



CIDX Cybersecurity Initiative

Process Control Security Forum Spring 2005 Meeting

Dallas, TX
May 18, 2005



Mark Heard
mheard@eastman.com
Eastman Chemical Company

Agenda



- Initiative Background
- Organization
- Activities

CIDX Cybersecurity Initiative Background



- Key element in U.S. Chemical Sector Cybersecurity Strategy

- CIDX Initiative Launched in 2003

- 30 leading companies as charter members
 - 10 founding members

Albermarle

BearingPoint

Celanese

Dow Corning

E.I. DuPont de Nemours

Eastman Chemical

Occidental Chemical

Rohm and Haas

SAP

The Dow Chemical Co

Chemical Sector Cybersecurity Program

Mission

Implement a program that focuses on cyber-security risk management and reduction **to ensure open but secure information and process control systems** that enable collaborative business operations

Principles

Reduce risk through effective management
Solutions that are appropriate for the diversity of membership and risk/consequence profiles
Address systemic security vulnerabilities (enterprise and supply chain)
Address US needs consistent with global nature of industry
Leverage expertise
Evolve program as needs change
Inclusive participation from entire supply chain

Key Program Elements

Involvement & Commitment

Encourage broad support & participation throughout the sector

Practices & Standards

Establish voluntary management practices, procedures, guidelines & standards to support overall sector cyber-security

Technology & Solutions Dev'l.

Proactively work with service providers, govt, & academia to accelerate development & commercialization of improved cost, effective solutions

Information Sharing Network

Identify & reduce infrastructure vulnerabilities, to guard against cyber-attacks & speed recovery from incidents

Public Affairs

Provide opportunities for participants to work together to advocate establishment of sector practices and policies

Chemical Sector Cybersecurity Program



Infrastructure

CIO Executive Board

Chemical company executives who direct the Program activities

Cybersecurity Program Management Office

Team of chemical company directors and managers who lead implementation of the strategy and ensure integration of Program activities

Leveraged Organizations

Strategy Elements

Chemical Trade Associations (FORUM)

- Involvement & Commitment
- Public Affairs

CIDX

- Practices & Standards
- Accelerate Technology Solutions

Chemical Sector ISAC

- Information Sharing Network



Cybersecurity Initiative

Long-Term Objectives



- Provide **tools and resources** to help the Chemical sector address cybersecurity risks
- Establish a **program with vendors** to define and encourage the commercialization of cost effective solutions
- **Represent the Chemical Sector** to standards bodies, and in government funded or academic research programs

