ammonium nitrate

### Cyanide (Sodium cyanide)

#### Legal Use

Used in production of agrochemicals (herbicides and pesticides)

#### Illegal Use

Poison  
Precursor to HCN ( a CW agent)



How Dangerous Is the Sodium Cyanide at the Tianjin Explosion Site?



### Ammonium Nitrate (NH<sub>4</sub><sup>+</sup>NO<sub>3</sub><sup>-</sup>)

#### Legal Use

Used in Agriculture  
Industrial explosive

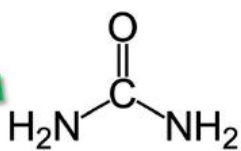
#### Illegal Use

ANFO (Ammonium nitrate/fuel oil) is a widely used bulk industrial explosive.  
Used Nastily



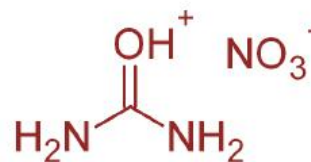
## Dual-use chemical example 'Urea'

### Fertilizer in Agriculture



Urea

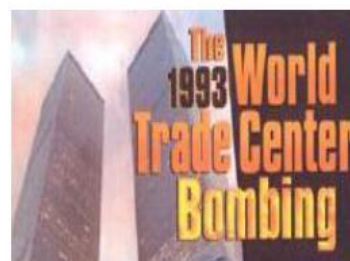
HNO<sub>3</sub>



Urea nitrate

2012 -13 to 2016 -17 (Thousand tons)

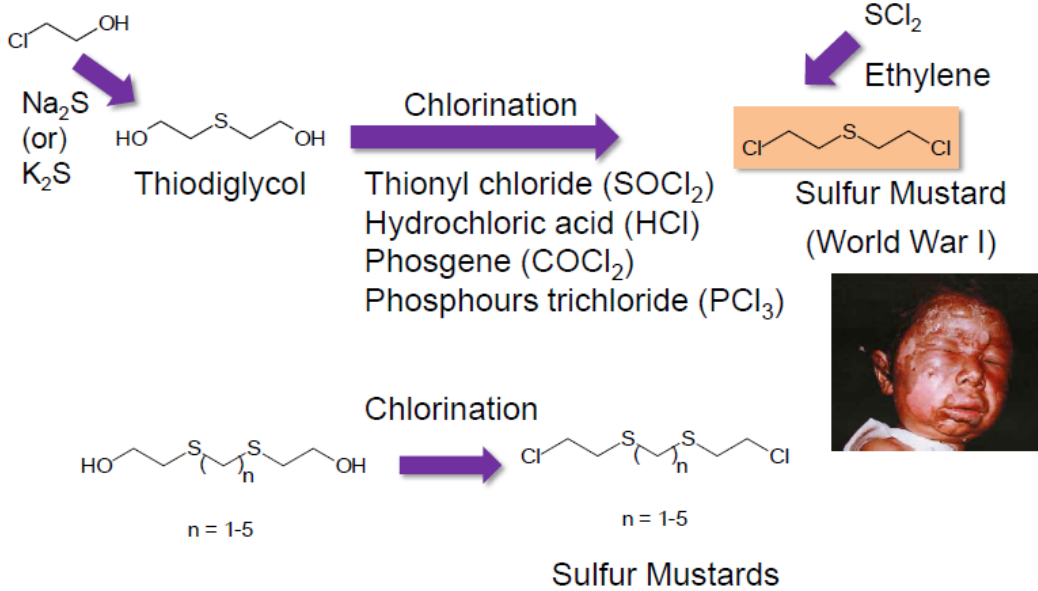
Year	Urea
2013-14	31192
2014-15	32029
2015-16	32858
2016-17	33677
2017-18	33754



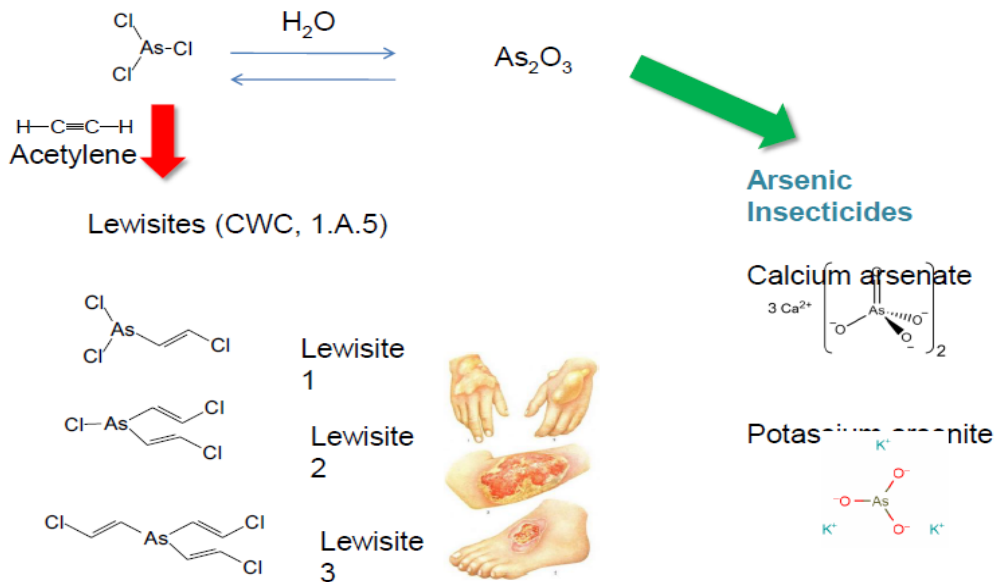
Fertilizers and their use in India



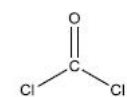
# Thiodiglycol and thionyl chloride



# Arsenic Trichloride



# Phosgene

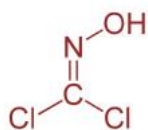


Phosgene



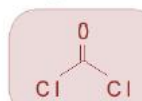
Warfare agent

World War 1

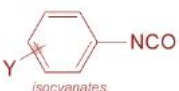


Phosgene Oxime  
(Blistering agent)

## Phosgene Chemistry

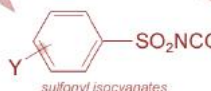


isocyanations

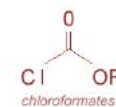


isocyanates

chlorinations



sulfonyl isocyanates



chloroformates



acid chlorides



imidyl chlorides

Dimethylcarbamate insecticides

E.g. Dimetan  
Pyramat

Oxime carbamate insecticides

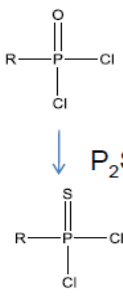
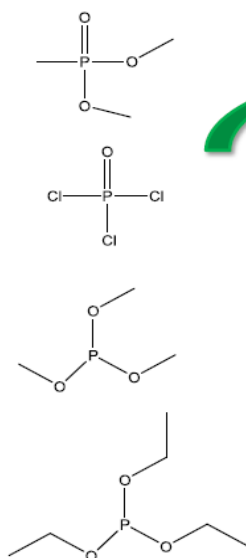
E.g. Alanycarb  
Butocarboxim

Phenyl methylcarbamate insecticide

E.g. Butacarb  
Dimethacarb



# Organo phosphorus pesticides



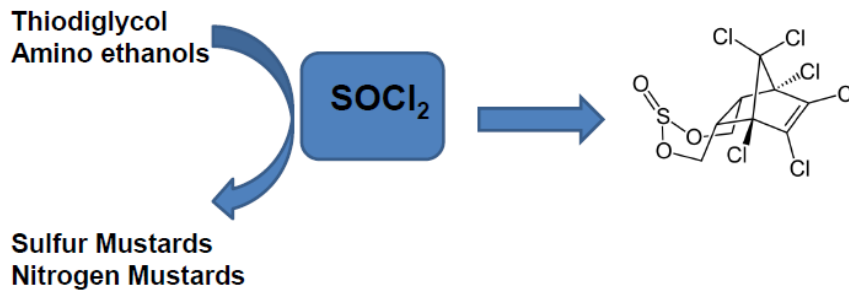
R-OH  
R-SH  
R-NH<sub>2</sub>

Pesticide

S

Warfare agents

# Thionyl Chloride



15

# Exposure Limits



[www.cdc.gov/niosh](http://www.cdc.gov/niosh)

National Institute for Occupational Safety and Health ((NIOSH)  
Recommended Exposure Limits (RELs)

[www.osha.gov](http://www.osha.gov)

Occupational Safety and Health Administration ((OSHA)  
Permissible Exposure Limits (PELs)

[www.ilo.org](http://www.ilo.org)

International Labour Organization  
Occupational exposure Limits (OELs)  
Maximum Exposure Limits (MELs)

[www.hse.gov.uk](http://www.hse.gov.uk)

Health and Safety Executive  
Control of substances Hazardous to Health (COSHH)  
Workplace Exposure Limits (WELs)  
Long term (LTEL)  
Short term (STEL)

16

## Definitions

### IC50

Indicates the **concentration in air necessary to incapacitate or disable 50%** of exposed and unprotected individuals through inhalation of the agent.

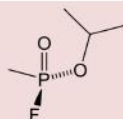
### LC50

Indicates the agent **concentration in air necessary to kill 50%** of exposed and unprotected individuals through inhalation of the agent.

### LD50

The amount of liquid or solid material **required to kill 50%** of exposed and unprotected individuals. The agent enters the body through skin absorption unless indicated as ingestion.

## SARIN



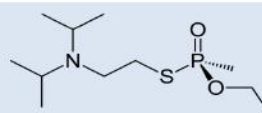
Attack in Matsumoto (1994) Tokyo subway (1995) in Japan - used Sarin gas – 19 people killed, a large number of injuries

Many times used in Syria



Ghouta chemical attack in Syria (2013) – Sarin gas used; thousands of people died.

## VX



Dugway Sheep Incident in USA (1968), nerve agent killed 6000 sheep

The Telegraph HOME | NEWS | SPORT  
 News  
 UK | World | Politics | Science | Education | Health | Brexit | Royals | Investigations

★ News  
 Malaysia decontaminating airport after revealing North Korean agents 'assassinated Kim Jong-nam with highly-toxic VX nerve agent'



# SULPHUR MUSTARDS



Mainly causes bone-marrow suppression, neurological and gastrointestinal toxicity in human body.

## Exposure Limits

- **Inhalation**
  - ✓ Up to 100 to 200 mg-min/m<sup>3</sup> causes airway injuries in the body.
- **Eye/Skin contact**
  - ✓ Median incapacitating dose in vapour form is **200mg-min/m<sup>3</sup>**.
  - ✓ When eyes are directly exposed to these vapours it produces eye lesions in the range of **12 to 70 mg-min/m<sup>3</sup>** of exposure.
  - ✓ In the form of liquids nearly **10 small droplets** are capable of producing blisters on skin.



**Lethal Limit**      100 to 200 mg-min/m<sup>3</sup> (vapour form)  
                             100mg/kg or 1 to 1.5 tsps (liquid)

19

# BLOOD AGENTS



e.g. HCN, CNCl

- Do not typically affect the blood
- Interrupt the production/function of blood components
- Prevent the normal utilization of oxygen by body tissues
- Interrupt the electron transport chain in the inner membranes of the mitochondria.
- Inhibit certain specific enzymes (Systemic agents)

20



## HYDROGEN CYANIDE



### Inhalation

- ❑ Poisoning occurs within seconds to minutes of direct exposure.
- ❑ Rapid olfactory fatigue occurs on intake of vapours, but its odour is detectable in the range of 2 to 10 ppm.

### Skin/Eye contact

- ❑ Systemic poisoning takes place within 30 to 60 min of its contact with the body

Permissible exposure limit: 10 ppm (15 min)

Acute exposure level: 2.5 ppm (10 min) and 1 ppm (nearly 8 hrs)

## ARSINE

Permissible Exposure Limit – 0.05ppm

Lethal or leads to death when exposure is beyond 3ppm

Acute exposure level- 0.3ppm(for 10 min ) and 0.02ppm (for 8hrs range)

21

## CHOCKING AGENTS



E.g.  $\text{Cl}_2$ , and phosgene, diphosgenes, nitric oxide and perfluoroisobutylene (PFIB)

- Injure the respiratory tract (nose, throat, lungs)
- In extreme cases, “choke”  
(the lungs filled with liquid and death due to lack of oxygen)
- Phosgene reacts with the  $-\text{SH}$ ,  $-\text{NH}$  and  $-\text{OH}$  groups of biological macromolecules
- PFIB is a byproduct from overheating of Teflon  
(10-times toxic than phosgene)

22

## CHLORINE

Permissible exposure limit: 1 ppm

Lethal limit: 10 ppm

- Acts as an irritant beyond 0.32 ppm
- Maximum bearable: up to 3 ppm (can take protective actions)

## CHLOROPICRIN

Recommended exposure limit : 0.7mg/m<sup>3</sup> or 0.1 ppm

- IDLH (Immediately dangerous to life and health): > 4ppm
- Intolerable pain is caused when ingested 7.5ppm for 10 minutes

## PHOSGENE

Permissible exposure limit: 0.1 ppm

- IDLH (Immediately dangerous to life and health): > 2ppm
- Maximum bearable: up to 0.2 ppm (can take protective actions)

## RIOT CONTROL AGENTS

(Irritants, lachrymators, harassing agents, tear gases)

E.g.

2-chloroacetophenone (**CN**),

2-chlorobenzilidenemalononitrile (**CS**)

Dibenz-1,4-oxazepine (**CR**)

- Cause temporary incapacitation by irritation of the eyes
- On exposure, they cause pain in the eyes, flow of tears and skin irritation.

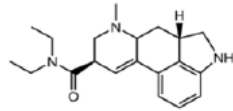
Three types

Lachrymators (tears, eye irritation)

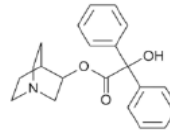
Sternutators (sneezing and respiratory tract irritation)

Vomiting agents

## PSYCHOMIMETIC AGENTS



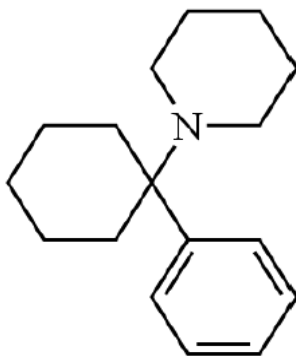
Lysergic acid diethylamide  
(LSD)



3-quinuclidynyl benzilate  
(BZ)

- Changes in thought, perception and mood
- No major disturbances in the autonomic nervous system
- Stimulates the sympathetic nervous system in the mid brain that affects the biochemistry of psychic functions
- Low doses (<10 mg) cause psychotic disorders (such as loss of feeling, paralysis, hallucinations, etc.)
- LSD :aerosol (ID<sub>50</sub>) 6 µg/kg
- BZ (25-times more potent than atropine); ID<sub>50</sub> for BZ is 6 µg/kg
- Less than 1 mg of BZ can produce acute brain syndrome

## Phencyclidine



- ✓ Widely used by drug addicts
- ✓ Analgesic and Anesthetic properties

@Doses of 5-20 mg

Symptoms

- Disturbed body-awareness
- Disorientation
- Vivid dreams

@Very high doses (>100 mg)

Respiratory depression and death.

## International Chemical Control Groups



### Chemical Weapons Convention

Organization for the Prohibition of  
Chemical Weapons (OPCW)



### The Australia Group

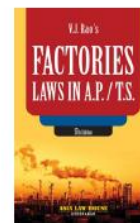
### Export Controls

### EU Regulations REACH



### UN Security Council Resolution 1540

### India Hazardous Substances Factories Laws in AP



27

## CWC ; Article II Definitions

### Chemical Weapons

- Toxic chemicals and their precursors
- Munitions and devices, specifically designed to cause death or other harm through the toxic properties of those toxic chemicals
- Any equipment specifically designed for use directly in connection with the employment of munitions and devices

### Toxic Chemical

- Any chemical which through its chemical action on life processes can cause death, temporary incapacitation or permanent harm to humans or animals. This includes all such chemicals, regardless of their origin or of their method of production, and regardless of whether they are produced in facilities, in munitions or elsewhere.

### Precursor

- Any chemical reactant which takes part at any stage in the production by whatever method of a toxic chemical.

28

## Toxic Industrial Chemicals

- Less deadly than CWAs
- Some of them listed in Schedule-2 (CWC)
- Not Fatal
- Cause serious health problems

High	Medium	Low
Ammonia	Acetone cyanohydrin	Allyl isothiocyanate
Arsine	Acrolein	Arsenic trichloride
Boron trichloride	Acrylonitrile	Bromine
Boron trifluoride	Allyl alcohol	Bromine chloride
Carbon disulfide	Allylamine	Bromine pentafluoride
Chlorine	Allyl chlorocarbonate	Bromine trifluoride
Diborane	Boron tribromide	Carbonyl fluoride
Ethylene oxide	Carbon monoxide	Chlorine pentafluoride
Fluorine	Carbonyl sulfide	Chlorine trifluoride
Formaldehyde	Chloroacetone	Chloroacetaldehyde
Hydrogen bromide	Chloroacetonitrile	Chloroacetyl chloride
Hydrogen chloride	Chlorosulfonic acid	Crotonaldehyde
Hydrogen cyanide	Diketene	Cyanogen chloride
Hydrogen fluoride	1,2-Dimethylhydrazine	Dimethyl sulfate
Hydrogen sulfide	Ethylene dibromide	Diphenylmethane-4,4'-diisocyanate
Nitric acid, fuming	Hydrogen selenide	Ethyl chloroformate
Phosgene	Methanesulfonyl chloride	Ethyl chlorothioformate
Phosphorus trichloride	Methyl bromide	Ethyl phosphonoethioic dichloride
Sulfur dioxide	Methyl chloroformate	Ethyl phosphonic dichloride
Sulfuric acid	Methyl chlorosilane	Ethylselenamine
Tungsten hexafluoride	Methyl hydrazine	Hexachlorocyclopentadiene
	Methyl isocyanate	Hydrogen iodide
	Methyl mercaptan	Iron pentacarbonyl
	Nitrogen dioxide	Isobutyl chloroformate
	Phosphine	Isopropyl chloroformate
	Phosphorus oxychloride	Isopropyl isocyanate
	Phosphorus pentafluoride	n-Butyl chloroformate
	Selenium hexafluoride	n-Butyl isocyanate
	Silicon tetrafluoride	Nitric oxide
	Stibine	n-Propyl chloroformate
	Sulfur trioxide	Parathion
	Sulfuryl chloride	Perchloromethyl mercaptan
	Sulfuryl fluoride	sec-Butyl chloroformate
	Tellurium hexafluoride	tert-Butyl isocyanate
	n-Octyl mercaptan	Tetraethyl lead
	Titanium tetrachloride	Tetraethyl pyrophosphate
	Trichloroacetyl chloride	Tetramethyl lead
	Trifluoroacetyl chloride	Toluene 2,4-diisocyanate
		Toluene 2,6-diisocyanate



## Biosketch of Dr. Clifford Glantz

### **CLIFFORD S. GLANTZ**

*Pacific Northwest National Laboratory  
902 Battelle Boulevard, P.O. Box 999, MSIN K6-81  
Richland, WA 99352  
Office: +1 509-375-2166; Fax: +1 509-371-7249  
Email: [cliff.glantz@pnnl.gov](mailto:cliff.glantz@pnnl.gov)*



**Clifford Glantz** is a Senior Staff Scientist and project manager with PNNL's National Security Directorate. Cliff's research focuses on consequence assessment modeling, emergency response and preparedness, critical infrastructure protection, risk management, and cyber-physical security. A key current interest is the role of supply chain security in maintaining an effective level of security for critical infrastructure. He is an author of the energy sector's widely-used cybersecurity guidance for procuring energy systems. He is the Co-Chair of the U.S. Department of Energy (DOE) Emergency Management Subcommittee on Technical Analysis and Response Support (STARS). Cliff Glantz's work is conducted for the U.S. DOE; Department of Homeland Security (DHS); Department of State; European Union Chemical, Biological, Nuclear, and Radiological (CBRN) Risk Mitigation Center of Excellence Initiative; International Atomic Energy Agency (IAEA); United Nations Interregional Crime and Justice Institute; and other agencies and organizations. Cliff has authored over 100 technical publications and papers and 150 conference presentations. He has won several awards for his research and project management during his 37-year tenure at PNNL.





## Session 2: Examples of Security Risks in Supply Chain and Customer Vetting

Cliff Glantz, John Cort, and Radha K Motkuri  
Pacific Northwest National Laboratory (PNNL)  
Richland, WA, 99352  
USA



PNNL is operated by Battelle for the U.S. Department of Energy

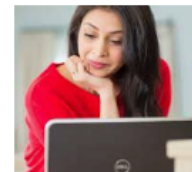


## Let's Consider a Few Hypothetical Cases

### Example 1 – Customer Vetting

- The sales office of your specialty chemical company receives an order from a new start-up company for a dual-use chemical.
- Your sales office checks out the company's website and calls the company to verify the order -- everything looks legitimate. Payment is received in advance and the product is prepared and shipped to the listed address.
- Alas, the new start-up company is a front for a terrorist organization. They are ordering the chemical to manufacture a weapon.

Sales Order		CUSTOMER NAME
Order #	0001	
Customer		
Address		
City		
State		
Zip		
Phone		
Fax		
Email		
Product		
Quantity		
Unit Price		
Total		



## Consider a Few of Hypothetical Cases (cont)

### Example 2 – Customer Vetting

- A regular customer submits an order to your chemical company for a dual-use chemical.
- Your sales office confirms the validity of the order.
- A terrorist organization mounts a successful cyber intrusion into your shipping system. They change the delivery address for the legitimate order of the dual-use chemical from the customer's facility to their warehouse.
- The product is shipped to the warehouse and delivered to the terrorists instead of the intended recipient.
- This mistake is not detected until a week later after the legitimate customer inquires as to the location of their order (that is now late in arriving). By then, the product is gone and the warehouse where it was delivered is abandoned.



3

## Consider a Few Hypothetical Cases (cont)

### Example 3 – Sabotage

- A criminal organization obtains a username and password to your industrial control network.
- They break into the network and map the functions of several chemical processes.
- They threaten sabotage that could cause an explosion if the company does not pay a ransom in bitcoin.



4



## Consider a Few Hypothetical Cases (cont)

### Example 4 – Sabotage

- A nation state engineers a backdoor into a control system product that their government-controlled company sells internationally.
- This product sells at a price that is lower than offered by other international suppliers.
- When in service, the control system can be accessed via required internet connection to provide information on its operations
- The product can be reprogrammed by the supplier to malfunction if their country and the host country are in conflict.



5

## Consider a Few Hypothetical Cases (cont)

### Example 5 – Loss of Intellectual Property

- A supplier has access to your inventory database.
- An employee of the supplier uses the supplier's access to search for information on your information network that they can sell.
- The might find useful information in the database they are permitted to access, or they can escalate their privileges and search for intellectual property on other computers in the network



6

## Consider a Few Hypothetical Cases (cont)

### Example 6 – Loss of Intellectual Property

- An employee used an insecure hotel Wi-Fi connection to access a company system.
- Access information is intercepted and stolen.
- Sometime later, the company finds its markets being flooded by cheap imitations of its own products. The stolen access credentials were used to hack into the company's systems and steal product design information.
- Counterfeiters make their own cut-rate versions of the products and offer them at substantial discounts, but with original manufacturer's logo.
- The legitimate manufacturers starts to hear of the problem when customers begin contacting the company with problems and complaints, believing the counterfeit products to be genuine articles.