Agenda



- Initiative Background

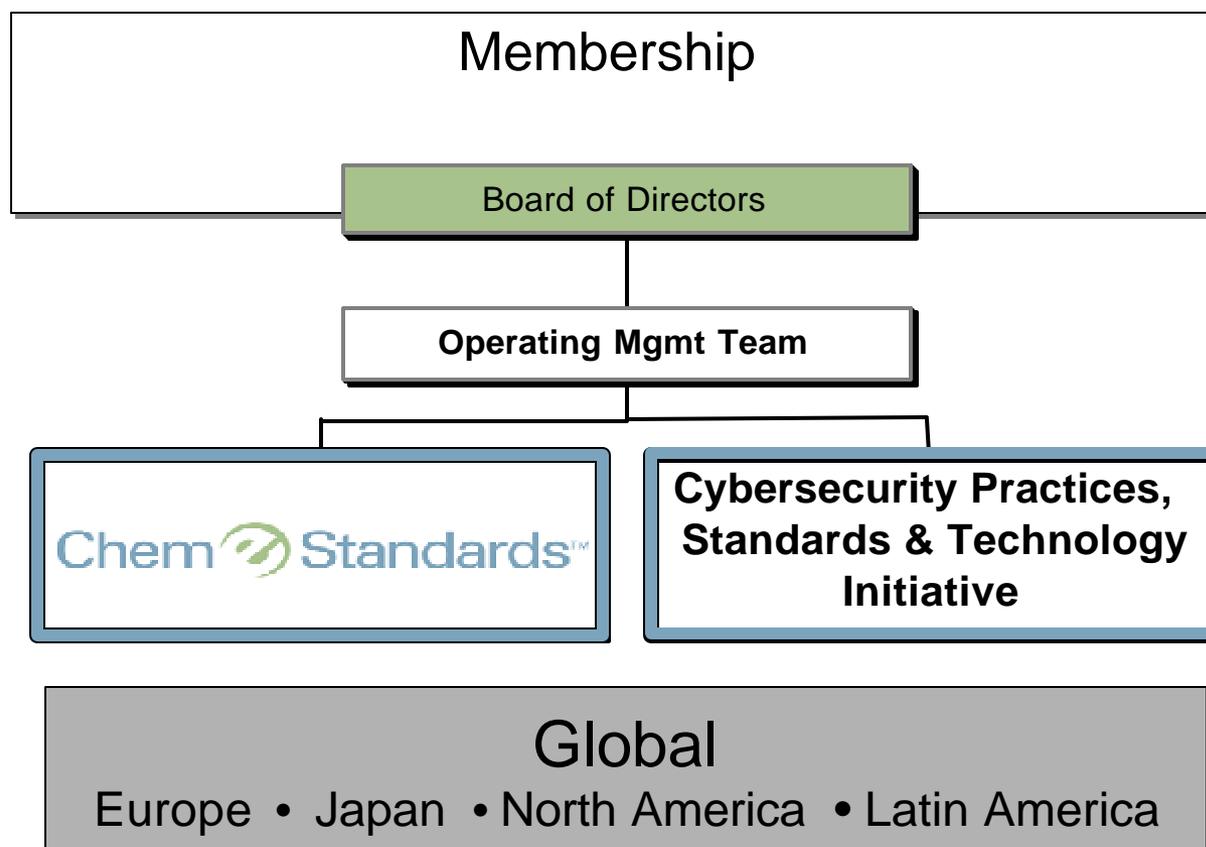


- Organization



- Activities

Organization



Steering Teams

Role: Portfolio of Prioritized Projects



- High level expertise and thought leadership
- Chartering projects to address high priority sector needs
- Oversight and guidance of project work-products and achievement of objectives
- Objectives, goals and plans for initiative
- Processes for guidelines, standards and practices development

Project Teams

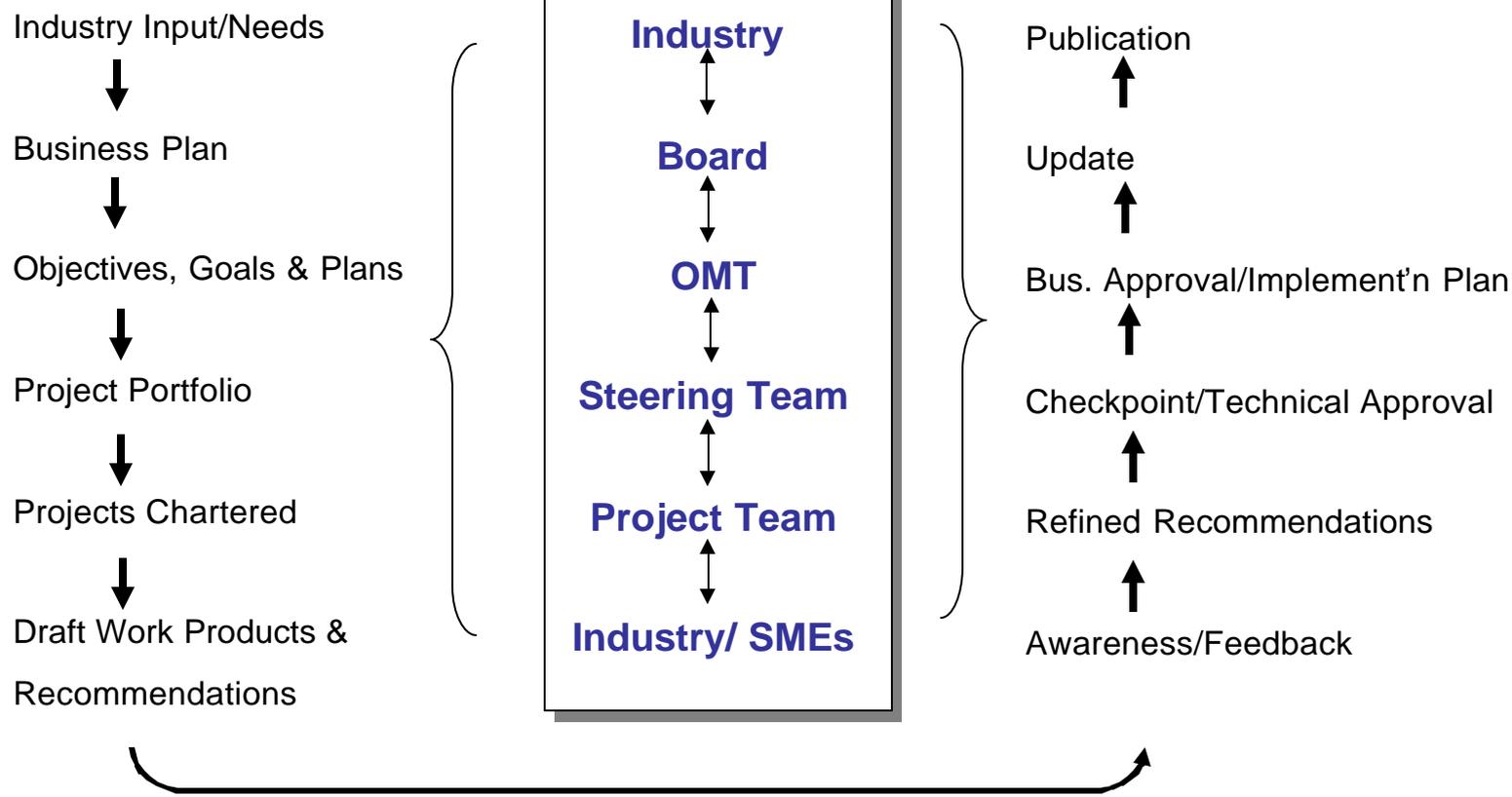
Role: Deliver Project Results



- Company and industry representation
- Practical knowledge and skill
- Resource leverage



Basic Approach "Needs Driven"

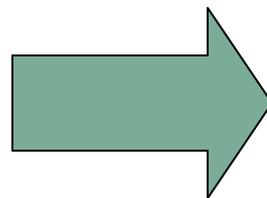


Project Process



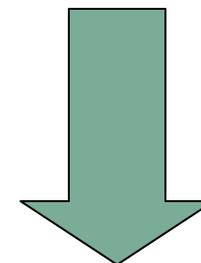
Pre-project

- ☐ Charter - scope & deliverables
- ☐ Team lead
- ☐ Timelines
- ☐ Resources
- ☐ Define milestones & checkpoints
- ☐ Team lead on-boarding