7

## Eli Lilly Warehouse Theft (2010)

- In the U.S., an organized crime group repeatedly traveled to Eli Lilly warehouse to collect information about the warehouse and the Lilly employees.
- One group of the thieves used a ladder to climb onto the roof of a large Eli Lilly warehouse.
- They cut a hole through the roof and descended inside without activating arrays of motion detectors. Once inside, they deactivated the alarm system.
- Associates backed a large truck into the only loading bay not covered by cameras
- Used warehouse forklifts to pack their truck with thousands of boxes of products.
- Stole \$60 million in pharmaceuticals heist and committed similar million-dollar warehouse jobs in four other states .
- Caught and sentenced to prison.



8



## Target Attack (2013)



- Target loses sensitive customer payment data as a result of an exploit of a vendor
- The attackers backed their way into Target's corporate network by compromising a third-party vendor (Fazio Mechanical, a refrigeration contractor).
- A phishing email duped at least one Fazio employee, allowing malware to be installed on Fazio computers.
- With the malware in place, undetected by antivirus software, the attackers waited until the malware offered what they were looking for -- Fazio Mechanical's login credentials in **Target's**.
- Target learned that vendors accessing their systems must use appropriate anti-malware software. Mandated two-factor authentication to contractors who have internal access to sensitive information or systems.

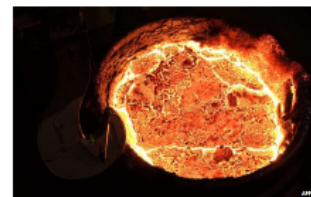
9



## Real World: German Steel Works (2014)

Cyberattack causes 'massive damage' at steel works

- **What:** Unscheduled shutdown of blast furnace
- **How:** phishing email
- **Who:** Unknown
- **What:** "Serious damage" wrecking a blast furnace
- **Consequences:** Business loss, potential for safety impacts on workers



Digital attack that resulted in physical damage



## Ukraine Power Grid Attack (2015, 2016, and 2017)

**Event:** Cyberattack and exploitation of SCADA system for Ukraine power grid.

**Threat:** Advanced and persistent threat

**Consequences:** Power outages at 3 regional electric power distribution companies impacting approximately 225,000.

**Specifics:**

- Initial infection through spear phishing emails with malicious Microsoft Office attachments.
- Coordinated attack (30 minutes attack window)
- Malicious remote operation of the breakers
- Call centers hit with denial of service attack
- Selected deletion of computer files on affected machines
- *BlackEnergy* malware identified on the machines



11



## The Las Vegas Fish Tank “Heist” (2016?)

- At a Las Vegas casino, a new casino fish tank featured remote monitoring, adjustment of temperature and salinity, and feeding control.
- That internet connectivity was exploited by hackers.
- Fish tank communications were used to get a foothold inside the casino’s business network.
- This directly led to the loss of 10 gigabytes of data from the casino – including the casino’s high-roller database.

**GENIUS HACKERS  
USED A VEGAS  
CASINO'S FISH TANK  
THERMOMETER TO  
STEAL HIGH ROLLERS'  
PERSONAL  
INFORMATION**



July 3, 2019

12





## Cyberattack on Saudi Arabia Petrochemical Plant

- “In August, a petrochemical company with a plant in Saudi Arabia was hit by a new kind of cyberassault. The attack was not designed to simply destroy data or shut down the plant, investigators believe. It was meant to sabotage the firm’s operations and trigger an explosion.”
- “The attack was a dangerous escalation in international hacking, as faceless enemies demonstrated both the drive and the ability to inflict serious physical damage.”
- “The only thing that prevented an explosion was a mistake in the attackers’ computer code, the investigators said.”
- “The attackers compromised Schneider’s Triconex controllers -- controllers used in about 18,000 plants around the world, including chemical plants.”

<https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html>



### The New York Times

*The cyberattack on a Saudi petrochemical plant was the first known attempt to manipulate an emergency-shutdown system, which is designed to avoid disaster and protect human lives.*

13





Thank you



14

Dr. Clifford Glantz



**Session 3:  
Threats and  
Consequences**

Cliff Glantz, John Cort, and Radha K Motkuri  
Pacific Northwest National Laboratory (PNNL)  
Richland, WA, 99352  
USA

U.S. DEPARTMENT OF  
**ENERGY** **BATTELLE**

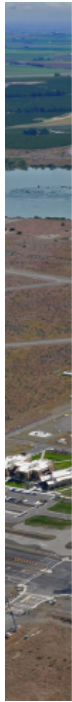
PNNL is operated by Battelle for the U.S. Department of Energy



**Potential Threat Agents/ Adversaries**

- External threat agents
  - Terrorists
  - Activists
  - Criminals
  - Nation states
  - Antisocial individuals
- Internal threat agents: “Insiders”
  - dissatisfied or mentally ill employees
  - former employees
  - external threat agents working within the organization





## The Objectives of Threat Agents

- Kill and injure people
- Damage the environment
- Economic disruptions or destruction of property
- Financial benefits (e.g., sell stolen goods, ransom, blackmail)
- Cause public unrest
- Revenge/embarrassment
- Affect the decisions of political leaders



3



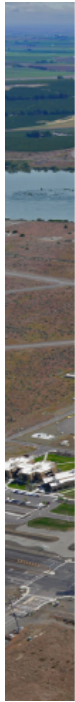
## Types of Adversaries: Insiders

- Insiders
  - May have detailed knowledge of facility operations, including critical systems.
  - May have physical or electronic access to plant information and control systems – including security systems and intellectual property.
  - May or may not have direct physical access to the facility.



4

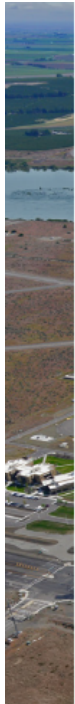




## Types of Adversaries: Insiders

Benign Intent	Malicious Intent
Disclose information to a friend or acquaintance	Disclose information to a known adversary
Inadvertently disclose access credentials	Use credentials to access unauthorized systems
Be the innocent victim of a cyber attack	Use known cyber attacks against the facility
Unintentionally fail to follow appropriate cyber security practices	Knowingly ignore cyber security policies and procedures

5



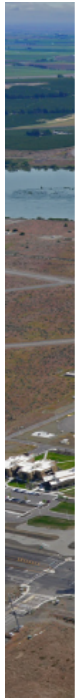
## Motivations for Malicious Behavior

- Disgruntled – Want to harm the company, management, co-workers because of past slights or other events
- Profit – hired to work for attackers
- Political/Cultural – want to make a political statement or advance the agenda of a certain group
- Mental illness – suffering from delusions, chemical or alcohol addiction, depression, etc.



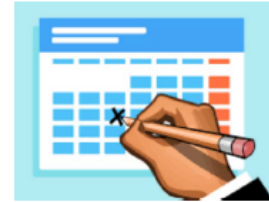
6





## Malicious Intentions – Bad Outcomes

- Possess system knowledge that can be used to their advantage
- Permitted to access sensitive parts of the facility and critical systems
- Can choose the best time to commit a malicious act. Can have adverse consequences occur long after the insider leaves the facility.
- Can take actions to reduce the likelihood that their malicious actions will be traced back to the perpetrator.



7



## Types of Adversaries: Hackers/Crackers

- Intentions range from relatively benign to malicious/destructive
- Motivations – Varied: the thrill of the attack, testing their capabilities, gaining bragging rights, profit.
- Numbers – may work alone or in groups
- Resources are limited by the intensity of their motivation and financial constraints.



8



## Types of Adversaries: Hackers/Crackers (Cont'd)

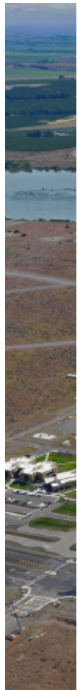
- Capabilities:
  - Their skill level may range from relatively low to highly sophisticated.
  - At the low level: “Script kiddies” may rely exclusively on off-the-shelf (including commercial) hacking technologies
  - At the high level: May develop their own sophisticated cyber attack methodologies and tools and use a suite of sophisticated tools to break down defenses one-by-one



## Types of Adversaries: Criminal Organization

- **Intentions:** Exploitation for profit
- **Motivation:** Money. Prestige may also be important to some. Actions moderated by concern over being caught and convicted!
- **Numbers:** Small to large groups
- **Resources:** Limited only by profit potential

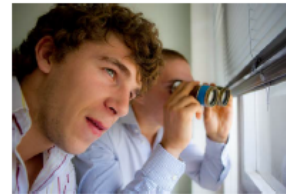




## Criminal Organization (cont)

### • Capabilities:

- May have the ability to acquire extensive technical knowledge and capabilities through research, coercion, and acquisitions.
- May attempt to utilize insiders to acquire target specific information.
- May seek to team with other adversaries to enhance capabilities



11

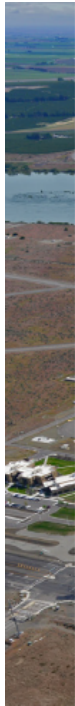


## Types of Adversaries: Terrorists

- **Intentions:** Cause damage, advance their political social, or cultural objectives.
- **Motivation:** Publicity, change public perception, make money to support their activities. May not care if they are caught. More likelihood to combine a physical and cyber attack.
- **Numbers:** Individuals to large groups
- **Resources:** Limited to extensive



12



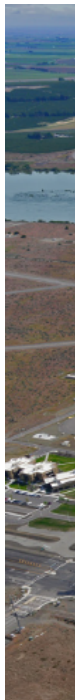
## Types of Adversaries: Terrorists (cont)

### • Capabilities:

- Like organized crime, may have the ability to acquire extensive technical knowledge and capabilities through research, coercion, and acquisitions.
- Groups may attempt to utilize insiders to acquire target specific information.
- May team with other categories of threat agents to enhance capabilities (“the enemy of my enemy is my friend.”)



13



## Types of Adversaries: Nation States

- Intentions: Ranges from information gathering to the intentional destruction/disabling of critical infrastructure.
- Motivation: Political influence, defense, preparation for potential future conflicts (military or non-military). May need to act with stealth.
- Numbers: Typically, extensive, well-organized, highly trained groups



14



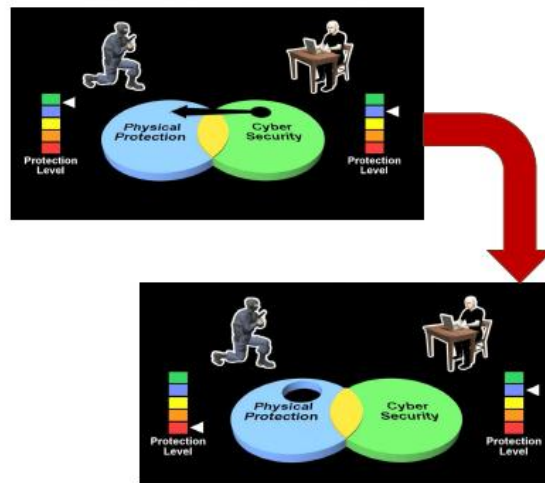
## Types of Adversaries: Nation States (cont)

- Resources: Can be enormous.
- May involve large groups spending many years to identify and plan potential attacks. May be permitted to practice on test ranges or on a small scale in the real world.
- Capabilities: May have the ability to acquire extensive technical knowledge and capabilities through research, coercion, and acquisitions. May use insiders.

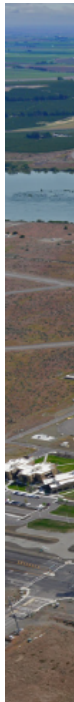


## Types of Attacks

- Physical attack
- Cyber attack
- Physically-enable cyber-attack (blended)
- Cyber-enabled physical attack (blended)







## Design Basis Threat

- No organization and facility can protect itself from all threats.
- To understand what types of threats the organization needs to design its security program to stop, it is helpful to determine an applicable Design Basis Threat (DBT).
- A Design Basis Threat (DBT) is:
 

*a description of the attributes and characteristics of potential insider and/or external adversaries, who might attempt sabotage, theft or diversion of materials, and the theft or alteration of information.*



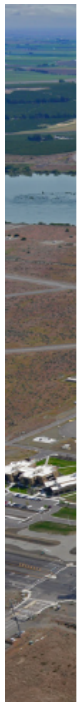
Design Basis Threat Example			
CAPABILITIES	LOW Threat	MEDIUM Threat	HIGH Threat
Type of threat	Criminal / disgruntled employee	violent extremists	Terrorists
Goal	Theft / property damage	multiple facilities / regional	Mass disruption with maximum media exposure / wide spread panic
Motivation	Monetary / revenge	Revenge / ideology	ideology / willing to die in order to complete the act
Strategy	Overt	Covert / police diversion / avoids violence of persons unless pressured	Covert / diversion / armed attacks / explosive suicide if pressured
Knowledge	limited local knowledge	Extensive regional / systems knowledge	Extensive targeting surveillance / Explosive breaching
Skills	Limited	surveillance advance planning	Highly trained in military special operational tactics and planning
Numbers of people and level of violence	up to 2 non-violent	up to 4	up to 5
Tools	hand tools	power tools	advanced power tools
Explosives	none	flammable liquids	up to 10 Kg each person
Advance Technical capabilities	none	simple hacking	advanced cyber penetration and manipulation / use of drones
Insider Assistance	1 passive	up to 1 active non-violent	up to 1 active violent
Weapons	knives	handguns	assault rifles and handgun with 100 cartridges each



## Types of Consequences

Consequences Fall into Three Categories:

1. Loss of Confidentiality
  - Theft of data, plans and other information
2. Loss of Integrity
  - System is operational but you cannot trust the data
3. Loss of Availability
  - Denial of service attack
  - System becomes inoperative or ineffective



## Loss of Confidentiality

- Loss of sensitive facility information. Examples include:
  - Loss of staff personnel records
  - Loss of access control information such as the physical access control database or computer system usernames and passwords.
  - Scheduling information for the offsite transportation of radiological or nuclear materials
  - Nuclear materials inventory information



## Loss of Availability

- Loss of ability to access or systems. Examples include:
  - Failure of digital security systems requiring the facility to rely on manual systems.
  - Reduced ability to monitor or control some plant functions using digital systems.
  - Reduction or elimination of electronic communications within the facility or with the outside world.
  - Taking over operational control of plant systems. Adversaries could take control and shut out legitimate operators.

21



## Loss of Integrity

- Loss of control over digital processes – including critical control systems. Examples include:
  - Manipulate data in plant security systems. This can include shutting off alarms, feeding security cameras false images, changing physical access authorizations, or data tampering.
  - Feeding false data to plant systems and system operators.

22





## Risk

- Risk – Consequences x probability of occurrence
- Probability can involve a number of factors:
  - Probability an attack will occur
  - Probability of it succeeding
  - Probability of worst-case consequences occurring (failure of safety systems, resiliency, etc.)



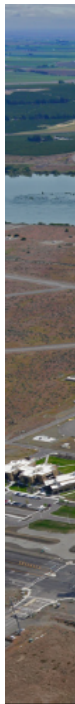
## Enhancing Security

- Steps to take to enhance security.

- **Predict**
- **Prevent**
- **Detect**
- **Respond**

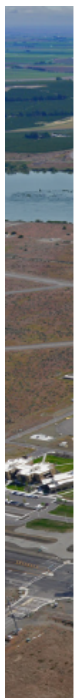


- These themes will be repeated throughout this workshop.



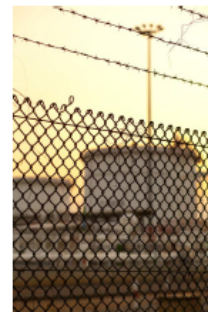
## Predict

- Understand the threat environment
- Understand potential security vulnerabilities
- Understand the consequences of potential security incidents.



## Prevent

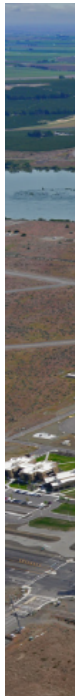
- Address security throughout the product lifecycle
- Implement cost-effective security controls to deter attackers (do not be seen as an easy target)
- Address and thwart attacks up to and including the design basis threat





## Detect

- Be vigilant
- Identify attacks in time to take supplementary protective actions
- Prevention without detection is of limited effectiveness
- Analogy – the castle without a watchman



## Respond

- Know how to respond before a security event occurs and train people on what to do.
- Report to law enforcement if there are
  - suspicious activities, vehicles, persons
  - threats made against people or property
  - Suspected sabotage of facilities or equipment
  - missing products.



**Biosketch of Dr. Radha Kishan Motkuri**

**RADHA KISHAN MOTKURI**

*Pacific Northwest National Laboratory  
902 Battelle Boulevard, P.O. Box 999, MSIN K6-81  
Richland, WA 99352  
Office: +1 509-371-6484; Fax: +1 509-371-7249  
Email: [radhakishan.motkuri@pnnl.gov](mailto:radhakishan.motkuri@pnnl.gov)*



**Radha Kishan Motkuri** is a senior research scientist and principle investigator with the PNNL Energy Processes and Materials Division. He has over 20 years of experience in the field of inorganic and material chemistry with an emphasis on nanoporous materials such as zeolites, metal-organic frameworks (MOFs), covalent organic frameworks, mesoporous silica, and hierarchical porous carbons (HPCs) for potential applications including sorption, separation, catalysis, detection and sensing. Radha Kishan's research supports the U.S. DOE's Office of Energy Efficiency and Renewable Energy, Advanced Research Projects Agency-Energy (ARPA-E), Energy Frontier Research Centers (EFRC), the U.S. Department of State Chemical Security Program (CSP), and other programs. Recent research successes include a series of cooling technology development projects and winning a prestigious R&D 100 Award (2017) for thermal vapor-compression cooling technology. Radha Kishan has published more than 75 peer-reviewed publications (including 11 journal cover articles) and has 14 international patents, including seven USA patents/patent applications. He organized several meeting sessions for the American Chemical Society. He performed his doctoral work at the Indian Institute of Chemical Technology (IICT) (awarded from University of Hyderabad) and has undergraduate and graduate degrees from Osmania University. He is on the editorial board for the journals *Inorganic Chemistry* (ACS), *Inorganic Chimica Acta* (Elsevier), and *Scientific Reports* (Nature).



## Exercise A – Plant Alpha -- Security Threats along the Supply Chain

Radha Kishan Motkuri, Cliff Glantz, and John Cort  
Pacific Northwest National Laboratory (PNNL)  
Richland, WA, 99352  
USA



PNNL is operated by Battelle for the U.S. Department of Energy



## Welcome to Plant Alpha

### Plant Alpha

Pharmaceutical and Specialty  
Chemical manufacturing facility  
and laboratory

*Serving Ruritania and our community with  
distinction since 1923*







## Welcome to Plant Alpha: Mission

Plant Alpha produces:

- pharmaceuticals
- Intermediate/precursor chemicals
- special order chemical
- agricultural chemicals



## Welcome to Plant Alpha: Background Information

- Located In the country of “Ruritania”
- Plant founded in 1923. 10 years ago it launched it’s “21<sup>st</sup> Century” initiative.
- Motto: *“Putting Technology to Work to Benefit the People of Ruritania”*.
- Employs 270 people.







## Welcome to Plant Alpha: Supply Chain

- Plant Alpha manufactures and stores an array of pharmaceutical and chemical products.
- Plant Alpha manufactures specialty/fine/custom/intermediate chemicals for its industry customers. This includes dual-use, hazardous chemicals.
- Bulk materials, including hazardous chemicals, are shipped to Plant Alpha for processing.



## Welcome to Plant Alpha: Supply Chain (cont)

- Pharmaceuticals and specialty chemicals (including dual-use chemicals), are shipped to customers for further processing and packaging.
- Procurement of products, hiring, sales of finished products, billing and accounts receivable, inventory management, shipping, and other business functions are performed in the company office.





## What are the Security Threats Facing Plant Alpha?

What are the attacks that external and internal threat agents might carry out during the five listed steps in the following simplified supply chain?

- External threat agents
  - Terrorists
  - Activists
  - Criminals
  - Nation states
- Internal threat agents
  - disaffected employees
  - former employees

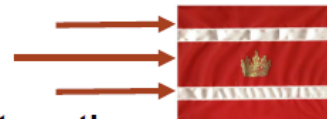


### Supply Chain Steps

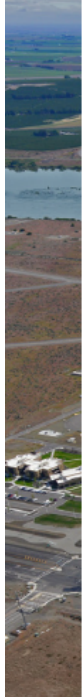
1. Supply of raw materials for processing at Plant Alpha
2. Manufacture/processing of chemicals at Plant Alpha
3. Storage of chemicals at Plant Alpha
4. Transport of chemical products to customers
5. Delivery of chemicals to customers



## Example Scenarios



- **A nation state mounts a cyberattack to sabotage the plant during the manufacturing process, potentially releasing hazardous materials into the environment.** The attackers objectives are to negatively impact public health and morale, lower confidence in the government of Ruritania, distract people's attention from other actions by the attacking nation state.
  - The attackers recruit an experienced hacker
  - They acquire control system malware from the dark web
  - They send spear phishing emails to company executives
  - They wait for malware to be transferred to a Plant Alpha control system.
  - The malware "calls home" to let the attackers know it is installed.
  - The attackers activate the malware whenever they want to take over operation of the control system.



## Example Scenarios (cont)

- **Criminals hijack chemicals during transport from Plant Alpha to a customer.**
  - They acquire information from a Plant Alpha insider (through a bribe or a threat) about shipments of specialty chemicals to customers.
  - They follow a selected shipment when it leaves the plant
  - They hijack the truck when the driver stops for lunch.
  - They sell the hijacked chemicals on the black market.



9



## Instructions

- Come up with other attack scenarios that take place at various steps in Plant Alpha's supply chain.
- Choose a representative to present this to the class.
- Try and identify a broad range of potential supply chain attack scenarios.
- You will use these scenarios later – so be creative and realistic



10

## Scenarios for Sabotage, Theft or Diversion of Materials, and Theft of Intellectual Property

- External threat agents
    - Terrorists
    - Activists
    - Criminals
    - Nation states
  - Internal threat agents
    - disaffected employees
    - former employees
- 
1. Supply of raw materials for processing at Plant Alpha
  2. Manufacturing of chemicals at Plant Alpha
  3. Storage of manufacturing chemicals at Plant Alpha
  4. Transport of manufactured chemicals to customers
  5. Delivery of chemicals to customers

11

## Present Results



12





Thank you



## Biosketch of John R. Cort

### **JOHN R. CORT**

*Pacific Northwest National Laboratory*  
902 Battelle Boulevard, P.O. Box 999, MSIN K6-81  
Richland, WA 99352  
Office: +1 509-371-6334; Fax: +1 509-371-7249  
Email: [John.Cort@pnnl.gov](mailto:John.Cort@pnnl.gov)



**John R. Cort** is a senior research scientist in the Biological Sciences Division at PNNL. John's research involves application of NMR spectroscopy and mass spectrometry to a broad range of problems requiring structural and functional characterization of organic and biological molecules. Since 2010 he has developed a program relevant to chemical security where NMR and other methods are used for chemical forensics and source attribution of chemical threat agents. This approach has since been adapted for a project developing mathematical methods to characterize biological similarity in distinct lots or batches of macromolecular pharmaceutical substances such as glycosaminoglycans and monoclonal antibodies that are produced by different manufacturers, an issue of critical importance for insuring generic drug safety and efficacy prior to approval. John has coauthored more than 80 peer-reviewed publications and has deposited more than 100 structure entries in the Protein Data Bank. He has presented his work at national and international scientific meetings and has organized symposia on chemical forensics for national meetings of the American Chemical Society and on NMR in national security applications for the Practical Applications of NMR in Industry conference. He is also a member of the Chemical Forensics International Technical Working Group. John is a research associate professor (joint appointment) in the Institute of Biological Chemistry at Washington State University and has taught general and organic chemistry at the WSU branch campus in Richland. He obtained a Ph.D. in organic chemistry from the University of Washington in 1997 and a B.A. in chemistry from Williams College in 1991.