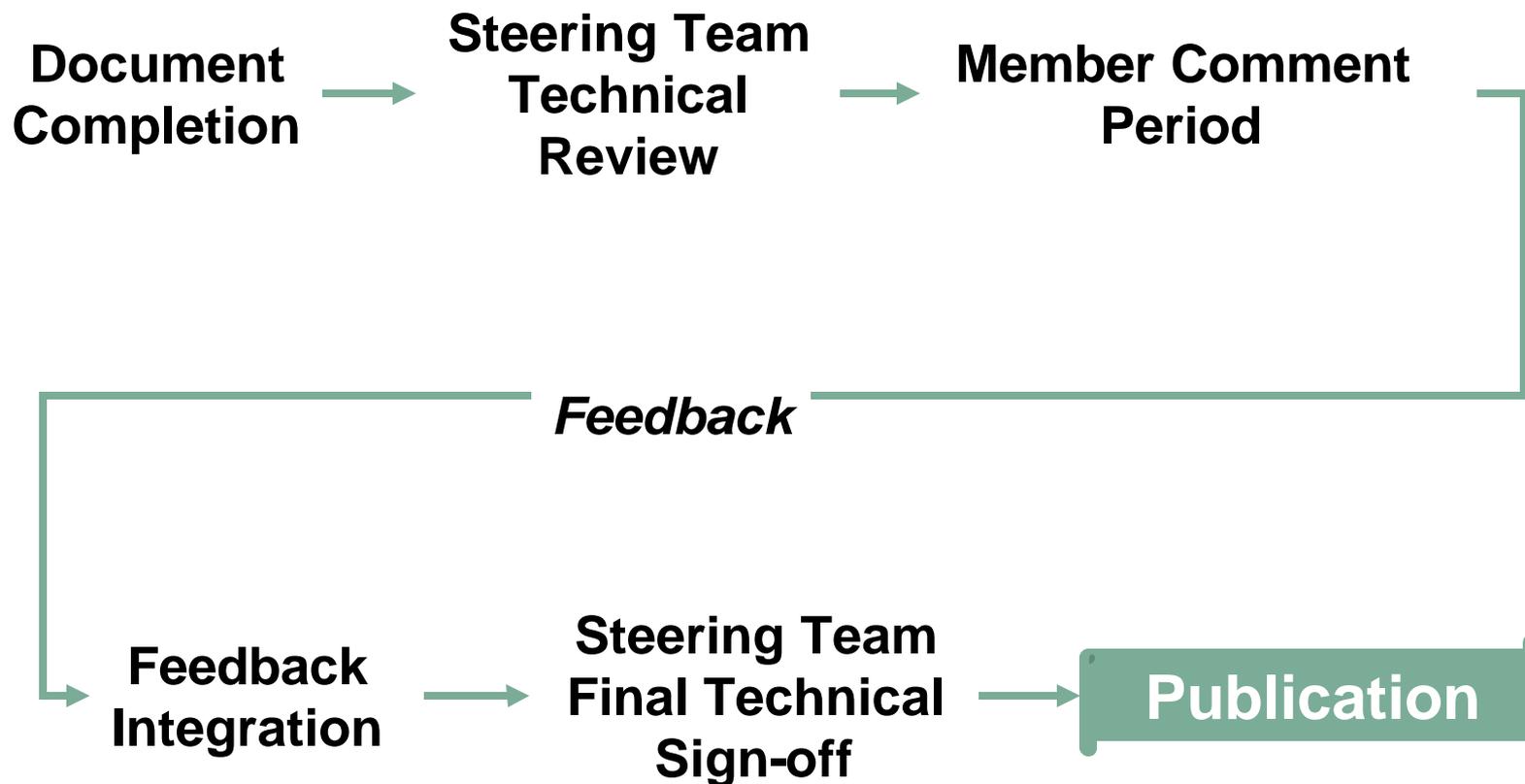
Project

- ☐ Weekly conference calls
- ☐ Webex
- ☐ eRoom usage
- ☐ Action Register



Approval Process

Approval Process for CIDX publications



Guidance Philosophy

- Voluntary
- Descriptive rather than prescriptive
- Vendor neutral
- Provide options rather than a single answer
- Examples rather than specificity
- Applicable across the sector recognizing the diversity in size and culture
- Consistent with antitrust policy

Agenda



- Initiative Background
- Organization
- **Activities**

Cybersecurity Initiative

Long-Term Objectives



- Provide **tools and resources** to help the Chemical sector address cybersecurity risks
- Establish a **program with vendors** to define and encourage the commercialization of cost effective solutions
- **Represent the Chemical Sector** to standards bodies, and in government funded or academic research programs

2004 Themes

- Development of a comprehensive set of cybersecurity program guidance
 - Scope included Information Technology, Manufacturing Control Systems, and Value Chain
- Tools for implementation

2004 Accomplishments

Guidance Publications

- **Published a comprehensive set of guidance and tools, addressing IT, manufacturing & control systems and value chain systems security**
 - Guidance for Addressing Cybersecurity in the Chemical Sector Version 2.0
 - Report on the Evaluation of Cybersecurity Vulnerability Assessment Methodologies Version 2.0
 - Report on the Evaluation of Cybersecurity Self-assessment Tools and Methods
 - Cybersecurity Reference Model
 - The Cybersecurity Journey – How to Begin an Integrated Cybersecurity Program (2Q05)