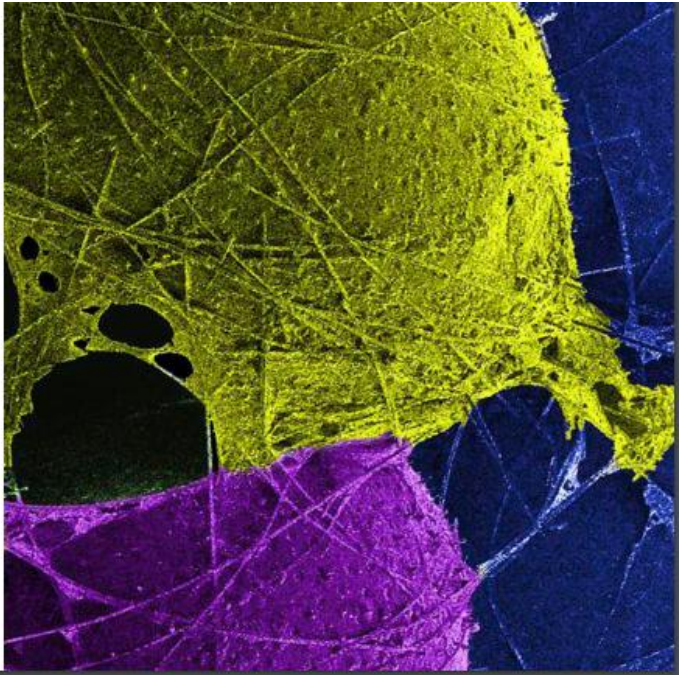
## 4: Supply Chain Security and Customer Vetting: Background

John Cort  
Clifford Glantz  
Radha Motkuri

Pacific Northwest National Laboratory

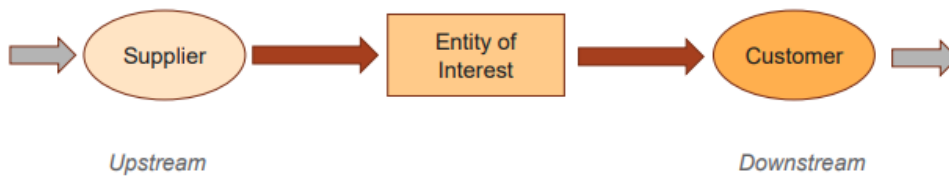
U.S. DEPARTMENT OF ENERGY **BATTELLE**

PNL is supported by Battelle for the U.S. Department of Energy.



## Supply Chain Security and Customer Vetting: Background

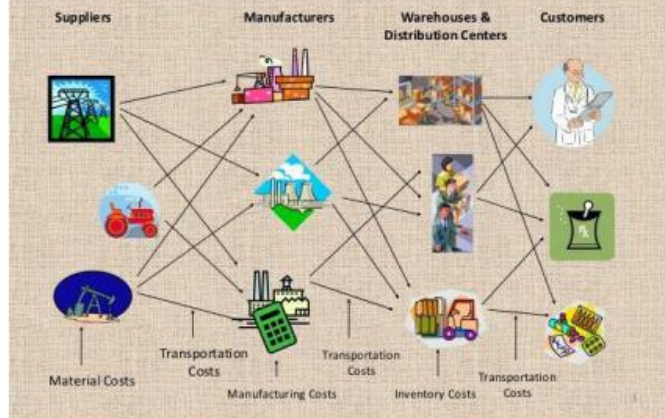
A simplified supply chain



## Supply Chain Security and Customer Vetting: Background

In reality, the supply chain is a dynamic complex network of relationships

### Supply Chain complexity:



3

## Supply Chain Security and Customer Vetting: Background

### • Outline

- What is supply chain security? contrast with supply chain management.
- What are security requirements?
- What is the difference between defense and resilience
- What is customer vetting?
  - Know the customer

4



## Motivations

- Motivations—(Cliff covered in session 2)

6



## Supply Chain Security and Customer Vetting: Background

- What is supply chain security?
  - **Definition:** Supply chain **security** in this context is the maintenance of control over chemicals and materials transiting to or from a specific industry entity, in order to prevent diversion or misuse
  - Supply chain security IS NOT the assurance of consistency in the supply chain so that processes and schedules are not disrupted by shortages or delays—this is supply chain **management**.
  - Part of supply chain management is addressing risks—among which are security risks. Thus, supply chain security and supply chain management are related.

6



## Supply Chain Security and Customer Vetting: Background

- Why might an individual or group disrupt the supply chain or divert chemicals?
  - Supply chain disruption:
    - Economic sabotage
    - Criminal mischief
    - Unintentional / accident / incompetence
    - **To obtain specific chemicals of interest**

7



## Supply Chain Security and Customer Vetting: Background

- Why would someone want to disrupt the supply chain or divert chemicals?
  - Diversion of chemicals
    - Theft—chemicals have value, and can be resold on the market; many are commodities and are not *easily* traceable.
    - For illicit activity—purchasing some chemicals in legitimate markets may be difficult or impossible for some parties, or may draw unwanted attention
  - ✓ **Types of illicit activity**
    - Terrorism by non-state actors
    - State-Sponsored Chem/Bio
    - Illicit manufacturing, e.g. drugs
    - Smuggling materials to other parties for their illicit activities
    - Purchase on open or lightly-regulated markets

8





## Supply Chain Security and Customer Vetting: Background

- Diversion of chemicals, cont.
  - Traceability of chemicals: even pure chemicals can be traced; chemicals can be the same but not the same
    - **Chemical Forensics**: source attribution and sample matching to identify how, where, when, or by whom a chemical was synthesized, isolated, and purified from specific starting materials.
  - Chemical forensics relies on stable isotope ratios, impurity profiles, stereoisomer distributions, and other intrinsic and extrinsic *attribution signatures*

9

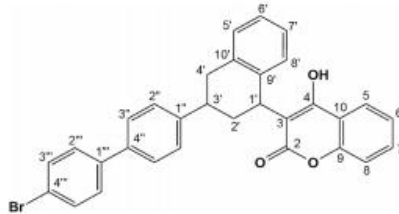
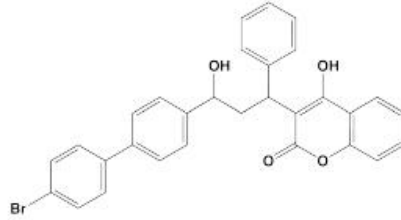


## Supply Chain Security and Customer Vetting: Background

- Diversion of chemicals, cont.
  - Case study: brodifacoum
    - Dual use: pesticide and poison

10

## Case Study: Brodifacoum



"superwarfarins"

(anticoagulant vitamin K epoxide reductase inhibitors)

Tiny quantity present in baits: 0.005%



Unit of Measure : **Kilograms/Kilograms**  
Minimum Order Quantity : **1**

[Get Latest Price](#)

### Rodenticide Brodifacoum 97%TC

We have made our mark as a reliable Exporter, Manufacturer and Supplier of Rodenticide Brodifacoum 97%TC in Shanghai, Shanghai, China. It belongs to the second-generation anticoagulant which has a good palatability and is popular with all over the world. Usually, it will be safe for the human and non....

[View More](#)

**SHANGHAI ZZ NEW MATERIAL TECH. CO., LTD.**

📍 Shanghai , China ...[More](#)

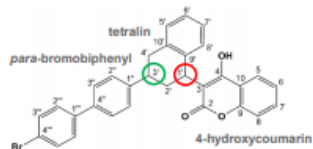
[View Contact Details](#)

[Send Inquiry](#)



## Supply Chain Security and Customer Vetting: Background

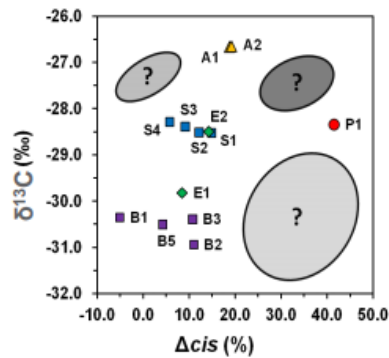
- Diversion of chemicals, cont.
  - Traceability of chemicals and chemical forensics, brodifacoum example



### Key to sources

- ▲ A: Germany
- B: US
- S: UK
- P: Asia
- ◆ E: US EPA, attr. to B (US) & S (UK)  
(numbers are different batches)

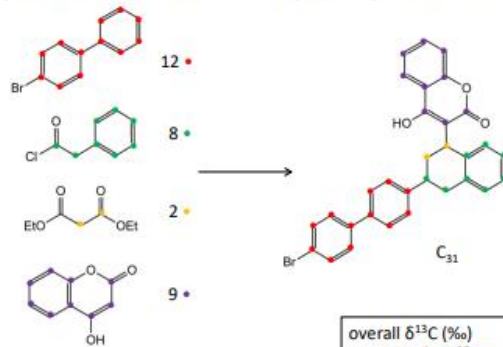
? = other plausible parameter space



13

## Supply Chain Security and Customer Vetting: Background

- Diversion of chemicals, cont.
  - Traceability of chemicals and chemical forensics, brodifacoum example
  - Specific atoms come from specific precursors



$$\text{overall } \delta^{13}\text{C} (\text{‰}) = 12/31\Delta^{13}\text{C} + 8/31\Delta^{13}\text{C} + 2/31\Delta^{13}\text{C} + 9/31\Delta^{13}\text{C}$$

14

## Supply Chain Security and Customer Vetting: Background

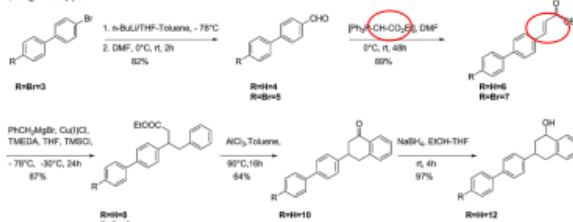
- Diversion of chemicals, cont.

- Traceability of chemicals and chemical forensics, brodifacoum example

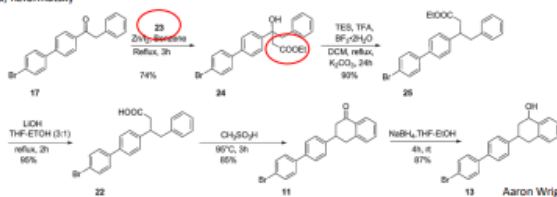
- Specific atoms come from specific precursors

- Supply chain and process chemistry are interrelated.

Scheme 1, Organocopper



Scheme 3, Reformatsky



Aaron Wright, Kajal Nandy, PNNL

15

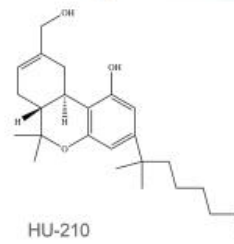
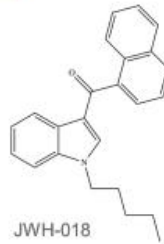
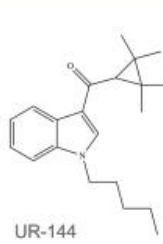
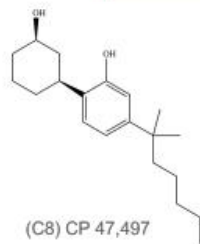
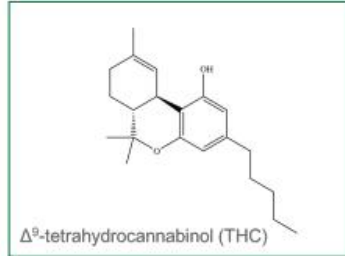
## Supply Chain Security and Customer Vetting: Background

- Diversion of chemicals, cont.

- Case study: synthetic cannabinoids
  - No legitimate use

16

## Case Study: Synthetic Cannabinoids



MANDELSTEIN | TORBERT

## 2 Chicago-area companies sold narcotics online and shipped from local warehouses, prosecutors say

By RICK KAMBIC | PIONEER PRESS | MAY 31, 2018 | 5:28 PM



Federal prosecutors say Liangfu "Larry" Huang, 53, of Northbrook, ran a business known as **Ark Pharm Inc.**, which operated from a warehouse at 1840 Industrial Drive, Libertyville, until recently moving to 3860 N. Ventura Drive, Arlington Heights, according to the federal complaint.

Huang was taken into custody Wednesday night at O'Hare International Airport after exiting a plane that arrived from China, according to the release. He was charged with one count of conspiracy to knowingly and intentionally possess with intent to distribute, and to distribute, a controlled substance. Prosecutors say he used the company to sell controlled substances, including a fentanyl precursor.

A multi-jurisdictional task force also raided Ark Pharm Inc. late Wednesday and recovered an unspecified amount of drugs, according to Joseph Fitzpatrick, spokesman for the U.S. Attorney's Office in Chicago.

In the complaint, DEA agents say they successfully made multiple purchases from both companies, which are registered with the Illinois Secretary of State as "domestic corporations." Neither have federal licenses to handle narcotics, prosecutors said.

Both companies' websites offered "controlled substances that are commonly recreationally abused," according to each complaint, and both used FedEx to disseminate their products. Both complaints state the purchases were sent from the suburban warehouses.

Before completing purchases, DEA agents say both companies required signatures on a disclaimer that said the available drugs were for laboratory use only.

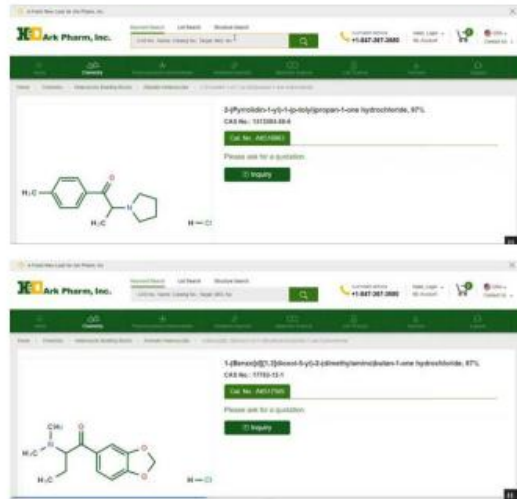
"I believe this is a common disclaimer that is used by internet drug traffickers on the mistaken belief that the disclaimer absolves them of criminal liability for distributing controlled substances," one agent testified in the complaints.

Fitzpatrick declined to comment on targeted customers until evidence from the raids could be reviewed, but he said the DEA found no indication that either company verified the agents' fake credentials.

"These were websites available on the open internet, not on any intranet or any dark web server," Fitzpatrick said.

Between January 2016 and February 2017, Ark Pharm Inc. made approximately 28,988 shipments and approximately 23,054 listed Huang as the shipper, according to the federal complaint.

Federal agents say they began investigating Ark Pharm Inc. because numerous packages labeled as plastic supplies were seized at the U.S. border after inspections revealed drug contents.



from: USA v. LIANFUANG HUANG,  
United States District Court, Northern  
District of Illinois, Eastern Division,  
May 25, 2018

## Supply Chain Security and Customer Vetting: Background

- What is customer vetting?
  - Know the customer
  - Understand why the customer is purchasing
  - Costs and benefits of vetting
  - Short-term vs. long-term benefits



- A few case studies are presented here
- Customer Vetting will be covered in greater detail in another module



BREAKING NEWS NEWS

## More people sickened by synthetic marijuana believed to be tainted with rat poison



By ROBERT MCCOPPIN | CHICAGO TRIBUNE | JUN 25, 2018 | 6:20 PM



Several new cases of severe bleeding caused by tainted synthetic marijuana have been reported in Illinois, most of them in Winnebago County, health officials announced Monday.

Officials in Winnebago County, in the Rockford area, confirmed there were fewer than five new suspected cases over the past two weeks, some requiring hospitalization. The causes of the illnesses are being investigated but are believed to have been the result of poisoning from synthetic marijuana.

"We don't know if this is a new batch of drugs or product that has been held back from when we began seeing cases at the end of March, but it reiterates the importance of staying away from synthetic cannabinoids," Illinois Department of Public Health Director Nirav Shah said in a news release.

In May, Illinois health officials reported that 164 people had being sickened over the previous two months by tainted synthetic marijuana, and four people died. The vast majority of cases were in Tazewell, Peoria, and Cook counties.

As the outbreak slowed recently, officials stopped counting the number of new cases, but reported the latest cases because it was an unusual outbreak of unknown cause, spokesman Melaney Arnold said.

"It's now a matter of those individuals seeking help for substance use disorder so they do not use synthetic cannabinoids," she said.

Synthetic cannabinoids are not marijuana, but are manmade drugs marketed as mimicking the effect of cannabis. They are sold both on the street and in places like gas stations and convenience stores in small packets under the brand name Blue Giant, K2, Spice, and other labels. This spring, some "fake weed" users began coughing up blood, having severe bloody noses or having blood in their urine.

Lab tests revealed that the drug had been contaminated with brodifacoum, a blood thinner used in rat poison.

An additional seven cases have been reported recently in Wisconsin, in Dane, Milwaukee and Outagamie counties, while another eight cases are suspected to be linked to the drug but not yet confirmed, officials said.

The treatment involves high doses of vitamin K, first intravenously, then up to 30 tablets a day for up to six months.

State law outlaws certain synthetic cannabinoids, but drug makers have repeatedly changed the ingredients slightly to get around the prohibition. Lawmakers passed a measure to ban all forms of synthetic cannabinoids, and the measure is awaiting a decision by Gov. Bruce Rauner.

[rmccoppin@chicagotribune.com](mailto:rmccoppin@chicagotribune.com)



## Supply Chain Security and Customer Vetting: Background

- Diversion of chemicals, cont.
  - Case study: fentanyl and fentanyl derivatives
    - Dual or even multi-use



## Supply Chain Security and Customer Vetting: Background

- Case study: Fentanyl
  - An essential medical drug (anesthesia and analgesia)



## Supply Chain Security and Customer Vetting: Background

- Case study: Fentanyl
  - A serious drug of abuse—easily available through batch custom fine chemical synthesis

### Chemical weapon for sale: China's unregulated narcotic

By ERIKA KINETZ and DESMOND BUTLER October 7, 2016



SHANGHAI (AP) — For a few thousand dollars, Chinese companies offer to export a powerful chemical that has been killing unsuspecting drug users and is so lethal that it presents a potential terrorism threat, an Associated Press investigation has found.

The AP identified 13 Chinese businesses that said they would export the chemical — a synthetic opioid known as carfentanil — to the United States, Canada, the United Kingdom, France, Germany, Belgium and Australia for as little as \$2,750 a kilogram (2.2 pounds), no questions asked.

Despite the dangers, carfentanil is not a controlled substance in China, where it is manufactured legally and sold openly online. The U.S. government is pressing China to blacklist carfentanil, but Beijing has yet to act, leaving a substance whose lethal qualities have been compared with nerve gas to flow into foreign markets unabated.

"We can supply carfentanil ... for sure," a saleswoman from Jilin Tely Import and Export Co. wrote in broken English in a September email. "And it's one of our hot sales product."

Despite periodic crackdowns, people willing to skirt the law are easy to find in China's vast, freewheeling chemicals industry, made up of an estimated 160,000 companies operating legally and illegally. Vendors said they lie on customs forms, guaranteed delivery to countries where carfentanil is banned and volunteered strategic advice on sneaking packages past law enforcement.

Speaking from a bright booth at a chemicals industry conference in Shanghai last month, Xu Liqun said her company, Hangzhou Reward Technology, could produce carfentanil to order.

"It's dangerous, dangerous, but if we send 1kg, 2kg, it's OK," she said, adding that she wouldn't do the synthesis herself because she's pregnant. She said she knows carfentanil can kill and believes it should be a controlled substance in China.

"The government should impose very serious limits, but in reality in China it's so difficult to control because if I produce one or two kilograms, how will anyone know?" she said. "They cannot control you, so many products, so many labs."

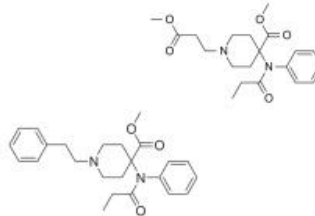
## Supply Chain Security and Customer Vetting: Background

- Case study: Fentanyl; Alleged use as incapacitating agent

**HOSTAGE DRAMA IN MOSCOW: THE AFTERMATH; Hostage Toll in Russia Over 100; Nearly All Deaths Linked to Gas** NY Times, Oct. 28 2002



Wikipedia



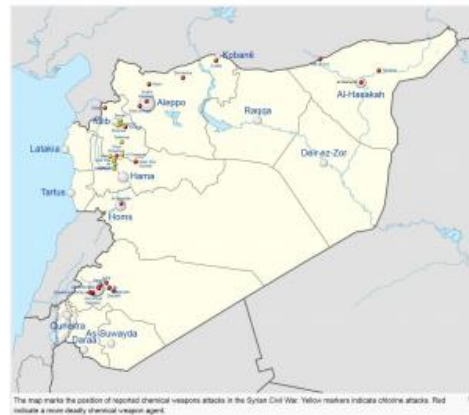
- Oct 23, 2002: Chechen terrorists seized the Melnikov Street Theatre, Moscow, during a performance of the musical "Nord-Ost,"
- 800 hostages were taken
- Oct 26, 2002, Russian Federal Security Service (FSB) unit pumped a chemical aerosol into the building and stormed it.
- At least 33 terrorists and 129 hostages died during or shortly after the raid.

Riches *et al.*, Analysis of clothing and urine from Moscow theatre siege casualties reveals Carfentanil and Remifentanyl use. *J. Analytical Toxicology*, 2012

25

## Supply Chain Security and Customer Vetting: Background

- Diversion of chemicals, cont.
  - Case study: Syrian CWA
    - Alleged use of Sarin and chlorine
    - Did Syria obtain chlorine and/or Sarin precursors through the supply chain?
    - Hypothetically, could better supply chain security and customer vetting have led to a different outcome?



26



## Supply Chain Security and Customer Vetting: Background

- What is supply chain management?
  - What are security requirements?
  - What is the difference between defense and resilience
  - What is customer vetting?
    - Know the customer

27



## Supply Chain Security and Customer Vetting: Background

- What are security requirements?
  - Measures necessary for confidence and trust associated with
    - ✓ People
    - ✓ Materials
    - ✓ Information
    - ✓ Transport
    - ✓ Transfer (acceptance, delivery, or import/export)

28



## Supply Chain Security and Customer Vetting: Defense and Resilience

- Defense stops an attacker before the attacker can fully achieve their goal
  - Reduces probability of occurrence of a successful attack without having much impact on potential consequences
  - Examples:
    - Adding security fencing or guards reduces the probability of a successful break-in
    - Carefully vetting of suppliers reduces the probability of their providing counterfeit products
    - Periodic security screening of employees reduces the probability of having a malicious insider
    - Multi-factor authorization for external access to control systems reduces the probability of an attacker gaining unauthorized access and manipulating the systems.



29



## Supply Chain Security and Customer Vetting: Defense and Resilience

- Resilience reduces the impact of a successful attack
  - Reduces consequences without having much of an impact on the probability of the attack
  - Examples:
    - Having redundant production or storage systems allows operations to continue even if primary systems are damaged
    - Having frequent, automatic backups of IT systems allows a prompt restoration of the systems in the event a cyberattack corrupts or deletes key information.
    - Having multiply suppliers allows production to continue even if one supplier needs to be fired after providing counterfeit products.



30



## Finding the Right Balance between Defense and Resilience

- An effective security program utilizes both defense and resiliency to achieve an optimal level of risk management.
- The key is to assess the risks and costs and then find the right balance for your company and circumstances.



Thank you



Dr. Radha Kishan Motkuri



## Exercise B – Identify Security Practices to Reduce the Threat of an Attack

Radha Kishan Motkuri, Cliff Glantz, and John Cort  
Pacific Northwest National Laboratory (PNNL)  
Richland, WA, 99352  
USA



PNNL is operated by Battelle for the U.S. Department of Energy

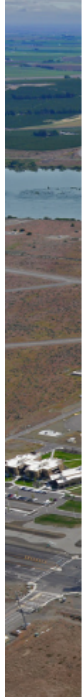


## Instructions

In the previous exercise you documented an array of attack scenarios with “threat agents” mounting attacks on Plant Alpha during various steps in the product supply chain.

Now shift your attention to the physical, cyber, and personnel security enhancements Plant Alpha might implement to reduce or eliminate those attack venues.





## Example Scenarios

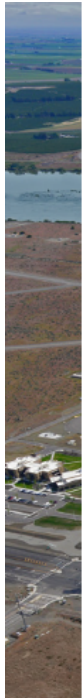


A nation state mounts a cyberattack to sabotage the plant during the **manufacturing process**, potentially releasing hazardous materials into the environment.

### Security Enhancements:

- Develop and implement a cybersecurity program to protect Plant Alpha's information systems and industrial control systems (ICS).
- Tighten access controls on the ICS to eliminate unauthorized pathways into the ICS network (e.g., two-factor authentication)
- Limit external access via the Internet to ICS.
- Ensure that when ICS fail, they fail to a safe state.
- Put ICS in locked rooms or cabinets to prevent unauthorized physical access by insiders.
- Train staff to quickly respond to a cyberattack and take steps to minimize negative consequences.

3



## Example Scenarios



**Criminals** hijack chemicals during transport from Plant Alpha to a customer. They acquire information from a Plant Alpha insider (through a bribe or a threat) about shipments of specialty chemicals to customers. They follow the truck and hijack it truck when the driver stops for lunch.

### Security Enhancements:

- Improve personnel security screening
- Enhance staff training and awareness programs that cover what to do when approached by someone who wants company "inside information".
- Place GPS tracking devices on trucks (useful if a truck is hijacked).
- Label all containers with identification numbers to enhance traceability.
- Restrict online access to the shipping information database to only those personnel who need that information.
- Provide training for drivers on what to do when faced with a security incident.

4



## Instructions

- Reform into groups.
- For each scenario your group developed in Exercise A (or interesting scenarios mentioned by other small groups), pick a range of physical, cyber, and personnel security steps that could prevent or minimize the loss from the attack.
- Choose a representative to present your proposed security enhancements this to the class.



5



## Present Results



6

## Biosketch of Dr. M. Surianarayana

**Dr. M. SURIANARAYANAN**

*Principal Scientist  
CSIR-Central Leather Research Institute  
Chennai, TN, INDIA*



Dr. Surianarayana, a fellow of the Madras Science Foundation, is currently the Principal Scientist at the Cell for Industrial Safety and Risk Analysis, CSIR-Central Leather Research Institute. His research areas of interests are chemical process safety and security, thermokinetic analysis of chemical process reactions, occupational safety and health, accident database, drug delivery systems, water and wastewater treatment, greener applications of ionic liquids in biological and chemical reaction systems and bioreaction calorimetry. He is in the Editorial Board of Chemical Engineering Journal as well as the Material Science for Energy Technologies.



# Security Vulnerabilities in Indian Supply Chain

Dr M Surianarayanan & Dr Clifford Glantz  
CSIR-CLRI & PNNL



## PREAMBLE: Supply Chain Vulnerability

- Security has been an issue since supply chains began
- "Unwanted effects" by internal or external forces
- Company information, facilities, and products may be subject to theft, sabotage, and hijacking, fraud, smuggling and piracy.
- Vehicles to deliver threats e.g., counterfeit materials and products, tampering the goods in transit, digital devices provided with malware pre-installed.
- Rising risks of terrorism
- Complex networks of storage and intermodal transport face these challenges
- The more complex a supply chain is, the more chance of a chink in its armour\*.
- Longer chains and more actors increase risk.
- Customer vetting is important in supply chain and product life-cycle ; a company may inadvertently provide hazardous materials to someone or some group with a malicious intent to misuse or weaponize that product.

Vulnerabilities in many parts of supply chain operations – targets and vehicles for delivering threats

\*Chink in its armour- vulnerability



# Supply Chain Areas of Security Vulnerability

- Security vulnerabilities may show up in three areas:
  - ✓ **People**  
Crime is driven by humans. Criminals may go to great lengths to obtain employment of one of their gang in a supply chain that they want to target.
  - ✓ **Processes**  
Processes have maximum vulnerability due to parametric sensitivities of hazardous inventory and critical operating limits
  - ✓ **Technology**  
With IT systems driving larger parts of supply chains, IT security is a growing issue. Examples are ERP, CRM and TMS.  
Rogue access to one system can lead to access to the next one, and so on.

## The Vulnerabilities in Supply chain

Vulnerabilities may pop up at any stage in the supply chain and during any portion of the lifecycle of a product

- Design– are facilities, systems, equipment, and software designed with security in mind. Are designs secure from theft or manipulation? Are designers properly vetted and trained for security?
- Construction – Are facilities, systems, and equipment built/installed according to design? Are personnel working in construction properly vetted and trained on security matters?
- Acquisition – Tampering and unauthorized replacement of products can make goods unsatisfactory or dangerous to customers.
- Manufacture -- Supply chain partners may not have the same standards or priorities when it comes to security.
- Storage – products and information are vulnerable for theft while they are being stored at many steps in the supply chain. This includes while being stored at the pharmaceutical or specialty chemical facility and again they have been delivered to customers for further processing, re-packaging, and distribution.
- Packaging – Theft and tampering are also concerns when goods are being loaded into containers and then placed in vehicles for transit.
- Transport – Cargo diversion, hijacking and piracy are all concerns.
- Waste management – Hazardous waste materials may be diverted for malicious purchases and so have to be properly tracked through their disposal, recycling, or transfer for re-use.

# Potential Supply Chain Vulnerabilities

## Physical Security System

Is your **physical security system** adequate to deter, detect, delay, or deny physical attacks up and including your design basis threat.

- **Potential vulnerabilities:**
- Inadequacies in the security guard force to deter, detect, delay, or deny attackers from achieving their objective.
  - Do you always have sufficient **numbers or guards** given the threats you face and the consequences of a successful attack?
  - Are guards adequately **training and equipped** to delay or deny attackers?
  - Do they have a plan **to call in law enforcement or reinforcements** to help address a security incident?
  - Is the plan **exercised** and does it produce a response capable of keeping an attack from being successful?

# Potential Supply Chain Vulnerabilities

- Inadequate protection of physical security-related **critical infrastructure**
  - Are critical infrastructure assets (e.g., electrical power, water) adequately protected within the facility fence line?
  - Are security barriers properly maintained (e.g., is your fence falling down or are there gaps or breaks in the fencing?)
  - Are power supplies to security equipment protected with back-up sources of power, batteries, or other mechanisms to keep them operating.
  - Are digital security systems protected against cyberattack or inappropriate manipulation by workers, contractors, or vendors?

# Potential Supply Chain Vulnerabilities

- Inadequate access control
  - Do employees display appropriate identification that indicates **approved access** to their location?
  - Is access by contractors, vendors, and suppliers **carefully controlled** and are outsiders escorted when in potentially sensitive areas to the facility.

# Potential Supply Chain Vulnerabilities

## Personnel Security

- Is your personnel security system adequate **to deter malicious actions by insiders** and respond to other types of security events?
- Do all facility workers have adequate **security training**?
- Do all workers know how to **detect and respond** to a security incident?
- Does security training cover **physical, cyber, information, and personnel security**?
- Are events conducted to raise and test security awareness and response by plant personnel (**drills**).
- Is monitoring conducted for **inappropriate use of plant computer systems**?
- Are penalties in place for **security violations**?
- Are all personnel with **unescorted access to the facility subject to security screening** when hired (including a criminal background check)?
- Does this **include contractors and vendors** who have unescorted access to the facility?
- Is any **criminal background screening** conducted of personnel entering Plant Alpha to deliver goods or pick-up products?
- Are workers or visitors to the plant ever searched for **weapons** or other contraband either when **entering or leaving** the property?

## Potential Supply Chain Vulnerabilities

- **Information Security**

- Is your **information security program** adequate to prevent the denial of access to, theft, or manipulation of information assets?
- Are adequate access and authentication processes in place to limit physical or electronic access to **sensitive information and information assets**?
- Are hardcopies of **sensitive company documents** kept in locked rooms or file cabinets when not in use?
- Are **policies and procedures** in place to cover the secure **storage, communication, and transportation** of sensitive company information?
- Are policies and procedures in place to cover the **secure disposal** of sensitive information and information assets.

## Potential Supply Chain Vulnerabilities

### Acquisition of Materials and Equipment

- Does the **acquisition of material** and **equipment** involve adequate checks for security issues?
- Is there inspection for **counterfeit parts and materials**?
- Are **suppliers vetted** for quality and reliability?
- Are security inspections conducted of **all deliveries and delivery equipment**.
- Are equipment adequately tested for security issues prior to **installation** or use at the facility?

## Potential Supply Chain Vulnerabilities

### Customer Vetting

- Are customers adequately vetted to guard against the **malicious use of products**?
- Are customers vetted to determine that they are **legitimate**?
- Are **restrictions on the sale of certain products** to customers rigorously followed?
- Are suspected **attempts to acquire hazardous or dual-use materials** reported to the authorities?

## Potential Supply Chain Vulnerabilities

### Transport

- Is the transportation of goods conducted in a **secure manner**?
- Are the transportation companies carrying products to **customers carefully vetted for security and reliability**?
- Are security requirements included in the **transport contracts**?
- Are goods **tracked during transport**?
- Is there a prompt **acknowledgement of receipt of goods** provided by customers?



# Potential Supply Chain Vulnerabilities – cyber security

Dr Clifford Glantz

## Cybersecurity

- Is your cybersecurity program adequate to protect your digital assets from a loss of availability, integrity, or confidentiality?
- Does the company have a comprehensive cybersecurity program?
- Are cybersecurity roles and responsibilities clearly defined and put in place?
- Are cybersecurity requirements for the acquisition of digital systems and assets put into procurement contracts?
- Is there coordination among IT, systems engineers, and physical security staff regarding cybersecurity.
- Is compliance with company cybersecurity policies and procedures periodically assessed?
- Does the company employ a defensive architecture for its business and control system networks?
- Is there regular logging and auditing of traffic through system firewalls to detect unauthorized activities (e.g., malicious intrusion, malware)?
- Are unused or unwanted software automatically removed?
- Are unused and unneeded communication ports on devices disconnected?
- Are tight security restrictions placed on external access to plant business and control systems – including restrictions on workers, contractors, and vendors?
- Are wireless pathways into systems protected at an equivalent level with wired communication pathways?
- Are adequate access and authentication processes in place to limit access to digital systems and assets?
- Are access permission lists reviewed and kept current?

## Case study 1: Theft of hydrocarbon fuel

- Powerful person contracted tanker lorries
- Hand-in-glove with Drivers
- Regularly siphoned fuel on its way to the stations
- Was not aware of the safety
- Unsafe fuel discharge resulted in huge fire
- Destroyed the neighbouring SME

Typical case of a supply chain vulnerability

## Case Study 2: Theft of a classified substance

- Pharmaceutical Company manufacturing anti bacterial solvents
- Involved the use of Cyanide Egg
- Cyanide Egg issued and handled carefully under direct supervision of the production incharge
- During night shifts –violation of rules
- Contract labor stole one of the eggs in his pant pocket for handing over it to a terrorist
- Got red-handed in the dressing room

## Case Study 3: Sabotage of oil pipelines

- Un-secured oil pipeline in a north-east refinery
- Agitating workers set fire to the oil pipeline
- Huge loss of fuel and exchequer

Case Study 4: Rented Warehouses- Major cities and near ports –  
A real potential for security threats!



- Poor storage practices
- Anything is stored with any – compatibilities are not checked –potential for safety and security issues
- Warehouse is not physical protected & access control
- Transportation threats
- ??????

## Case Study 5: Theft of methanol, rectified spirit & absolute alcohol

- Ease accessibility
- Workers distil in the lab
- Cases of poisoning and affected CNS

Thank you

D. Radha Kishan Motkuri



**Exercise C – Spot the Vulnerabilities**

Radha Kishan Motkuri, Cliff Glantz, and John Cort  
Pacific Northwest National Laboratory (PNNL)  
Richland, WA, 99352  
USA

U.S. DEPARTMENT OF ENERGY **BATTELLE**  
PNNL is operated by Battelle for the U.S. Department of Energy



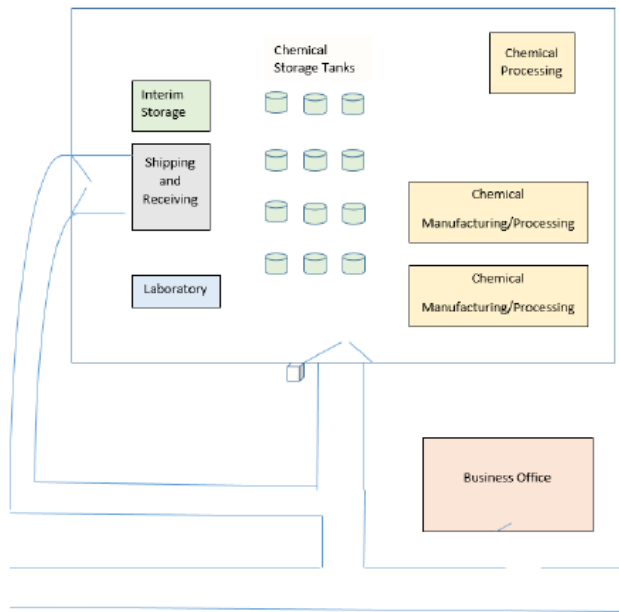
**Instructions**

In the previous exercise you have:

- identified an array of attack scenarios involving threat agents mounting attacks on Plant Alpha.
- Identified preliminary physical, cyber, and personnel security enhancements Plant Alpha might implement to reduce or eliminate those attack pathways.

In this exercise, we will take a deeper dive into identifying supply chain vulnerabilities





## Plant Alpha Map



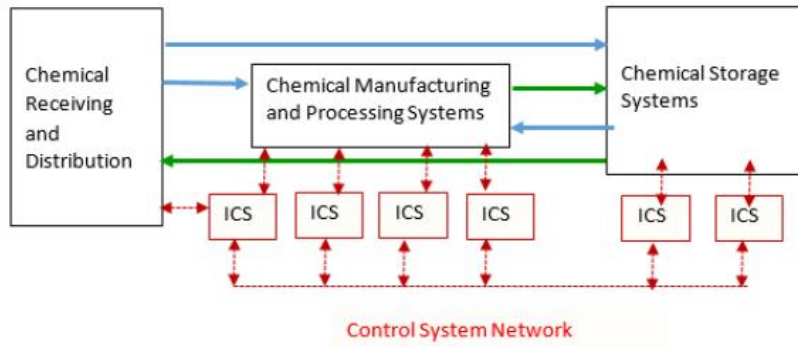
## Flow of Materials



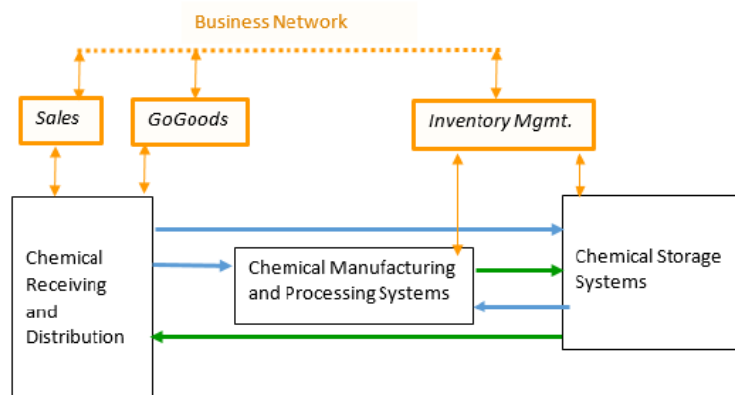


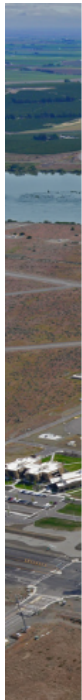


## Control System Network

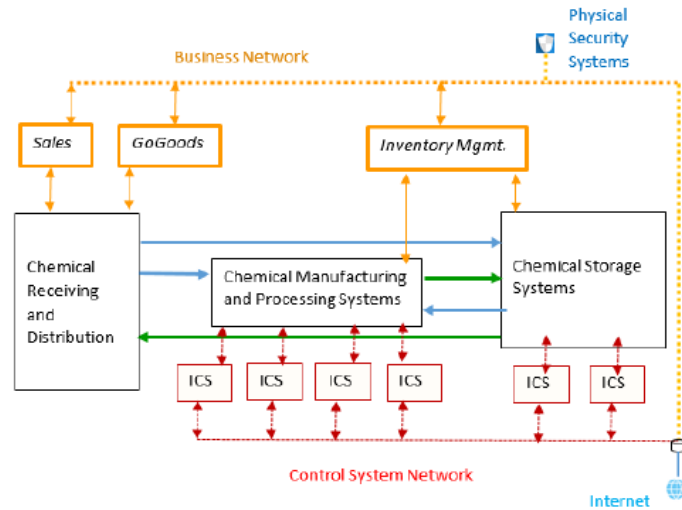


## Business IT Network





## Integrated View of Facility Networks and Flows



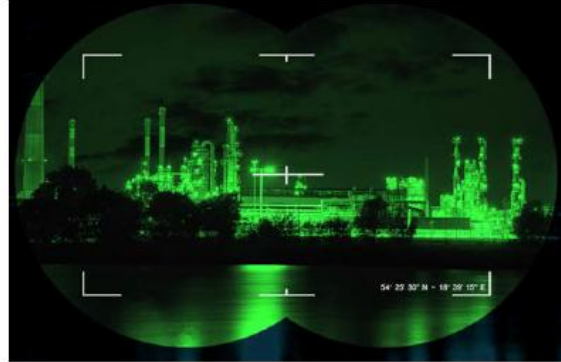
## Instructions

- Reform into groups.
- Review handouts regarding aspects of the Plant Alpha supply chain and product lifecycle.
- Pick select areas and identify specific supply chain vulnerabilities. Concentrate on security vulnerabilities that could allow the sabotage, theft, and diversion of hazardous or weaponizable chemicals.
- Choose a representative to present your proposed security enhancements this to the class.





## Present Results



9

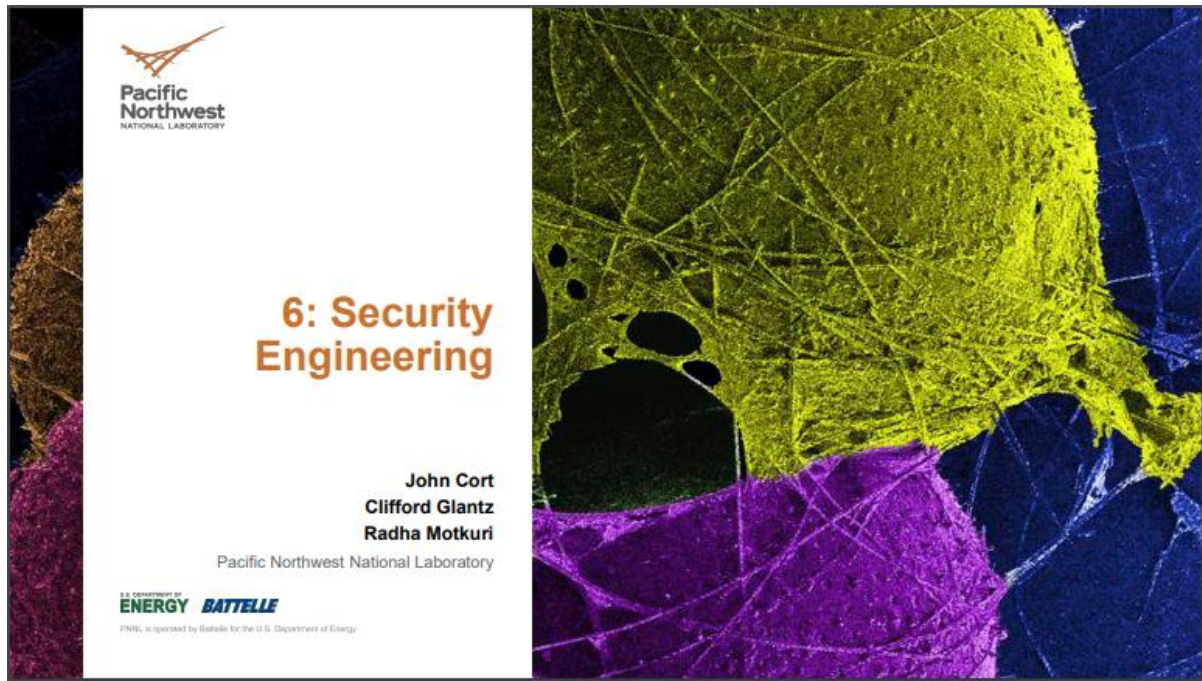


## Thank you



10

Dr. John Cort



Pacific Northwest NATIONAL LABORATORY

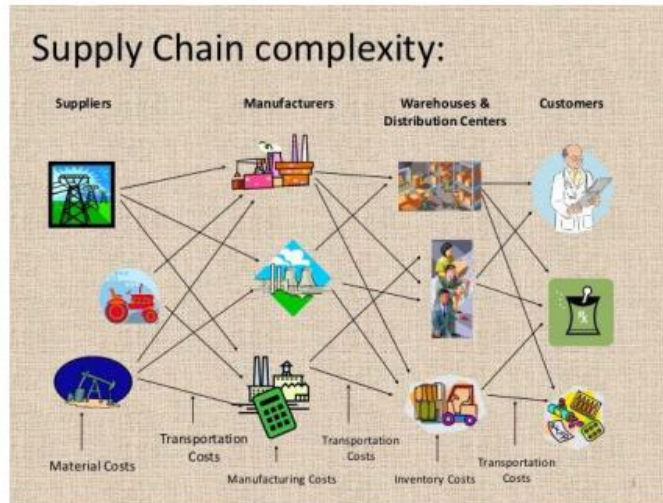
## Security Engineering

- Outline
  - Challenges due to a very complex system
  - Supply chains can be securely engineered to prevent abuse and crime
  - Approaches to reduce the risks of threats and vulnerabilities can be strategic, tactical, or both
  - A popular strategy is layered defence
  - Building security into equipment
  - This is ideal for ongoing supply chains that persist for long durations, e.g. product lifecycles

2



**Challenges due to Complexity:**  
The supply chain is a continuously evolving multilayered network of physical and cyber systems



3

- Complexity does not prevent the problem from being addressed if we recognize which elements of chemical supply chains are more attractive:
  - Chemicals
  - Manufacturing and production facilities
  - Transport and distribution infrastructure
  - Personnel
  - Symbolic nature of the industry itself
  - Along with many, many others

4





## Security Engineering

- Supply chains can be securely engineered to prevent abuse and crime
  - Secure storage areas: security reduces losses
  - Employee vetting
  - Cooperation and collaboration with upstream and downstream nodes in the supply and distribution network, recognizing shared interests in security, quality control, scheduling, etc.
  - Inventory Control: benefits business and security
  - Partnership with Import/Export regulators, border security
  - Transportation Security: trained and vetted professionals to safely and securely transport chemicals and materials

5



## Security Engineering: Strategies and Tactics

- Approaches to reduce security risks should include both strategies and tactics.
- Strategies are used to define or outline the desired outcome or goal
- Tactics represent the specific actions that are required to implement the strategy
  - What is to be done
  - Order of operations
  - Tools to be used
  - Personnel involved
- Strategies and Tactics must work in tandem:
  - Strategy without Tactics = Big plans and little action
  - Tactics without Strategy = Plenty of action, but little structure or order

6

*"Strategy without tactics is  
the slowest route to victory.*

*Tactics without Strategy is  
the noise before defeat."*

Sun Tzu



*"All men can see these  
tactics whereby I conquer, but what  
none can see is the strategy out of  
which victory is evolved."*

Sun Tzu

FamousQuotes123.com

## One Strategy: Defense-In-Depth

- "Defense-in-Depth" or a "layered defense":
  - Benefits both physical and cyber security
  - Avoid single points of failure
  - Helps limit access to products, systems, and data systems to only those who require it.
  - Prevents one individual from controlling multiple security layers in the system
- *Example: Truck drivers may need to view inventory data to know what to load or what they are carrying. However, they should not be able to manipulate the inventory control system. That might tempt them to manipulate the system for their own benefit.*



## Defense-in-Depth (cont)



- *Example:*
  - *Senior managers may want to see the status of products as they are being manufactured. However, having access to data should not include the ability to control production.*
  - *Senior managers at company headquarters may ask for remote access to facility control systems so they can observe production. However, providing remote access to control systems could allow an attacker to gain access to and then manipulate the control systems*
  - *A better approach is to allow the one way transfer of data to a control system viewer that can be remotely accessed. That viewer would not have a pathway for communicating instructions back to the control system and therefore could not be used to compromise the security of the control system.*

9

## Security Engineering

- Building security into infrastructure, equipment, data systems, and processes
  - This is ideal for ongoing supply chains that persist for long durations, e.g. product lifecycles
  - Topic for Discussion: What about custom chemical synthesis, where any order/customer is potentially unique or one-time-only.