- **Plus two white papers that state a case for action**
 - A Case for Taking Action on Cybersecurity
 - Addressing Cybersecurity in Process Control

downloadable from <http://www.cidx.org>

2004 Accomplishments

Manufacturing & Control Systems

- Contributed to ISA SP-99 Technical Reports
 - ISA-TR99.00.01 Security Technologies for Manufacturing & Control Systems
 - ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment
- ISA SP-99 Standard
 - Providing working group co-leads for Part 1 and Part 2 of the standard
 - Providing document editor for Part 1
- Participant in NIST PCSRF (Process Control Security Requirements Forum)
- Established liaison with DHS-funded project at Idaho National Laboratory (INL)
- Participated in development of a DHS-sponsored chemical sector security tabletop exercise

2004 Accomplishments

Needs-Driven

- **Chemical sector market segmentation analysis and company surveys contributed to development of 2005 business plan**
 - U.S. Chemical Sector market segmentation
 - U.S. Chemical Sector Survey
 - Europe Chemical Sector Survey (completion Mar '05)
- **Supplier market segmentation analysis and identification of key technology issues**

Themes for 2005

- Shift emphasis from developing guidance to providing support for implementation
- Expand our external reach, by partnering with other sectors and organizations to work on areas of common interest
- Continue to promote manufacturing and control systems security by proactive engagement in standards bodies and government programs

Cybersecurity Initiative

2005 Goals



Long-Term Objective 1
Provide **tools and resources** to help the Chemical sector address cybersecurity risks

Goal 1: Provide educational and awareness support for implementation of CIDX work products

Goal 2: Provide enhancements to CIDX guidance documents to improve usability and expand adoption

Goal 3: Leverage cybersecurity activities globally

Cybersecurity Initiative

2005 Goals



Long-Term Objective 2

Establish a **program with vendors** to define and encourage the commercialization of cost effective solutions

Goal 4: Promote the sector position on technology issues and requirements with key vendor segments and with U.S. government-sponsored research programs through collaboration with other sectors.

Cybersecurity Initiative

2005 Goals



Long-Term Objective 3

Represent the Chemical Sector to standards bodies, and in government funded or academic research programs

Goal 6: Ensure manufacturing and control systems standards meet the needs of the chemical sector

Goal 7: Establish relationships and credibility with DHS organizations in order to be a part of the dialogue around security issues affecting the chemical sector

Cybersecurity Initiative

2005 Program Plan



- Awareness and Education Phase 2 Project
- Manufacturing & Control Systems Security Team
- Technology Project
- Europe Cybersecurity Team
- Guidance for Small & Medium Companies Project
- Guidance Enhancements Project

2005 Projects

Awareness & Education Phase 2

■ Deliverables

- Conduct training sessions and/or web seminars
- Develop or acquire case studies to support adoption and implementation
- Contribute to the development of executive awareness materials
- Participate in ACC/SOCMA security summit
- Develop awareness materials describing cyber risks, their economic impact as well as the link between physical and cyber risks

2005 Projects

Manufacturing & Control Systems Security Team

■ Deliverables

- Lead in the development and promotion of ISA Security Standards.
- Participate in NIST PCSRF.
- Participate in the INL Control Systems Security Testing Center project in order to ensure that sector needs are incorporated into their work products.
- Represent the Chemical industry in activities of the OMAC Microsoft Manufacturing Users Group (MS-MUG)
- Outreach to other initiatives as appropriate to ensure cybersecurity is adequately considered.

2005 Projects

Technology

■ Deliverables

- Document sector position on key technology issues, especially as they relate to infrastructure and regulatory control systems
- Engage with other key infrastructure sectors to jointly promote technology issues and needs with the vendor community
- Document sector research needs
- Develop metrics to track progress
- Work through DHS Science & Technology Division to ensure sector research priorities are reflected in U.S. government research program for 2006 and beyond

2005 Projects

Europe Cybersecurity Team

- Deliverables
 - Develop a value case for cybersecurity in Europe
 - Grow network in Europe





2005 Projects

Guidance for Small & Medium Companies

- 
- Deliverables
 - Pilot and assess usability of CIDX Guidance with small and medium companies
 - Evaluate other available small company guidance and tools
 - Recommend approach for training and implementation support
 - Recommend solutions to unmet needs
- 

2005 Projects

Guidance Enhancements

- Deliverables
 - Define a document revision process
 - Implement a formal feedback mechanism
 - Enhance current guidance documents as needed, to support small/medium companies or to address specific needs
 - Develop check-list for DHS security threat levels
 - Pilot an Experts Panel (topic area: Overall Guidance)

Raising the Bar Requires Broad Participation

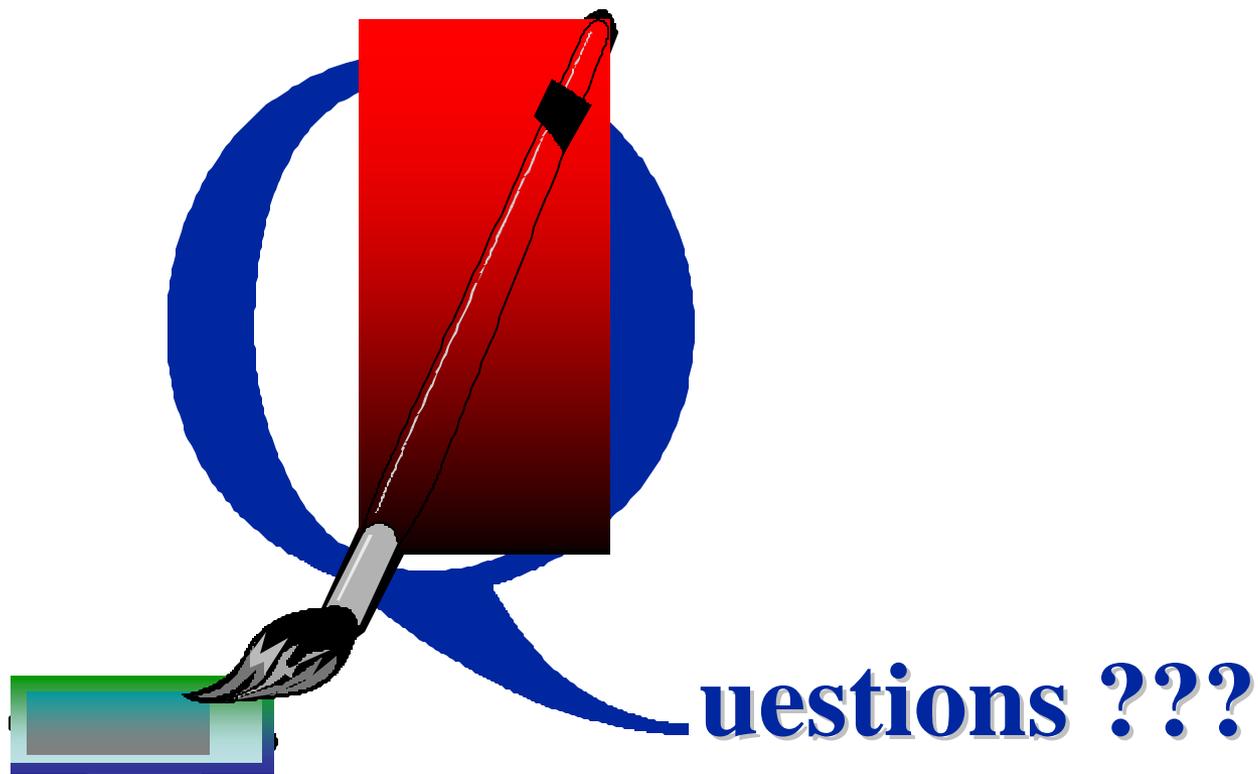


- Threats to our cybersecurity are growing in number and sophistication
- Potential impact is enormous
 - 90 percent of survey respondents detected computer security breaches in the last 12 months
 - 80 percent acknowledged financial losses due to computer breaches
 - The most serious financial losses occurred through Theft of Proprietary Information and Financial Fraud
- What's at stake:
 - Public Safety
 - Brand image
 - Company reputation
 - Ability to conduct business

What's So Special About the Chemical Industry?



- We're here
 - We're organized, active, ready to work to develop solutions and standards
- We're a good representative cross-section of manufacturing industry
 - Variety of process applications
 - Strong safety culture
 - Solving our cybersecurity problems will create solutions for other sectors



uestions ???



cidx[®]

By the Industry ... For the Industry