10



## Security Engineering—elements

- **Physical security:** Security guards, perimeter security devices, locking devices, lighting, alarms, CCTV
- **Physical access control:** Access controls for employees, visitors, vendors and vehicles
- **Personnel security:** Policies for hiring, background investigations and termination procedures
- **Information security:** User ID, passwords, e-mail, Internet access, hardware & software security

11



## Security Engineering—elements

- **Procedural security:** Policies for shipping & receiving hazardous materials, warehouse security, document review and recordkeeping
- **Security training:** Safety and security training and related procedures.
- **Conveyance security:** Policies for control of seals, container and seal inspection and container storage
- **Business partner requirements:** Security-aware selection of carriers, suppliers and warehouses
- **Utilization of container security devices** (special for tier 3 companies)

12





## Security Engineering—elements

- Reduction of HazMat shipments

- Conversion to less hazardous derivative chemicals before shipping
- Relocation of facilities to be closer to buyers of dangerous chemicals
- •Order swaps with own factories / competitors
- •Security-aware consideration of mode of transport
- •Closer collaboration / coordination of operations with clients

13



## Security Engineering—details

- Engineering solutions for chemical security—ideas
  - Hiding of storage tanks and keeping them far from perimeter
  - Inventory control
  - Tamper-evident packaging
  - Biometric driver identification
  - Make security a personal responsibility
  - Safe driver behaviour (no hitchhikers, no social media updates)
  - Background checks
  - Performance monitoring
  - Training (expectations, procedures, responsibilities)
  - Creating strong security culture (engage shippers, carriers, freight forwarders and authorities in security & make security a internal priority)

14





## Security Engineering—details

- Engineering solutions for chemical security—ideas
  - Try to keep chemical facilities and shipping routes away from vulnerable infrastructure (government buildings, tunnels, bridges, urban areas)
  - Advanced route planning to reduce number and distance of HazMat shipments (DOW case)
  - If possible, alternate routings and shipping times
  - Observe criminal and insurgent activity outside facilities and near shipping routes
  - Tracking & tracing with GPS solutions (spill over benefits in terms of logistics)
  - Electronic cargo sealing systems
  - Remote vehicle immobilization capabilities
  - Cyber security (information about shipping schedules and routes)
  - Integration of cyber security into the overall supply chain security strategy

15

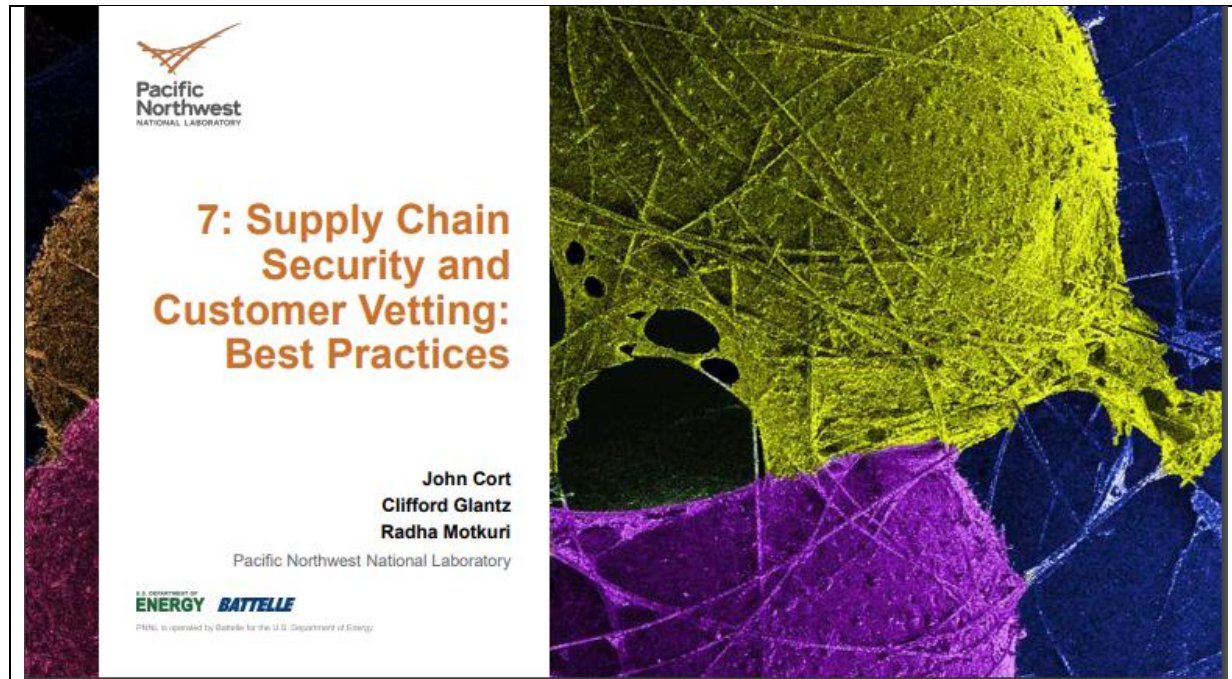


## Security Engineering—details

- Engineering solutions for chemical security—ideas
  - Other ideas?
  - What are we missing?
  - Can we use a "red team" approach to find vulnerabilities?

16

Dr John Cort



Pacific Northwest NATIONAL LABORATORY

## Supply Chain Security and Customer Vetting: Best Practices

- Outline
  - Chemical Weapons and TICS are global threats requiring global counter approaches
  - However, regional efforts integrated globally are more easily implemented
  - Examples
    - Gene synthesis as a model practice that has been widely adopted *regionally* (US)
    - Custom synthetic narcotics as a problem in search of a practice
  - Regulations (no consensus) vs. Practices (can reach consensus)
    - Failures of prohibition and traditional concepts of chemical weapons
  - Incentivization of best practices
  - Different practices are suitable for different types and sizes of firms
  - Addressing People
  - Addressing Processes
  - Addressing Equipment
  - New Technologies (e.g. RFID chips, digital monitoring, blockchain)

2



## Supply Chain Security and Customer Vetting: Best Practices

- Customer Vetting in practice:
  - Custom DNA synthesis
    - In molecular biology, cloning has become increasingly less attractive as a means of genetic manipulation.
    - Instead, assembly of synthetic oligonucleotides has become cheaper and more reliable
    - However, this makes it possible to assemble entire genomes, in principle
    - Smaller genomes are easier to assemble than others
    - Virus genomes are quite small; horsepox synthesis published in Science was a wake-up call
    - Some viruses are very bad; ergo we do not want irresponsible custom DNA synthesis to occur
    - Solution: customer vetting and screening of oligonucleotide synthesis requests has been adopted by the major US vendors

3



## Supply Chain Security and Customer Vetting: Best Practices

- Customer Vetting Case Study:
  - Custom organic synthesis and chemical vendors—is customer vetting ever done?  
Probably not:
    - ✓ Several years ago, in a project probing chemical security practices, custom synthesis of 1 kg of a highly toxic pesticide (technical grade, 90+ % purity) was ordered online, paid for by personal credit card, and delivered to a residential street address. No questions were asked. The material was analyzed and shown to be the compound that was ordered, and it was highly pure—as pure as the technical grade material produced and formulated into a product.
    - ✓ Numerous vendors online offer custom synthesis services.
    - ✓ Organic synthesis is moving towards automated determination of the synthetic route (see Sigma's software) and automation of the synthesis itself.

4



## Supply Chain Security and Customer Vetting: Best Practices

- Customer Vetting Case Study:
  - Large Chemical Vendors: is customer vetting ever done?  
Yes, at least in some cases. Examples:
    - ✓ Sigma-Aldrich policy, first time orders policy:  
"...supply the service representative with shipping and billing information. The representative will ask some questions about your general business, along with taking the order. The New Account Department will then very this information, as well as validate our intend use of our products. You may be contacted for further clarification..."
    - "...buyer will property test, use...products purchased from Sigma-Aldrich in accordance with the practices of a reasonable person who is an expert in the field and in strict compliance with all applicable laws and regulations, now and hereinafter enacted."

5



## Supply Chain Security and Customer Vetting: Best Practices

- Customer Vetting Case Study:
  - Custom organic synthesis and chemical vendors—is customer vetting ever done?  
Often it is not, either by default or with complicity in misuse by the customer.  
Examples:
    - ✓ Fentanyl. Fentanyl is a significant threat to public health in the US and elsewhere (users, and first responders). Many fentanyl derivatives are active, potency is often not known. New variants inevitably come from custom synthesis. China crackdown on Fentanyl.
    - ✓ Anabolic steroids operation in WA and elsewhere. Steroids are sold (to athletes, high school students, etc.) online and delivered through the mail. Sometimes they come directly from overseas (typically, China), unclear if it is from the manufacturer or (more likely) a middleman, also sometimes through a U.S. middleman. Does the manufacturer know their product is being sold in this market? Or are chemicals being diverted away from legitimate downstream customers? Does the manufacturer care? Or suspect anything is happening?
    - ✓ Synthetic Cannabinoids

6



Dr. Radha Kishan Motkuri



## Exercise D – Supply Chain Security Best Practices

Radha Kishan Motkuri, Cliff Glantz, and John Cort  
Pacific Northwest National Laboratory (PNNL)  
Richland, WA, 99352  
USA



PNNL is operated by Battelle for the U.S. Department of Energy



## Instructions

In the previous exercise you have:

- identified an array of attack scenarios involving threat agents mounting attacks on Plant Alpha.
- Identified preliminary physical, cyber, and personnel security enhancements Plant Alpha might implement to reduce or eliminate those attack pathways.
- Identified specific security vulnerabilities in the Plant Alpha supply chain and chemical lifecycle.

In this exercise, we will explore specific supply chain security best practices that could be applied at Plant Alpha to remedy the observed vulnerabilities.







## Areas to Consider

- Plant Alpha's Infrastructure: Design, Construction, Testing, and Maintenance
- Business Network Security
- ICS Network Security
- Physical Security
- Personnel Security
- Acquisition of Materials for Manufacture
- Processing/Manufacture/Storage of Chemicals
- Sale of Products to Customers
- Transport and Delivery of Products
- Waste Management

3



## Instructions

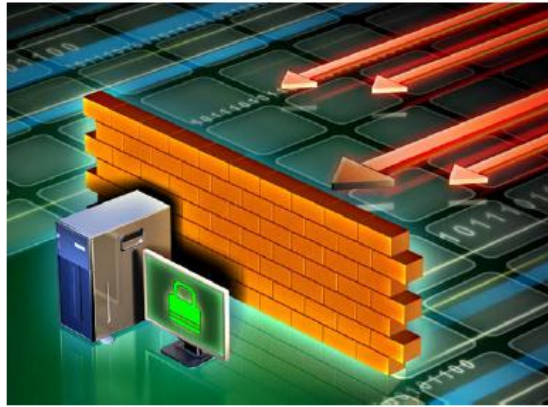
- Reform into groups.
- Select several areas of concern.
- Review information on vulnerabilities of the Plant Alpha supply chain and product lifecycle.
- Identify security practices that can reduce or eliminate specific vulnerabilities and therefore improve supply chain security.
- Choose a representative to present your proposed security enhancements this to the class.



4



## Present Results



v



## Thank you



**BIO-SKETCH of Mr. V.V Sasi Kumar**



Mr. Sasi Kumar is presently working as, Deputy Chief Inspector of Factories, Nalgonda, for the Factories Department of Government of Telangana State, India. He has 27 years of experience in the Factories Inspectorate. Basically, he was post graduated in Production Science and Technology (M.Tech) from IIT, Kharaghpur, with Mechanical Engineering Background from JNTU, College of Engineering , Anantapur. He has done L.L.B from Kakatiya University ,Warangal. TS. He attended P.G Diploma in Environmental Laws at NLSIU, Bangalore and submitted Project Work on Environmental Performance Indicators related to the Cement Plants. He is a member of ASME, Aichee, ACM and Sigma Xi and previously served as NSC Council, A.P Chapter, Hon. Secretary. Earlier he worked as a Junior management Trainee at Bhilia Steel Plant, Bhilia (SAIL).

**BIO-SKETCH of Mr. C. Sudhakar**



Mr. C Sudhakar, M. Tech, ADIS (CLI, Bombay)

Presently working as Principal Technical Officer – Safety and having an experience of 29 years in various fields/industries (CSIR-IICT (R&D Institute), Bulk Drug, Battery, Glass Fiber industries and Construction & Consultancy).

Indo-US Workshop on  
**Strengthening Supply Chain Security**  
in  
**The Pharmaceutical**  
And  
**Contract Chemical Synthesis Industries**  
Day-2

**INDIAN**  
**SECURITY REGULATIONS**  
**AND**  
**STANDARDS**

Mr. C SUDHAKAR M.Tech, ADIS.,  
Principal Technical Officer – Safety  
CSIR- IICT, Govt of INDIA  
sudhakarc@csiriict.in

Presented By

Mr. V V SASI KUMAR, M. Tech, L.L.B,  
Deputy CIF, Department of Factories,  
Government of Telangana State, TS.  
Velloresasikumar39@gmail.com

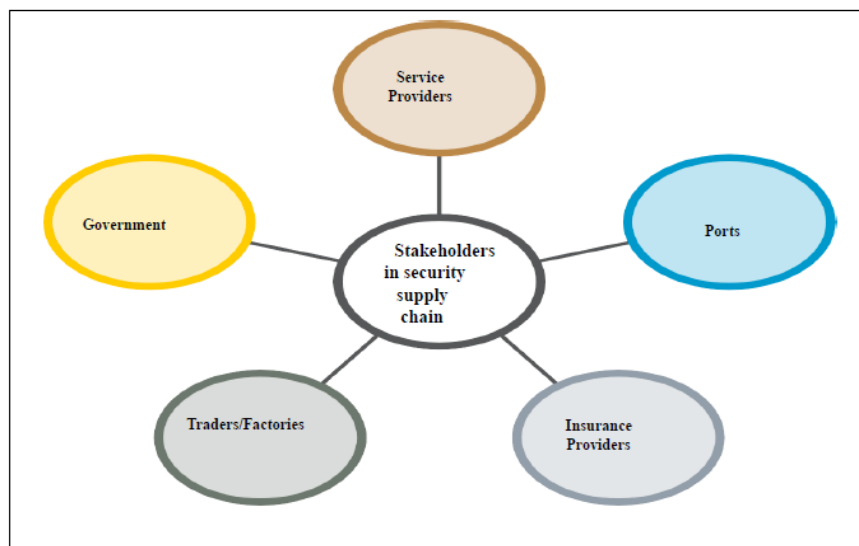
**Brief :** In India there are about 1861 Major Accident Hazard (MAH) units, spread across 301 districts and 25 states & 3 Union Territories, in all zones of the Country.

Besides, this there are about thousands of Registered and Hazardous Factories (below MAH criteria) and un-organized sectors dealing with the numerous range of Hazardous chemicals as a Raw materials, posing a serious and complex levels of Disaster risks, during its Supply chain (SC), vulnerabilities.

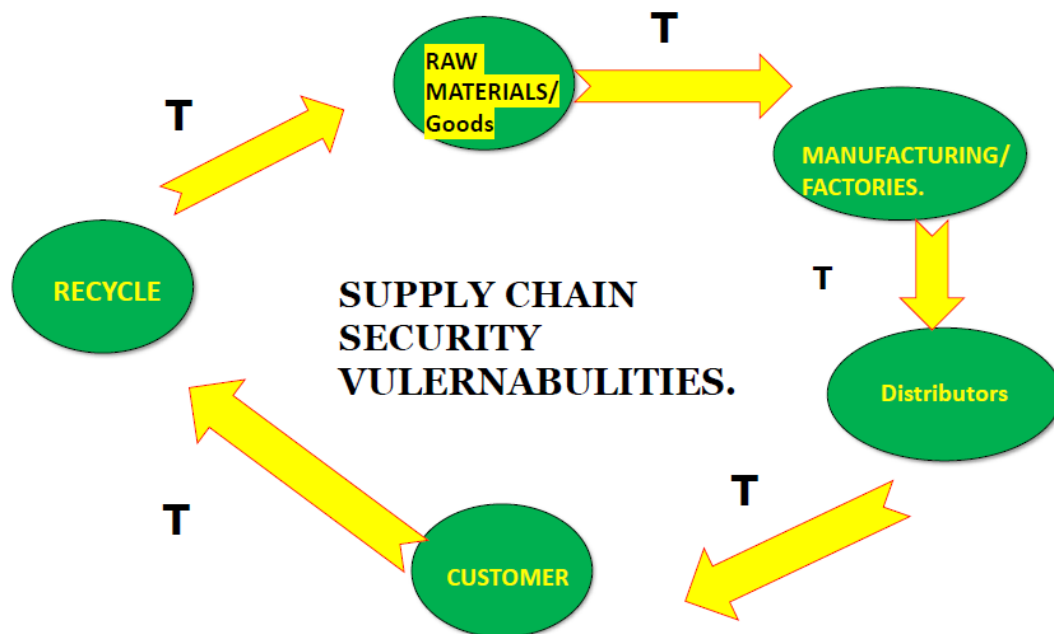
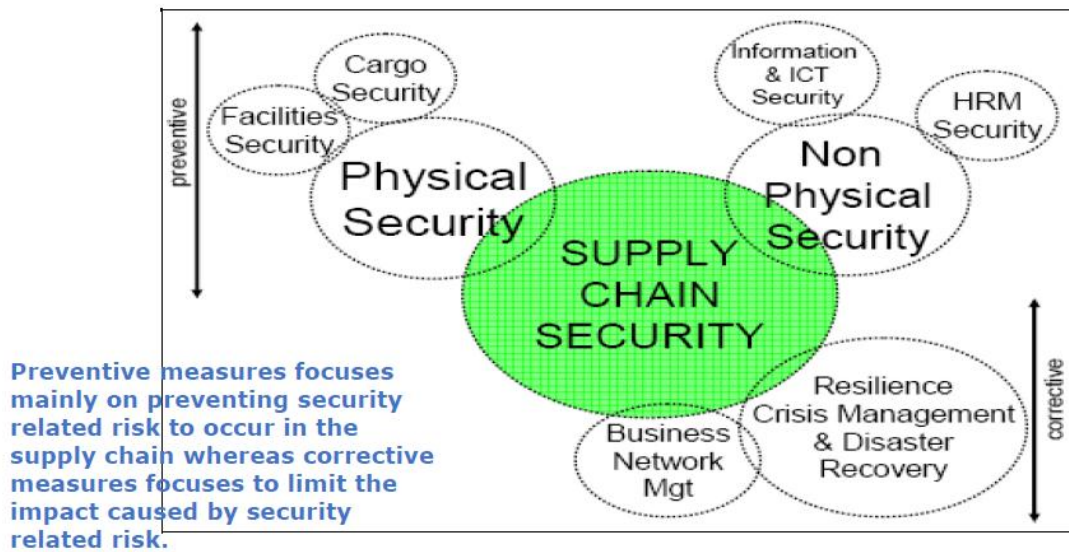
These Risks may manifest in to accidents and which are significant in terms of injuries, pain, suffering, loss of lives, damage to property and environment. India continued to witness a series of chemical accidents even after Bhopal had demonstrated the vulnerability of the country.

Only in last decade, there are about 130 significant chemical accidents are reported in India, which resulted into 259 deaths and 563 persons are got Injured.

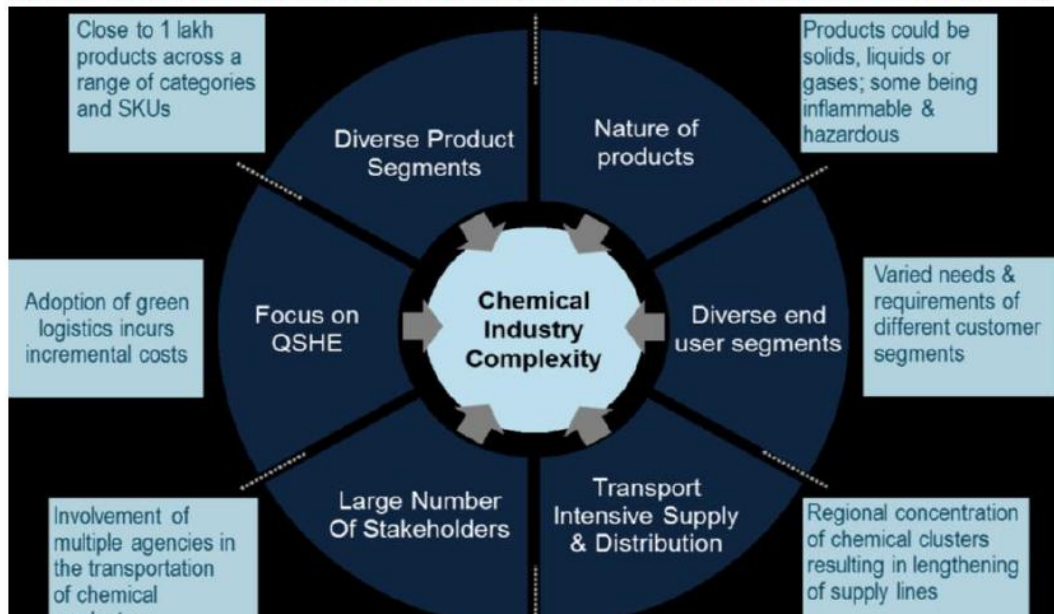
**All Stakeholders in the supply chain are dependent on each other, so all basic security requirements in a supply chain must be fulfilled by all of them, in order to prevent and recover during disruptions while goods are in transit.**







**The complexity of the chemical industry makes chemical logistics very challenging**



**ISO -28000 STANDRD –ESTABLISHES THE SECURITY MANAGEMENT OF THE SUPPLY CHAIN VULERNABULITIES ,**

- Presently the Standard had been adopted by Maritime, Logistics and Warehousing providers, Manufacturing facilities, Services, Hotel and Tourism Industries,
- **Benefits of the Standard:** Benefit of having Qualification of Tenders, Cost Savings from Both increased Efficiency, Budget Awareness, Reduction in Custom Compliance Audits and Inspections, having easy Integration with other Standards like, **ISO-9001,14001,OSHAS-18001**.
- Standard establishes an effective Security Management System,
- Identifying of Security Threats, Adopting of Security Management Policy & Planning,
- Establishes Procedures to Manage the Legal, Statutory, Regulatory Security Requirements,
- Establishes the Security Management Structures-Roles, Responsibilities , Authorities,
- Establishing Competence & Training and Security Communication Procedures, Security Management Emergency Plan, Investigation of Security Incidents

<u>Standard No</u>	<u>Publication Year</u>	<u>Reaffirmed Year</u>	<u>Title</u>
<u>IS 6566</u>	2001	2017	Series 1 Freight containers - Classification, dimensions and ratings
<u>IS 6865</u>	1973	2014	Pallets for Use in ISO Series 1 Freight Containers
<u>IS 6928</u>	2001	2017	Freight Containers - Coding, Identification and Marking
<u>IS 7622</u>	2001	2017	Series 1 Freight Containers - Handling and Securing
ISO International Shipping Container Standards			

- ❖ **STANDARD COMMUNICATION PROTOCOLS ARE TO BE ESTABLISHED FOR PREVENTING OF CRASHES BETWEEN THE VEHICLES TO VEHICLES.**
- ❖ **THE PROTOCOL WILL ENHANCE THE SAFETY AND SECURITY OF THE VEHICLES CARRYING THE HAZARADOUS CHEMICALS ACROSS THE CITIES.**
- ❖ **ONE SUCH TECHNOLOGY IS **RFID** EXISTS IN SEVERAL FREQUENCY BANDS FOR MANY DIFFERENT APPLICATIONS, EACH WITH ITS OWN CHARACTERISTICS.**
- ❖ ****RADIO-FREQUENCY IDENTIFICATION (RFID)** USES**
- ❖ **ELECTROMAGNETIC FIELDS TO AUTOMATICALLY IDENTIFY AND TRACK TAGS ATTACHED TO OBJECTS.**
- ❖ **THE RFID TAGS CONTAIN AT LEAST THREE PARTS: AN IC THAT STORES AND PROCESSES INFORMATION AND THAT MODULATES AND DE-MODULATES THE RADIO FREQUENCY (RF) SIGNALS;**
- ❖ **A MEANS OF COLLECTING DC POWER TOVFROM THE INCIDENT READER SIGNAL AND AN ANTENNA FOR RECEIVING AND TRANSMITTING THE SIGNAL.**

- ❖ **THE RFID TAG INCLUDES EITHER FIXED OR PROGRAMMABLE LOGIC FOR PROCESSING THE TRANSMISSION AND SENSOR DATA, RESPECTIVELY.**
- ❖ **THE RFID BASED LOCKING SYSTEM CAN BE USED FOR ACCESS MANAGEMENT, TRACKING OF GOODS, TRACKING OF PERSONS, TOLL COLLECTION AND CONTACTLESS PAYMENT, MACHINE READABLE TRAVEL DOCUMENTS, AIRPORT BAGGAGE TRACKING LOGISTICS,**
- ❖ **WASTE MANAGEMENT: RFID HAS RECENTLY DEVELOPED IN THE WASTE MANAGEMENT INDUSTRY. RFID TAGS ARE INSTALLED ON WASTE COLLECTION CARTS, CONTAINERS, LINKING CARTS TO THE OWNER'S ACCOUNT FOR EASY BILLING AND SERVICE VERIFICATION .**
- ❖ **THE MAIN SUCCESS FOR THE TECHNOLOGY HAS COME FROM THREE AREAS, TICKETING, PAYMENT SYSTEMS AND SUPPLY CHAIN TRACKING.**

## **THE RELEVANT INDIAN STATUTES FOR DEALING WITH THE SECURITY ISSUES OF SUPPLY CHAIN VULNERABILITIES :**

- ❖ **The Petroleum and Minerals Pipe Lines (Acquisition of Right of User in Land), Amendment Act, 2011,**
- ❖ **The Prevention of Damage to Public Property Act, 1984;**
- ❖ **Indian Penal Code (IPC) and Cr .P.C (Criminal Procedural Code);**
- ❖ **UAPA Act : Unlawful Activities (Prevention) Act, 1967,**
- ❖ **The Chemical Weapons Convention Act, 2000;**
- ❖ **THE MANUFACTURE, STORAGE AND IMPORT OF HAZARADOUS CHEMICALS RULES, 1989,**
- ❖ **EXPLOSIVES ACT 1884 & THE EXPLOSIVES RULES, 2008, THE EXPLOSIVE SUBSTANCES ACT, 1908, THE AMMONIUM NITRATE RULES, 2012,**
- ❖ **International Ship and Port Facility Security Code (ISPS Code). Under SOLAS**
- ❖ **THE INDIAN FACTORIES ACT, 1948 AND AMENDED ACT 1987 AND THE TELANGANA STATE RULES MADE THERE UNDER;**
- ❖ **THE CENTRAL MOTOR VEHICLES ACT, 1988 AND THE CENTRAL MOTOR VEHICLES RULES, 1989, Amended , 2015;**
- ❖ **The Hazardous Waste (Management , Handling Transboundary Movement) Rules , 2008.**
- ❖ **THE ENVIRONMENT (PROTECTION) ACT OF 1986;**
- ❖ **THE PUBLIC LIABILITY INSURANCE ACT, 1991;**
- ❖ **THE CHEMICAL ACCIDENTS (EMERGENCY PLANNING, PREPAREDNESS AND RESPONSE) RULES, 1996, Amended 2005.**
- ❖ **The Disaster Management Act, 2005 ;**
- ❖ **The Information Technology Act, 2000.**

## **The Petroleum and Minerals Pipe Lines (Acquisition of Right of User in Land), Amendment Act, 2011 :**

**Sec 7:** The Government had the Right of User Land for laying the Pipe Line to distribute the Petroleum, Gas and Other Minerals,

**Sec 15 (2):** Whoever wilfully disrupts the Pipe Line, Making any connection with the Pipe Line for Transferring of Petroleum or Gas any other Mineral or causing any Damage to the Pipe Line with Fire or Explosion are Rigorously Punishable,

The Offence is a Cognizable and Non-Bailable One . With this Statute the Govts. can Protect the Essential Commodities Like Petrol, Gas Supply Chain Distribution Network from Security Vulnerabilities.

## **THE PREVENTION OF DAMAGE TO PUBLIC PROPERTY ACT, 1984**

**Sec 2:** Defines Public Property Means and which includes any Moveable or Immoveable Property or Machine Owned by the Government,

**Sec 3(2) and Sec (4):** Who ever do any Mischief to the Public Property building, installation or other property used in connection with the production, distribution or supply of water, light, power or energy;  
(b) any oil installations;  
(c) any sewage works;  
(d) any mine or factory;  
(e) any means of public transportation or of tele-communications shall be a Punishable Offence.

- If the above Mischief has been Carried out by using Fire or Explosion the Violation is still more Rigorously Punishable .

The above Statutes is to Safeguard the Security Vulnerabilities of the Govt Supply Chain ,Transpiration, Manufacturing Facilities.



**Sec 284 & Sec 285 & 286 of IPC:** Whoever does with any Poisonous Substance or Fire or any Combustible Matter or Explosive Substance an Act of Rash and Negligently or Omitting an Act causing Danger to Life, Injury to any Person are Punishable under IPC With Imprisonment or with a Fine or Both.

By this Provision if Intentionally Rash and Negligently Causes any of the above Harm while Transporting, at Warehouse, resulted in the release of Hazardous Chemicals causing Potential Harm is Punishable.

**Sec 379 :** Whoever Causes any theft are Punishable with Imprisonment for three Years or With Fine Or Both

**and Sec 380 :** Who ever causes any theft in any Building or Vessel shall be Punishable with Imprisonment for Seven Years and With Fine.

By using the Provisions who ever disrupts the Supply Chain by doing the Act of Theft are Punishable.

**Sec 120-B :** Who ever is made Criminal Conspiracy or Party to it Causing Death is Punishable for Life or R.I for Two Years.

Under this Provision if nay Conspiracy made by disturbing the Hazardous Chemical Supply Chain, while doing the Transportation with an Intention to Cause Death are Punishable.

**Chapter VI of the IPC – offences against the State.** Chapter VI spans from section 121 to 130 in the IPC, and primarily contains the offence of 'waging war against the Government of India' (section 121), 147 and 'sedition' (section 124A) **(Terrorism),**

**UAPA Act :** Unlawful Activities (Prevention) Act, 1967.

## THE CHEMICAL WEAPONS CONVENTION ACT, 2000

**Sec 2(e)** : Defined Goods in relation to the Toxic Chemicals ,Pre- Cursors , Discrete Organic Chemicals, Containing ,P,S or Fluorine or Apparatus used in the Production ,Processing, Storing of Toxic Chemicals,

**Sec 2(k)**: The Handling of said Chemicals are not Prohibited for Industrial, Agricultural, Medical and Pharmaceuticals, Military Purposes, Law Enforcement for Riot Controls,

**Sec 7(s)**: The National Authority shall ensure Safety ,Health and Environment during the Transportation, Sampling, Storage, Destruction of C.W Production Facilities, lessening of Inventories,

**Sec 13**: No person shall Possess chemical Weapons, Pre-Cursors and Riot Controlling Agents,

**Sec 17**: Sch-I Chemicals Export/Import is Prohibited,

**Sec 18**: Sch-I to III mfg. facilities of Chemicals shall be Registered .

## The Manufacture ,Storage And Import of Hazardous Chemicals , Rules,1989, Amended Rules,1994 and 2000

**These Rules are promulgated under Sec 6,8 and 25 of E.P Act,1986.**

The Rules are dealing with the issues of an Operations, Storage, including Pipe Line Transfer, Import and Export of Hazardous Chemicals.

**Rule (2)(h)**: Industrial Activity includes an Operation or Process Carried out in an Industrial Installation as referred in Schd-4,involving one or more Hazardous Chemicals as listed in the Schedules. On Site Storage, Transport or Isolated Storage or a Pipe Line Transfer.

**Rule [2][j]** defines Major Accident includes involving loss of Life inside or out side the Installation, Ten or more Injuries Inside and or one or more injuries outside or release of Toxic Chemicals or explosion or fire or spillage of Hazardous chemicals resulting in On-Site or Off-Site Emergencies or adverse effects to the Environment.

**Rule [2][j][a]:** MAH installations Means –Isolated Storage and Industrial Activity at Site Handling(including Transport through Carrier or Pipe Line)

**Rule [2][ m] :** Site includes any Location where hazardous Chemicals are Stored, manufactured, handled, Disposed also includes Pier, Jetty, Similar any Floating Structurer whether Floating or Not.

**Rule [2][k] :** Pipe Line means a Pipe or a System of Pipes for the conveyance of a Hazardous Chemicals ,the Pipe Lines also includes Interstate Pipe Lines.

**Rule 4:** Under the general responsibility of the Occupier ,during the Industrial Activity shall Take adequate Steps to Prevent Major Accidents and to Limit its Consequences to Persons and Environment. Provide Information, Education, Training and Equipment including Antidotes if necessary.

**Rule 10 &11 :** Submission of Annual Safety Audit Reports and Updating.

**Rule 13 & 14 :** Preparation of On-Ste Emergency Plan and Off-Site Emergency Plan,

**Rule 15:** Giving of Advance Information to the Persons liable to be affected by a Major Accident,

If the affected one is Out-Side the Site, through the respective Dist. Emergency Authority the information can be Publicised,

Which Includes:

a).The Nature of Major Accident Hazard ,

b).The Safety Measures and Do's and Don'ts which can be adopted during the Major Accident,

**Rule 17:** Collection ,Development and Dissemination of Information, includes, Hazard Identification, Developing of M.S.D.S Sheets.

**Under Rule 17(4):** Ever Container of Hazardous Chemicals shall be clearly Labelled to Identify

a).The Contents of the Container,

b).The Name and Addresses of the manufacturer or Importer of the Hazardous Chemicals,

c).The Physical , Chemical and Toxicological Data as per the Criteria,

d).The Container can also be Tagged[GPS,RIFD] or accompanying of the Documents.

## **Rule 18.Import of Hazardous Chemicals :**

**Sub-Rule-(2):**Not less than "30" Days prior to Import or at least on the date of Import, the Responsible Person shall inform to CIF/DF the following Information Related to the Hazardous Chemicals as listed under the Schedule :

- i).The Name & Address of the Person receiving the Consignment in India,
- ii).The Port of Entry to India,
- iii).The Mode of Transport.
- iv).The quantity of Chemicals being Imported,
- v).Complete Product Safety Information.

**Sub-Rule (3) :** If the Chemical is being Imported is likely to cause Major Accidents, the Authority may direct to Take the Importer such Safety Measurers ,

**Sub-Rule3-A:** The Authority can also Stop the Imports on the Grounds of Safety and Environmental Considerations,

**Sub-Rule (4) :**The Authority can Simultaneously inform to Port Authorities ,regarding the Measures to be adopted while Off-loading the Consignment related to Safe Handling and Storage,

**Sub-Rule (5):** A Record also shall be Maintained regarding the imported Hazardous Chemicals as specified in the Sch 10 ,

**Sub-Rule (6):**The Importer Shall ensure the Transport of Hazardous Chemicals to the intended Destinations shall be in accordance with the central Motor Vehicles Rules ,1989 framed under the Provisions of the Motor Vehicles Act,1988.

## **Schedule 10 under Rule 18(5)**

- 1.Name and Address of the Importer:
- 2.Date and Reference No of issuing of Permission to Import Hazardous Chemicals.
- 3.Discription of Hazardous Chemicals :
  - a).Physical Form:
  - b).Chemical Form:
  - c).Total Volume and Weight:  
(In Kgs/Tonnes)
- 4.Description of Purpose of Import:
- 5.Description of Storage of Hazardous Chemicals:
  - a).Date:
  - b).Method of Storage:

# Explosives Act 1884:



### Explosives Act 1884:

It is an Act to regulate the manufacture, possession, use, sale, [ transport, import and export] of Explosives.

**Sec 4(d)"explosives" means gunpowder, nitro-glycerine, nitroglycol, gun-cotton, di-nitro-telemetry-nitrotoluene, picric acid, di-nitro-phenol, tri-nitro-resorcinol (styphnic acid), cyclo-trimethylenetrinitramine, penta-erythritol-tetranitrate, tetra, nitroguanidine, lead azide, lead styphnate, fulminate of mercury or any other metal, diazo-di-nitro-phenol, coloured fires or any other substance whether a single chemical compound or a mixture of substances, whether solid or liquid or gaseous used or manufactured with a view to produce a practical effect by explosion or pyrotechnic effect; and includes fog-signals, fireworks, fuses, rockets, percussion caps, detonators, cartridges, ammunition of all descriptions and every adaptation or preparation of an explosive ;**

# *The Explosives Rules, 2008:*

## ***The Explosives Rules, 2008:***

(22) "explosive limit" means the maximum quantity of explosives permitted by the licensing authority to be stored or processed in a particular premises,

*(33) "man-limit" means the maximum number of individuals permitted by the licensing authority to work inside a particular premises for manufacture or processing of explosives;*

*47) "safety management plan" means the comprehensive plan for ensuring and managing safety in an explosive manufacturing factory;*

*(48) "safety distance" means the distance necessary under these rules to be kept clear between any licensed factory shed, magazines, store house or other licensed premises and protected works as referred to in Schedule VIII.*

# THE EXPLOSIVE SUBSTANCES ACT,1908:

## **THE EXPLOSIVE SUBSTANCES ACT,1908:**

**Sec 2: (a)"explosive substance".-** In this Act the expression "explosive substance" shall be deemed to include any materials for making any explosive substance; also any apparatus, machine, implement or material used, or intended to be used, or adapted for causing, or aiding in causing, any explosion in or with any explosive substance; also any part of any such apparatus, machine or implement,

(b). the expression "special category explosive substance" shall be

research development explosive (RDX),

Penta erythritol tetra nitrate (PETN),

high melting explosive (HMX),

tri nitro toluene (TNT), etc.

and any other substance, by notification in the Official Gazette, specify or the purposes of this Act.

Stringent Punishments are prescribed under the Act for the unlawful possession of Substance and activities.

### **The Explosive Substances Act,1908:**

**Sec 3 :** Who ever Causes any explosion likely to endanger life or property , whether any injury to person or property has been actually caused or not, be punished with imprisonment for life, or with rigorous imprisonment of either description which shall not be less than ten years, and shall also be liable to fine.

**Sec 4:** Who ever Causes any explosion with special category explosive substance, an explosion of a nature likely to endanger life or to cause serious injury to property shall, whether any injury to person or property has been actually caused or not, be punished with death, or rigorous imprisonment for life, and shall also be liable to fine. [Under this Act the Security of Supply chain can be Guarded with Draconian Punishments.](#)

# *The Ammonium Nitrate Rules, 2012*

## *15. Safety and Security Management Plan.*

- (a) assigned responsibility and organisational structure;*
- (b) hazard identification, risk assessment and control;*
- (c) provision of information, education and training to the work force, contractors and visitors;*
- (d) accident reporting and investigation;.*
- (e) emergency response planning and preparedness such as first aid, testing of emergency plan once in a year;*



- (f) Disaster Management Plan and provision of escape routes, identifying and assessing security risk associated with the activities; evacuation plan, appropriate fire fighting controls;***
- (g) set of process adopted by the holder of the licence to carry out authorized activities and keeping of Ammonium Nitrate secure;***
- (h) maintenance of schedules for plant and equipment;***
- (i) standard operating procedure;***
- (j) competence of personnel for tasks;***
- (k) nature of the surveillance;***

***(3) Every person engaged in the manufacturing factory shall be imparted training in safety and security aspects -----***

A Diplomatic Conference on Maritime Security, held at the London Headquarters of the International Maritime Organization (IMO) from 9 to 13 December 2002 (the 2002 SOLAS Conference), was attended by 109 Contracting Governments to the 1974 SOLAS Convention, observers from two IMO Member States and observers from the two IMO Associate Members.

The 2002 SOLAS Conference adopted a number of Amendments to the International Convention for the **SAFETY OF LIFE AT SEA (SOLAS), 1974**, as amended, the most far-reaching of which enshrined the new **International Ship and Port Facility Security Code (ISPS Code)**.

**CODES RELEVANT T THE SECURITY OF PORTS AND SHIPS:**

Port-related security issues should be addressed in accordance with the ILO/IMO Code of practice, Security Imports (2004), and, as appropriate, with the **IMO'S,ISPS Code, 2003 edition (International Ship and Port Facility Security Code and SOLAS Amendments, 2002)**.

**ISPS (International Ship and Port Facility Security Code ) Code** is an Amendment to the SOLAS Convention on Minimum Security Arrangements for Ships, Ports and Government Agencies.

The Code developed in response to the perceived threats to the ports and ships in the wake of 9/11 attacks of U.S.

The Code is a two part Document on minimum requirements of Security arrangements at the Ports and inside the Ships. Part-A stipulates the mandatory arrangements and part-B stipulates the Implementation Part.

## **Under the ISPS legislation, the Ports are obliged to:**

- Develop and maintain an appropriate Port Facility Security Plan (PFSP), which meets the requirements of the ISPS Code.
  - Designate a Port Facility Security Officer .
  - Co-ordinate, Communicate and facilitate the implementation of Security measures required by the PFSP to the port community as appropriate.
  - Establish a Port Security Committee, comprising representatives of relevant Port facility groups, Regulators, Agencies and other interested parties within the Port.
- 
- Provide up to date advice, best practice and information on current security developments and on the implementation of the Port Facility Security Plans (PFSP) to the port community.
  - Co-ordinate and facilitate security training and testing of the PFSP and where necessary co-ordinate the overall port response to a security incident.
  - Ensure the effective management and resourcing of internal security arrangements in order to meet the requirements of the Port PFSP. Review this security policy and recommend revisions to the Board at least every 3 years.
  - Which are in concurrence with the ISO 28000 Standard.

FACTORIES ACT ,1948 AND AMENDED  
ACT,1987 AND TS FACTORIES RULES.  
Related to Security.

**The Factories Act ,1948 and the Amended Act,1987 &  
The Telangana State Factories Rues made there Under :**

**Under Sec 7-A(3) and Sec 41B(2) and Sec 112 and Rule 61(SB)A :  
HEALTH AND SAFETY POLICY:**

**Clause (5)(c) : Fixing the Responsibilities of the Contractors, Sub-  
Contractors, transporters and Other Agencies entering the  
premises- Under this clause an Agreement can be made with the  
Supply Chain Agencies for plugging the Security Vulnerabilities,**

**Clause (f): Integrating the H & S Policy decisions including those  
are dealing with the Purchase of RAW Materials –Under this Clause  
the Security Vulnerabilities in the Supply Chain of the mfg. facilities  
affecting the Health and Safety of the Persons shall be discussed as  
a Part of the Security Plan,**

**Clause (s) :** Arrangements for Informing, Educating, Training and also to the Public Concerned. -----Under this Clause the Security vulnerabilities can be Publicised for Planning & Preparing the Concerned and to this extent an Agreement can be made with the Supply Chain Agencies.

**Clause (8)(b):**Whenever any New Substances or Articles are Introduced in the mfg. Process ,the Policy shall be Reviewed. Under this Clause the Supply Chain Contract Agreement can be Reviewed the Security Vulnerabilities due to the Supply of the New Substances & Articles.

Even though the Indian Factories Act, is Regulating the Working Conditions , by the introduction of the **Sec 2 (cb) Hazardous Process** due to the Amended Act,1987, the Hazardous Process Provisions are taking care of the Supply Chain Raw Materials ,Intermediates, Finished Products, Bye-Products , Hazardous Waste & Effluents and thereby guarding the Persons Connected and the Environment there in, related to the Factories.-----  
----So SCM Agreements can be Made.

**RULE 129. TRANSPORTATION OF GOODS OF DANGEROUS OR HAZARDOUS NATURE TO HUMAN LIFE.(CMV RULES 1989).**

Every owner of a goods carriage transporting any dangerous or hazardous goods shall,

- (a). Shall display a distinct mark of the class label appropriate to the type of dangerous or hazardous goods as specified ;
- (b). Shall be equipped with safety equipment for preventing fire, explosion or escape of hazardous or dangerous goods;
- (c) .Shall be fitted with Tachograph (an instrument to record the lapse of running time of the motor vehicle; time speed maintained, acceleration, deceleration, etc.) conforming to the specifications of the Bureau of Indian Standards;
- (d). Shall be fitted with a spark arrester.



Rule 131. Responsibility of the consignor for safe transport of dangerous or hazardous Goods.

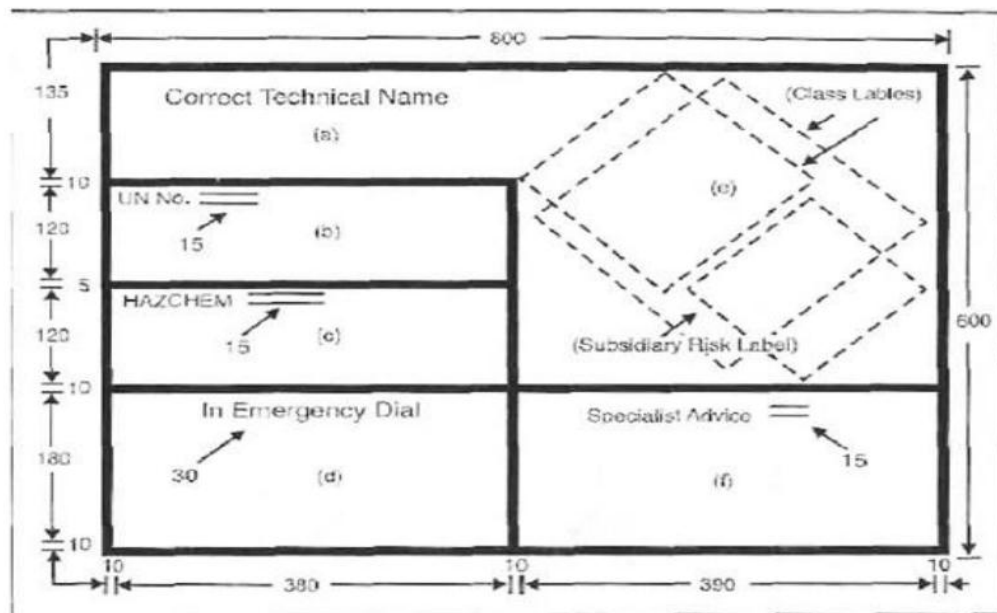
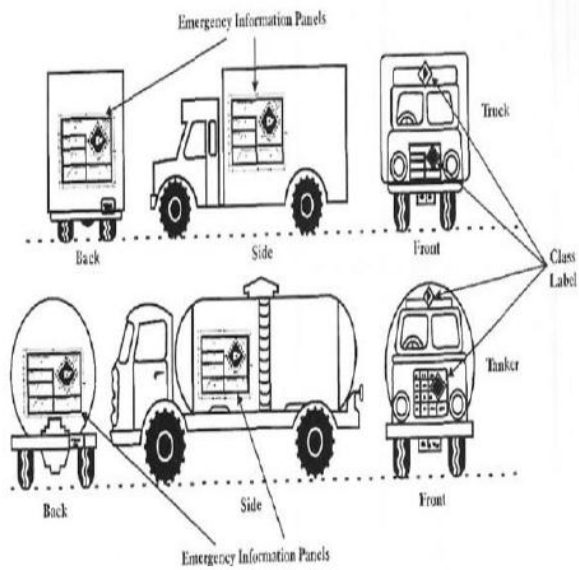
1) It shall be the responsibility of the consignor intending to transport any dangerous or hazardous goods listed in Table III, to ensure the following, namely:—

- (a) the goods carriage has a valid registration to carry the said goods;
- (b) the vehicle is equipped with necessary first-aid, safety equipment and antidotes as may be necessary to contain any accident;
- (c) that the transporter or the owner of the goods carriage has full and adequate information about the dangerous or hazardous goods being transported; and
- (d) that the driver of the goods carriage is trained in handling the dangers posed during transport of such goods.

RULE 133. RESPONSIBILITY OF THE DRIVER

(1) The driver of a goods carriage transporting dangerous or hazardous goods shall ensure that the information given to him in writing is kept in the driver's cabin and is available at all time while the dangerous or hazardous goods to which it relates, are being transported.

(2) Every driver of a goods carriage transporting any dangerous or hazardous goods shall observe at all times all the directions necessary for preventing fire, explosion or escape of dangerous or hazardous goods carried by him while the goods carriage is in motion, and when it is not being driven he shall ensure that the goods carriage is parked in a place which is safe from fire, explosion and any other risk, and at all times the vehicle remains under the control and supervision of the driver or some other competent person above the age of 18 years.]



- **Action plan is similar to an industrial installation.**  
ACTION PLAN FOR TRANSPORT ACCIDENT:
- **The person to inform the emergency is Driver of the vehicle/cleaner of the vehicle if they are safe.**
- **Otherwise any passerby will inform the emergency to the Emergency Control Center. The information flow thereafter is similar to the above.**
- **Possibility of affected region is lesser than in case of industrial installation but the nature of accident scenario being dynamic and sometimes occurs in the area where there is more population; control of the situation may become critical.**
- **Here the important role players are the first responders ie police, fire and medical authorities.**
- **Control of traffic, neutralizing the chemical or combating the fire**

### **The Hazardous Waste (Management ,Handling Transboundary Movement) Rules , 2008.**

**Rule 2(1):** Hazardous Waste means waste by reason of its Physical, Chemical, Reactive, Toxic, Flammable, Corrosive causes Danger or Likely to Cause DANGER TO Health, Environment ,when in alone or when in Contact with Other Substances , as specified WASTE in the Sch I,II,III,

**Rule 2(m):** Hazardous Waste Site means a place of Collection, Reception, Treatment ,Storage of Hazardous Waste and its Disposal to the Environment , as approved by the Competent Authority,

**Rule(4):**The Occupier shall be responsible for Safe and Environment friendly manner of handling Hazardous Waste that which is generated in his Establishment, The Occupier shall be Transported the generated Waste to any authorised re-cycler , Re-user,Re-Processor in accordance with the Rules,

**Rule (5):** The Occupier Shall Take adequate Steps while Handling the Hazardous Waste to Prevent Accidents, limit its Consequences on Humanbeings,and Environment.

**Chapter IV ,Rule 13 :**

Deals with the Import and Export of Hazardous Waste:

No Import Hazardous Waste from any Country for Disposal is Permitted except for Recycling, Re-use and for Re-Processing,

The Export of Hazardous Waste from India is Permitted by following the Prior Informed Consent Procedure of the Importing Country for having Sound Management of the Hazardous Waste,

No Import/Export of Hazardous Waste as specified in the Sch VI is permitted,

**Rule 20 :** The Packaging and Labelling and Transportation of the Hazardous Waste, shall be in accordance with the Central Motor Vehicles Act,1989 issued Guide Lines from Time to Time.

# **The E.P Act,1986:**

**Under The E.P Act,1986:**

**(e) "hazardous substance"** means any substance or preparation which, by reason of its chemical or physio-chemical properties or handling, is liable to cause harm to human beings, other living creatures, plants, micro-organism, property or the environment;

## The Public Liability Insurance Act, 1991.



## The Public Liability Insurance Act, 1991.

- Liability to give Relief under the Principle of No Fault.
- Where death or injury to any person (other than a workman) or damage to any property has resulted from an accident, the owner shall be liable to give such relief as is specified in the Schedule for such death, injury or damage
- Every owner shall take out, before he starts handling any hazardous substance, one or more insurance policies providing for contracts of insurance whereby he is insured against liability to give relief
- No application for relief shall be entertained unless it is made within five years of the occurrence of the accident .

## Chemical Accidents(Emergency Planning, Preparedness and Response) Rules,1996 and Amendment Rules,2015.

**Rule (2)(a):** Chemical Accident Means an Accident involving, while handling any Hazardous Chemical ,resulted in the Death, Injury or Damage to Property.

Hazardous Chemical: Any Criteria laid down in Part-I of Sch-I or as Listed in the Schedules -2 & 3, Any of listed 431 Hazardous Chemicals as listed in Part-II of Schd-2.

**Rule (2)(f) :** Major Chem Accident means an Occurrence of Major emission, Fire or Explosion involving Hazd Chem Transportation or due to the Natural event likely to cause substantial loss of Life, Property and also adverse effects on the Environment.

Supply Chain Definition can be extended to Pipe Line Mode of Transfer of Hazard Chem.

**Rule-4:**Constitutin of Crisis Alert System including Control Room, Info Networking, Communication, Creating Awareness to the Pubic.

**Rule 13:** Info to Public related to Chem Accident Prevention, Preparedness, Mitigation in the en-route of Transportation.

## Crisis Groups



- Formed under Chemical Accidents (Emergency Preparedness and Response) Rules 1996
- To deal with the emergencies arising out of chemical accidents.
- Central Crisis Group
- State Crisis Group
- District Crisis Group
- Local Crisis Group

## The Disaster Management Act, 2005 :

The Act comprises 79 sections and 11 chapters ,

- **Sec 2(d):** Defines Disaster means a Catastrophe, mishap, Calamity or grave Occurrence in any area arising from a Natural or manmade or by accident or Negligence which results in substantial loss of Life or Human Sufferings or Damage to and destruction of Property or degradation of Environment and is of such a nature of magnitude, is of beyond the coping capacity of the Community.

and Disaster management in its new concept

- It provides institutional mechanism for monitoring and implementation of plans
- Ensures measures by various wings of the Government for the prevention and mitigation of disasters

### **SALIENT FEATURES:**

The Act provides for a National Disaster Management Authority (NDMA), The State governments shall create State Disaster Management Authorities and District Disaster Management Authorities, There shall be a Disaster Response Fund and Disaster Mitigation Fund at National, State and District levels.

**NATIONAL DISASTER MANAGEMENT AUTHORITY (NDMA)** • National Disaster Management Authority (NDMA) under the Prime Minister with nine more members for laying down the policies, plans and guidelines for disaster management.

The Authority will be assisted by a **National Executive Committee (NEC)** of Secretaries to Central Government.

### **NATIONAL DISASTER RESPONSE FORCE (NDRF)**

The Section 44-45 of the Act provides for constituting a National Disaster Response Force "for the purpose of specialist response to a threatening disaster situation or disaster" under a Director General to be appointed by the Central Government.

### **Supply Chain Security Vulnerabilities Due to Cyber Attacks and Terrorism: The Information Technology Act, 2000**

**Sec 2(nb):** Cyber Security means protecting Information, equipment Devices, Computer, Communication device, and information Stored there in ,unauthorised access, use, disclosure, disruption , modification or disruption;

**Sec 2(ua):** Indian Computer Emergency Response Team ,as established under Sub-Section 70B; serves as a Nodal Agency to perform in the area of Cyber Security viz. Forecast and alert of Cyber Security Incidents, Emergency Measures for handling during the Threat and issue of advisory Guidelines during the Threat.,

**Sec 66 F :Defines Cyber Terrorism:** Whoever with an intent to threaten the Integrity , Security, Sovereignty of India or Strike Terror in the People, by denying access to the authorised Computer Resources, Causing Computer Contaminant, without authorisation accessing the computer Resources are Punishable under the Act.

**Conclusions :** STATUTORY REQUIREMENTS AND CERTAIN STANDARDS FOR GUARDING THE SUPPLY CHAIN SECURITY VULNERABILITIES:

ISO 28000 STANDARD, CONTAINER STANDARD, RFID,

SECURITY VULNERABILITIES RELATED TO THE GOVT ESTABLISHMENTS,

Explosives , Hazardous Process, Hazardous Substances, F.ACT, MSIHC Rules.

PLI Act , Hazd Waste Management and Handling , Transboundary Rules,

Types of Explosives, NH<sub>4</sub>NO<sub>3</sub> Ware House SECURITY PLAN,

Storage Container Design, Insurance, Labelling Significance, Training of the Employees, Transportation Risks, Disasters Containment and Off-site Plan , NDMA , Cyber Attacks , Crisis Groups.

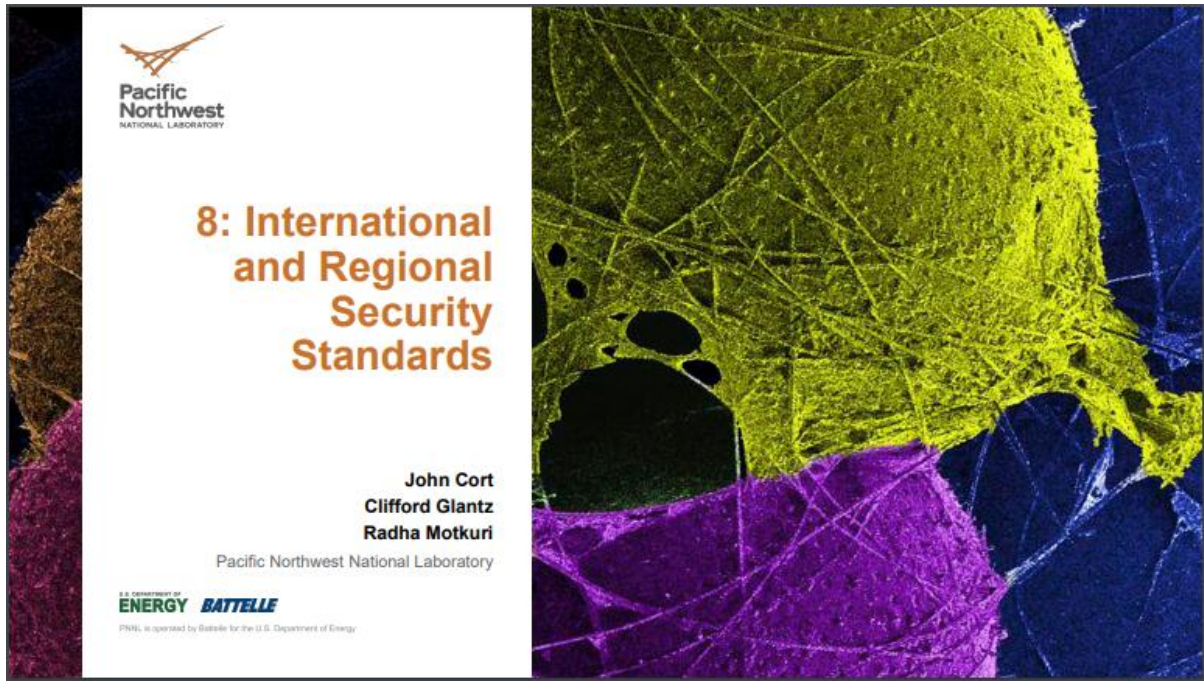
***THANKS***

*Your experiences can be shared at*

*[velloresasikumar39@gmail.com](mailto:velloresasikumar39@gmail.com)*



Dr. John Cort







## CFATS: Chemical Facility Anti-Terrorism Standards

- CFATS is a regulatory program (6 CFR Part 27) established by the U.S. Department of Homeland Security in 2007 to address chemical security by identifying and regulating high-risk facilities that possess certain chemicals of interest (COI) at specific concentrations and quantities.
- The CFATS regulation applies to facilities across many industries, including:
  - Chemical manufacturing, storage, and distribution
  - Energy and utilities
  - Agriculture and food
  - Explosives
  - Mining
  - Electronics
  - Plastics
  - Universities and laboratories
  - Paint and coatings
  - Healthcare and pharmaceuticals

3



## CFATS: Chemical Facility Anti-Terrorism Standards

- CFATS is a regulatory program (6 CFR Part 27) established by the U.S. Department of Homeland Security in 2007 to address chemical security by identifying and regulating high-risk facilities that possess certain chemicals of interest (COI) at specific concentrations and quantities.
- The CFATS regulation applies to facilities across many industries, including:
  - Chemical manufacturing, storage, and distribution
  - Energy and utilities
  - Agriculture and food
  - Explosives
  - Mining
  - Electronics
  - Plastics
  - Universities and laboratories
  - Paint and coatings
  - Healthcare and pharmaceuticals

3

Chemicals of Interest (COI)	Synonym	Chemical Abstract Service (CAS) #	Release: Minimum Concentration (%)	Release: Screening Threshold Quantities (in pounds)	Theft: Minimum Concentration (%)	Theft: Screening Threshold Quantities (in pounds unless otherwise noted)	Sabotage: Minimum Concentration (%)	Sabotage: Screening Threshold Quantities	Security Issue: Release - Toxic	Security Issue: Release - Flammable	Security Issue: Release - Explosive	Security Issue: Theft - CWICWP	Security Issue: Theft - WME	Security Issue: Theft - EXP/IEDP	Security Issue: Sabotage/Contamination
Cyclopropane		75-19-4	1.00	10,000						X					
DF	Methyl phosphoryl difluoride	676-99-3				CUM 100g						X			
Diazodinitrophenol		87-31-0	ACG	5,000	ACG	400					X			X	
Diborane		19287-45-7	1.00	2,500	2.67	15			X					X	
Dichlorosilane	[Silane, dichloro-]	4109-96-0	1.00	10,000	10.47	45				X				X	
N,N-(2-diethylamino)ethanethiol		100-38-9			30.00	2.2						X			
Diethyldichlorosilane		1719-53-5					ACG	APA							X
o,o-Diethyl S-[2-(diethylamino)ethyl] phosphorothioate		78-53-5			30.00	2.2						X			
Diethyleneglycol dinitrate		693-21-0	ACG	5,000	ACG	400				X				X	
Diethyl methylphosphonite		15715-41-0			30.00	2.2						X			
N,N-Diethyl phosphoramidic dichloride		1496-54-0			30.00	2.2						X			
N,N-(2-dileopropylamino)ethanethiol	N, N-dileopropyl-(beta)-aminoethane thiol	5842-07-9			30.00	2.2						X			
Difluoroethane	[Ethane, 1-1difluoro-]	75-37-6	1.00	10,000						X					
N,N-Diisopropyl phosphoramidic dichloride		23306-80-1			30.00	2.2						X			
1,1-Dimethylhydrazine	[Hydrazine, 1, 1-dimethyl]	57-14-7	1.00	10,000						X					
Dimethylamine	[Methanamine, N-methyl-]	124-40-3	1.00	10,000						X					
N,N-(2-dimethylamino)ethanethiol		108-02-1			30.00	2.2						X			
Dimethyldichlorosilane	[Silane, dichlorodimethyl-]	75-78-5	1.00	10,000			ACG	APA		X					X
N,N-Dimethyl phosphoramidic dichloride	[Dimethylphosphoramido-dichloridate]	677-43-0			30.00	2.2						X			
2,2-Dimethylpropane	[Propane, 2,2-dimethyl-]	463-82-1	1.00	10,000						X					

## CFATS: Chemical Facility Anti-Terrorism Standards

- Chemical security is not a temporary issue. As threats evolve, the Department is committed to working with stakeholders to protect the Nation's highest-risk chemical infrastructure.

## ISO/PAS 28000:2007

- ISO/PAS 28000:2007, Specification for security management systems for the supply chain
- Specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. Security management is linked to many other aspects of business management. Aspects include all activities controlled or influenced by organizations that impact on supply chain security. These other aspects should be considered directly, where and when they have an impact on security management, including transporting these goods along the supply chain.

## ISO/PAS 28000:2007

- ISO 28000:2007 is applicable to all sizes of organizations, from small to multinational, in manufacturing, service, storage or transportation at any stage of the production or supply chain that wishes to:
  - a) establish, implement, maintain and improve a security management system;
  - b) assure conformance with stated security management policy;
  - c) demonstrate such conformance to others;
  - d) seek certification/registration of its security management system by an accredited third party Certification Body; or
  - e) make a self-determination and self-declaration of conformance with ISO 28000:2007.
- There are legislative and regulatory codes that address some of the requirements in ISO 28000:2007.
- The ISO standard must be purchased (88 Swiss Francs)



## ISO/PAS 28000:2007

- How widespread is adoption of ISO 28000:2007, in US and abroad
- What does adoption and compliance with this standard look like in the real world

9



## Containerized intermodal shipping

- The Container Security Initiative (CSI)
- The Global Container Control Programme (CCP)
- The International Ship and Port Facility Security Code (ISPS Code)

10



## Standards for Smaller Scale Production and Fine Chemicals

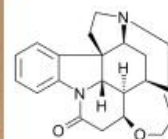
- The challenge of custom synthesis
- Disperse market with many participants
- Crossover with botanical extracts / traditional medicine
  - Example: strychnine production in India



*Strychnos nux-vomica*



credit: Smithsonian Tropical Research Institute



- *Input / discussion with participants*

11



## Global Chemical Security Summits

- Are new standards needed
- Are new regional or international organizations needed
- What are the major gaps that need to be filled to increase chemical security, and are standards (*versus* regulations, etc.) the best way to achieve this
- International vs. regional cooperation and organization

12



Dr. Clifford Glantz



Session 9:  
Assessing Security

Cliff Glantz, John Cort, and Radha K Motkuri  
Pacific Northwest National Laboratory (PNNL)  
Richland, WA, 99352  
USA



PNNL is operated by Battelle for the U.S. Department of Energy



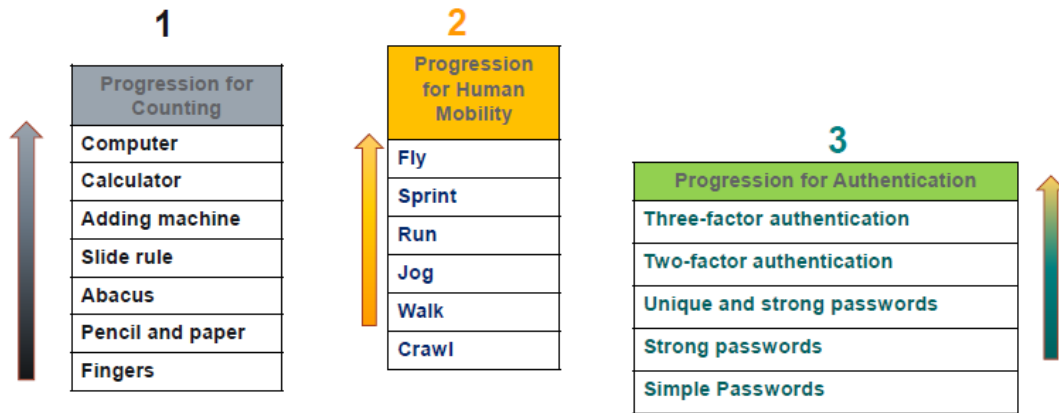
The Approach: Maturity Model

Maturity Model

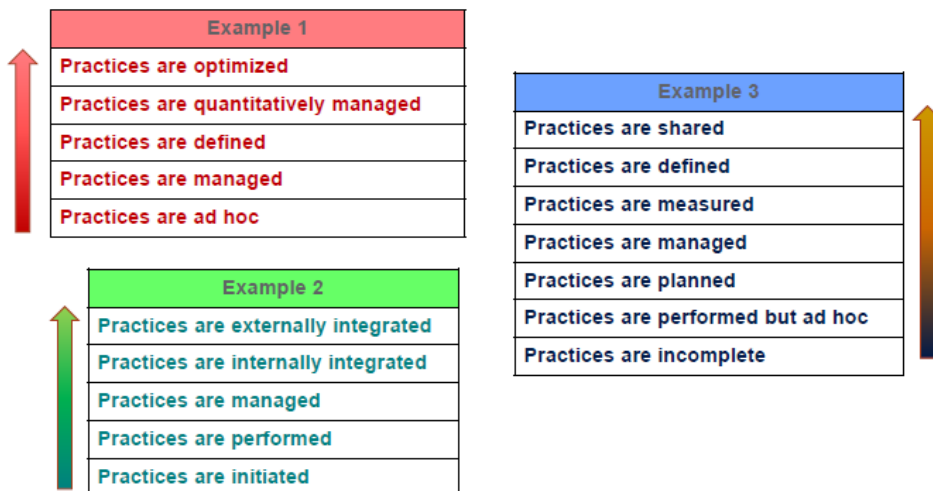
- An organized way to convey a path of experience, wisdom, perfection, or acculturation.
- The subject of a maturity model can be an object or things, ways of doing something, characteristics of practices or processes.



## Progression Model: Three Simple Examples



## Capability Maturity Model: Three Examples of Increasing Maturity



# Organization of a Maturity Model



## Example Set of 10 Supply Chain Security Domains

RM Risk Management	AM Access Management	CV Customer Vetting	VSV Vetting of Suppliers and Vendors
SPR Security Policies, Roles, and Responsibilities	ISC Information Sharing and Communications	IRR Incident Response and Reporting	TM Transportation Management
WM Workforce Management	ICT Inventory and Information Control and Tracking		



## Maturity Indicator Level Descriptions

Level	Name	Description
MIL0	Not Performed	<ul style="list-style-type: none"><li>• MIL1 has not been achieved in the domain</li></ul>
MIL1	Initiated	<ul style="list-style-type: none"><li>• Initial practices are performed, but may be ad hoc</li></ul>
MIL2	Performed	<ul style="list-style-type: none"><li>• Practices are documented</li><li>• Stakeholders are involved</li><li>• Adequate resources are provided for the practices</li><li>• Standards or guidelines used to guide implementation</li><li>• Practices are more complete or advanced than at MIL1</li></ul>
MIL3	Managed	<ul style="list-style-type: none"><li>• Domain activities are guided by policy (or other directives)</li><li>• Activities periodically reviewed for conformance to policy</li><li>• Responsibility and authority for practices are clearly assigned to personnel with adequate skills and knowledge</li><li>• Practices are more complete or advanced than at MIL2</li></ul>

7



## Special Note about MIL1 Practices

- By design, MIL1 practices may be implemented in an ad hoc manner and still be considered “Fully Implemented”
- Ad hoc means
  - Practice performance may depend on initiative and experience of an individual or team, without much organizational guidance (policy and/or procedures)
  - Methods, tools, techniques, priority, and quality may vary significantly depending on who is performing the practice or when it is performed
  - Lessons learned may not be captured and outcomes may be difficult to repeat
- Even if ad hoc, the practice needs to meet business and critical infrastructure objectives to be “Fully Implemented”

8



## Scoring Each Practice

### 4-point answer scale

The organization's performance of the practice described in the model is ...

Fully implemented	Complete
Largely implemented	Complete, but with a recognized opportunity for improvement
Partially implemented	Incomplete; there are multiple opportunities for improvement
Not implemented	Absent; the practice is not performed in the organization

9

## Using Practice Scores

- To achieve a Maturity Indicator Level for a domain, all the practices in that domain for that level (and all lower levels) must have a performance score of fully or largely implemented.
- A single partially or not implement score for a single practice will keep a Level from being achieved.

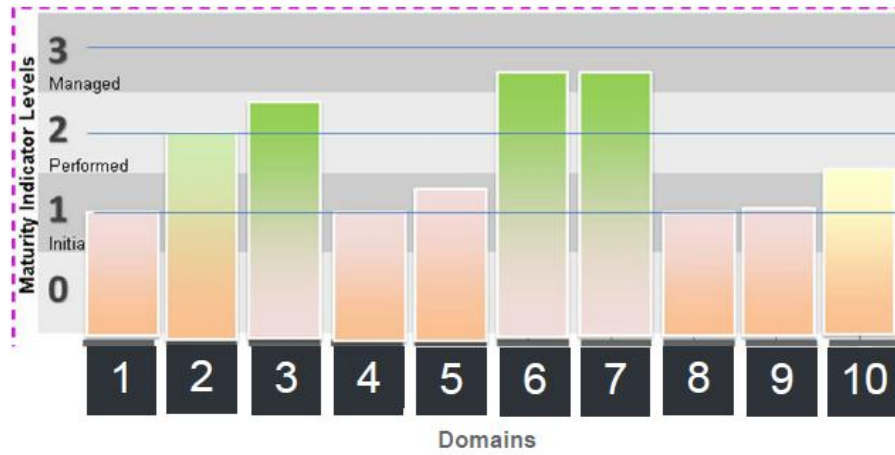
	Practice 1	Practice 2	Practice 3	Practice 4	Practice 5	Practice 6	MIL 1 Achieved?	
Utility A	LI	FI	FI	FI	FI	FI	Yes	All Practices are either FI or LI
Utility B	FI	PI	FI	LI	LI	FI	No	One PI = MIL <u>Not</u> Achieved
Utility C	FI	FI	PI	FI	LI	FI	No	One PI = MIL <u>Not</u> Achieved
Utility D	FI	FI	FI	PI	FI	NI	No	One PI and one NI = MIL <u>Not</u> Achieved
Utility E	FI	FI	LI	LI	PI	PI	No	Two PIs = MIL <u>Not</u> Achieved

10





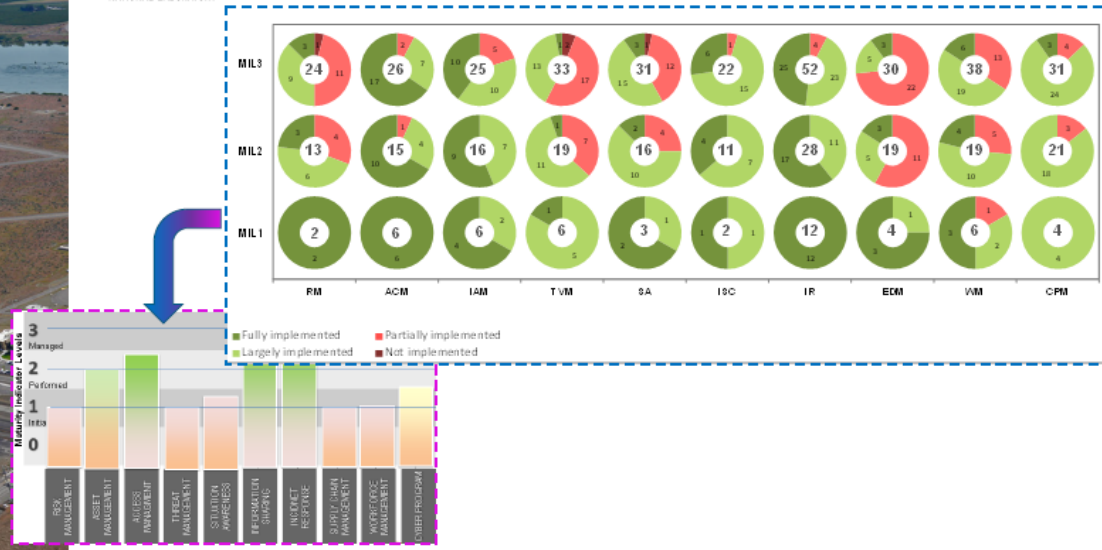
## How Can Results be Visualized? Here is One Simple Approach...



## Comparison of Two Results...

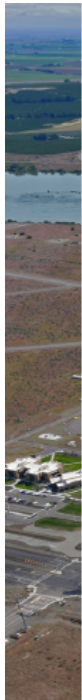


## A More Detailed Presentation of Results



## C-TPAT One Method of Assessing Security Risks

- The **Customs-Trade Partnership Against Terrorism (C-TPAT)** is a voluntary supply-chain security program led by U.S. Customs and Border Protection (CBP) focused on improving the security of private companies' supply chains with respect to terrorism. <https://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat>
- Involves documenting a company's process for determining and alleviating security risks throughout their international supply chain.
- In the US, companies with C-TPAT certification are classified as "low risk" and enjoy fewer customs inspections and enjoy priority in the processing of their shipments.
- There are over 11,400 certified C-TPAT partners



## 5 Steps in the C-TPAT

1. Identifying Business Partners (directly or indirectly contracted) and Mapping Material Transport
2. Conduct a Threat Assessment
3. Conduct a Vulnerability Assessment
4. Prepare an Action Plan
5. Document How Risk Assessments are Conducted



15



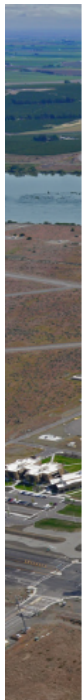
## Identifying Business Partners and Mapping Material Transport

Information gathering -- Identify ALL parties involved in the following processes:

- 1) Procurement
- 2) Production
- 3) Packing
- 4) Storage
- 5) Loading/Unloading
- 6) Transportation
- 7) Document Preparation



16



## Conduct a Threat Assessment

- Assign a threat risk rating based on the following.
  - 1 - **Low Risk** – No recent incidents/intelligence/information
  - 2 - **Medium Risk** – No recent incidents/some intelligence/information on possible activity
  - 3 - **High Risk** – Recent incidents and intelligence/information
- A Score of 3 in any of the following areas would deem the supply chain “**High Risk**”:
  - 1) Terrorism
  - 2) Contraband Smuggling
  - 3) Human Smuggling
  - 4) Organized Crime

17



## Conduct a Vulnerability Assessment

For all business partners in the supply chain (directly contracted or sub-contracted):

- 1) Identify the process they perform
- 2) Verify partners meet applicable minimum security criteria
- 3) Rate their compliance within each applicable minimum-security criteria category (**High**, **Medium**, **Low**)



18





## Prepare an Action Plan and Document How Risk Assessments are Conducted

- Establish a corrective action plan to address gaps or vulnerabilities found in business partner's security programs.
- Document the company's approach, policies, and procedures for conducting an international supply chain security risk assessment



19



Thank you



20



Dr. Radha Kishan Motkuri



## Exercise E – Security Program Maturity Modeling

Radha Kishan Motkuri, Cliff Glantz, and John Cort  
Pacific Northwest National Laboratory (PNNL)  
Richland, WA, 99352  
USA



PNNL is operated by Battelle for the U.S. Department of Energy



## Instructions

In the previous exercise you have:

- identified an array of attack scenarios involving threat agents mounting attacks on Plant Alpha.
- Identified preliminary physical, cyber, and personnel security enhancements Plant Alpha might implement to reduce or eliminate those attack pathways.
- Identified specific security vulnerabilities in the Plant Alpha supply chain and chemical lifecycle.
- Identified specific supply chain security best practices that could be applied at Plant Alpha

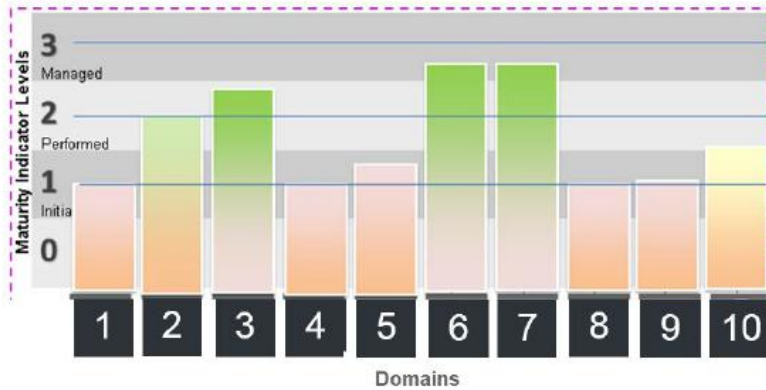


v

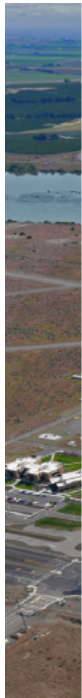


## In this Exercise...

- You will apply a simple maturity model to Plant Alpha to evaluate the maturity of its supply chain security program.



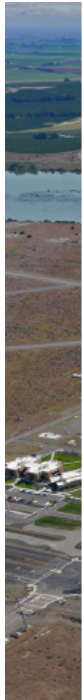
3



## Areas to Consider

- Plant Alpha's Infrastructure: Design, Construction, Testing, and Maintenance
- Business Network Security
- ICS Network Security
- Physical Security
- Personnel Security
- Acquisition of Materials for Manufacture
- Processing/Manufacture/Storage of Chemicals
- Sale of Products to Customers
- Transport and Delivery of Products
- Waste Management

4



## Focus on the Following Supply Chain Maturity Model Domains

- 1. Risk Management**
2. Security Policies, Roles, and Responsibilities
3. Inventory and Information Control and Tracking
- 4. Access Management**
5. Vetting of Suppliers and Vendors
6. Customer Vetting
7. Transportation Management
- 8. Workforce Management**
9. Information Sharing
10. Incident Response and Reporting

5



## Instructions

- Reform into groups.
- Go through the maturity model and identify the maturity of security in each of the three sample domains.
- Choose a representative to present your proposed security enhancements this to the class.



6





## Present Results



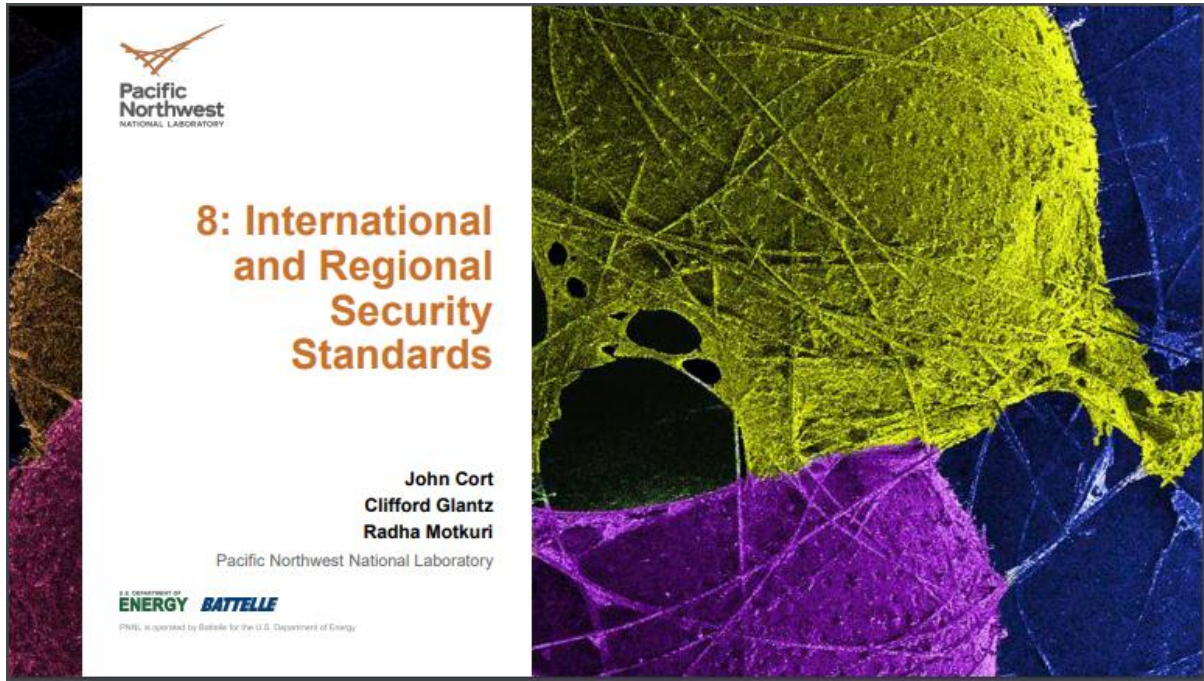
v



## Thank you



Dr. Clifford Glantz



## International and Regional Security Standards

- Outline
  - Different types of risks with a range of probabilities and consequences
  - CFATS
  - ISO/PAS 28000:2007 (Specification for security management systems for the supply chain)
  - The Container Security Initiative (CSI)
  - The Global Container Control Programme (CCP)
  - The International Ship and Port Facility Security Code (ISPS Code)
  - Standards for Smaller Scale and Fine Chemicals
  - Global Chemical Security Summits

2





## CFATS: Chemical Facility Anti-Terrorism Standards

- CFATS is a regulatory program (6 CFR Part 27) established by the U.S. Department of Homeland Security in 2007 to address chemical security by identifying and regulating high-risk facilities that possess certain chemicals of interest (COI) at specific concentrations and quantities.
- The CFATS regulation applies to facilities across many industries, including:
  - Chemical manufacturing, storage, and distribution
  - Energy and utilities
  - Agriculture and food
  - Explosives
  - Mining
  - Electronics
  - Plastics
  - Universities and laboratories
  - Paint and coatings
  - Healthcare and pharmaceuticals

3



## CFATS: Chemical Facility Anti-Terrorism Standards

- CFATS is a regulatory program (6 CFR Part 27) established by the U.S. Department of Homeland Security in 2007 to address chemical security by identifying and regulating high-risk facilities that possess certain chemicals of interest (COI) at specific concentrations and quantities.
- The CFATS regulation applies to facilities across many industries, including:
  - Chemical manufacturing, storage, and distribution
  - Energy and utilities
  - Agriculture and food
  - Explosives
  - Mining
  - Electronics
  - Plastics
  - Universities and laboratories
  - Paint and coatings
  - Healthcare and pharmaceuticals

3

Chemicals of Interest (COI)	Synonym	Chemical Abstract Service (CAS) #	Release: Minimum Concentration (%)	Release: Screening Threshold Quantities (in pounds)	Theft: Minimum Concentration (%)	Theft: Screening Threshold Quantities (in pounds unless otherwise noted)	Sabotage: Minimum Concentration (%)	Sabotage: Screening Threshold Quantities	Security Issue: Release - Toxic	Security Issue: Release - Flammable	Security Issue: Release - Explosives	Security Issue: Theft - CWICWP	Security Issue: Theft - WME	Security Issue: Theft - EXP/IEDP	Security Issue: Sabotage/Contamination
Cyclopropane		75-19-4	1.00	10,000						X					
DF	Methyl phosphonyl difluoride	676-99-3				CUM 100g					X				
Diazodinitrophenol		87-31-0	ACG	5,000	ACG	400				X				X	
Diborane		19287-45-7	1.00	2,500	2.67	15			X				X		
Dichlorosilane	[Silane, dichloro-]	4109-96-0	1.00	10,000	10.47	45			X				X		
N,N-(2-diethylamino)ethanethiol		100-38-9			30.00	2.2					X				
Diethylchlorosilane		1719-53-5					ACG	APA							X
o,o-Diethyl S-[2-(diethylamino)ethyl] phosphorothioate		78-53-5			30.00	2.2					X				
Diethyleneglycol dinitrate		693-21-0	ACG	5,000	ACG	400				X				X	
Diethyl methylphosphonite		15715-41-0			30.00	2.2					X				
N,N-Diethyl phosphoramidic dichloride		1499-54-0			30.00	2.2					X				
N,N-(2-diisopropylamino)ethanethiol	N, N-diisopropyl-(beta)-aminoethane thiol	5842-07-9			30.00	2.2					X				
Difluoroethane	[Ethane, 1-1difluoro-]	75-37-6	1.00	10,000					X						
N,N-Diisopropyl phosphoramidic dichloride		23306-80-1			30.00	2.2					X				
1,1-Dimethylhydrazine	[Hydrazine, 1, 1-dimethyl]	57-14-7	1.00	10,000						X					
Dimethylamine	[Methanamine, N-methyl-]	124-40-3	1.00	10,000						X					
N,N-(2-dimethylamino)ethanethiol		108-02-1			30.00	2.2					X				
Dimethylchlorosilane	[Silane, dichlorodimethyl-]	75-78-5	1.00	10,000			ACG	APA		X					X
N,N-Dimethyl phosphoramidic dichloride	[Dimethylphosphoramido-dichloridate]	677-43-0			30.00	2.2					X				
2,2-Dimethylpropane	[Propane, 2,2-dimethyl-]	463-82-1	1.00	10,000					X						

## CFATS: Chemical Facility Anti-Terrorism Standards

- Chemical security is not a temporary issue. As threats evolve, the Department is committed to working with stakeholders to protect the Nation's highest-risk chemical infrastructure.

## ISO/PAS 28000:2007

- ISO/PAS 28000:2007, Specification for security management systems for the supply chain
- Specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. Security management is linked to many other aspects of business management. Aspects include all activities controlled or influenced by organizations that impact on supply chain security. These other aspects should be considered directly, where and when they have an impact on security management, including transporting these goods along the supply chain.

## ISO/PAS 28000:2007

- ISO 28000:2007 is applicable to all sizes of organizations, from small to multinational, in manufacturing, service, storage or transportation at any stage of the production or supply chain that wishes to:
  - a) establish, implement, maintain and improve a security management system;
  - b) assure conformance with stated security management policy;
  - c) demonstrate such conformance to others;
  - d) seek certification/registration of its security management system by an accredited third party Certification Body; or
  - e) make a self-determination and self-declaration of conformance with ISO 28000:2007.
- There are legislative and regulatory codes that address some of the requirements in ISO 28000:2007.
- The ISO standard must be purchased (88 Swiss Francs)



## ISO/PAS 28000:2007

- How widespread is adoption of ISO 28000:2007, in US and abroad
- What does adoption and compliance with this standard look like in the real world

9



## Containerized intermodal shipping

- The Container Security Initiative (CSI)
- The Global Container Control Programme (CCP)
- The International Ship and Port Facility Security Code (ISPS Code)

10

## Standards for Smaller Scale Production and Fine Chemicals

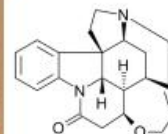
- The challenge of custom synthesis
- Disperse market with many participants
- Crossover with botanical extracts / traditional medicine
  - Example: strychnine production in India



*Strychnos nux-vomica*



credit: Smithsonian Tropical Research Institute



- *Input / discussion with participants*

11

## Global Chemical Security Summits

- Are new standards needed
- Are new regional or international organizations needed
- What are the major gaps that need to be filled to increase chemical security, and are standards (*versus* regulations, etc.) the best way to achieve this
- International vs. regional cooperation and organization

12



Dr. Radha Kishan Motkuri



## Exercise F – Making Informed Risk Management Decisions

Radha Kishan Motkuri, Cliff Glantz, and John Cort  
Pacific Northwest National Laboratory (PNNL)  
Richland, WA, 99352  
USA



PNNL is operated by Battelle for the U.S. Department of Energy



## Instructions

In the previous exercise you have:

- identified an array of attack scenarios involving threat agents mounting attacks on Plant Alpha.
- Identified preliminary physical, cyber, and personnel security enhancements Plant Alpha might implement to reduce or eliminate those attack pathways.
- Identified specific security vulnerabilities in the Plant Alpha supply chain and chemical lifecycle.
- Identified specific supply chain security best practices that could be applied at Plant Alpha
- Conducted maturity modeling of the Plant Alpha Security program





## In this Exercise...

- You will make programmatic choices on security enhancements based on risk reduction and cost.
- You will be given two different budgets (50 and 100 lakhs) to improve your security program
- From the list of available options, choose the set of security enhancements that will provide the most value under each budget.
- Document why you made your choices.

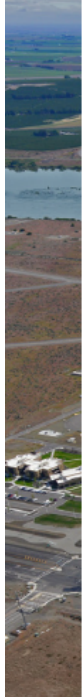


3



## Available Security Options and Costs

1. Document physical and cyber security requirements – including assigning roles and responsibilities. **10 lakhs**
2. Install two-factor authentication for remote access to Plant Alpha business and Control Systems **15 lakhs**
3. Require all system upgrades by vendors be performed on site (no remote access) **10 lakhs**
4. Disable direct connections to the control system network from the business network. **10 lakhs**
5. Do not buy hardware or software from countries that have strained relations with Ruritania **10 lakhs**
6. Increase staff security training and awareness programs **10 lakhs**
7. Require all staff and contractors with unescorted access to the plant to have up-to-date security background checks **15 lakhs**
8. Conduct security exercises **10 lakhs**

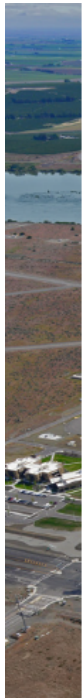


## Available Security Options and Costs (cont)

1. Add an extra security guard per shift **10 lakhs**
2. Install an enhanced security camera and alarms on the plant fenceline **15 lakhs**
3. Forge closer ties to the local law enforcement **1 lakh**
4. Place GPS tracking devices on trucks delivering products to customers **15 lakhs**
5. Increase customer vetting via call-backs for order verification, confirming delivery addresses as valid, requesting the rationale for ordering "risky" chemicals. **2 lakhs**
6. Conduct spot checks to verify the appropriate disposition of hazardous chemicals by customers **3 lakhs**
7. Include security provisions in contracts for the procurement of ICS **4 lakhs**
8. Have an independent contractor perform physical and cybersecurity assessments at Plant Alpha once every two years. **10 lakhs**

5

v



## Instructions

- Reform into groups.
- Assuming a budget of 50 lakhs, select the set of security enhancements that you believe gives the greatest overall risk reduction.
- Assuming a budget of 100 lakhs, select the set of security enhancements that you believe gives the greatest overall risk reduction.
- Choose a representative to present your proposed security enhancements this to the class.



6





Thank you

