Indo-US

Workshops on

Strengthening Supply Chain Security in the Pharmaceutical Industry

2020

VIRTUAL WORKSHOP

November 30, 2020 to December 2, 2020

9h00 to 12h30 (3h30)

by

CSIR-North East Institute of Science and Technology, Jorhat, Assam, India

and

CSIR-Central Leather Research Institute, Chennai, Tamilnadu, India

In association with
Pacific Northwest National Laboratory (PNNL), Richland, WA, USA
U.S. Department of State's Chemical Security Program (CSP), Washington DC, USA
CRDF Global, Arlington, VA, USA

Strengthening Supply Chain Security in the Pharmaceutical Industry

Theme

Pacific Northwest National Laboratory (PNNL), USA, CRDF Global, USA and the U.S. Department of State's Chemical Security Program (CSP), USA, along with CSIR-North East Institute of Science and Technology (CSIR-NEIST), India and CSIR-Central Leather Research Institute (CSIR-CLRI), India, are pleased to organize the 5th Indo-US Workshop on Chemical Security, on Strengthening Supply Chain Security in the Pharmaceutical Industry. The present workshop, due to the prevailing global situation, is going to be a VIRTUAL WORKSHOP.

The workshop syllabus and hands-on exercises are designed to help participants strengthen chemical security awareness, improve supply chain security, and enhance customer vetting. There is an immediate need for the pharmaceutical industry managers and staff, as well as others associated with the industry (academics, emergency services, transport and logistics) to learn how to deter and mitigate potential security threats involving the manufacture, use, or storage of hazardous or duel-use chemicals.

The workshop will take place over three consecutive days, for about 3½ hours per day.The contents of the workshop will be converted into an e-Learning course after the workshop to support the sustainability of the training.

The workshop will build chemical security awareness and provide cost-effective techniques for enhancing chemical supply chain security, provide a tool for evaluating the maturity of supply chain security programs, and enhance security coordination and communication. The workshop will assist companies to address and enhance chemical and product security beyond traditional concerns over product quality, counterfeiting, and transportation.

Who Should Attend?

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

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

Workshop Syllabus

The tentative syllabus for the workshop is as follows:

- Characterizing the potential adversary capabilities to divert or steal pharmaceutical chemicals, intermediates, and/or end products.
- Understanding threats to public safety and security from a potential attack involving the use of duel-use chemicals obtained from the pharmaceutical product supply chain.
- Raising security awareness throughout the product lifecycle.
- Improving incident response and security event reporting.
- Evaluating the maturity of existing chemical supply chain security programs, identifying security weaknesses in the supply chain, and identifying risk-based security objectives.
- Identifying high-value and cost-effective security controls that can improve security within the supply chain (e.g., security in product and process design, selection of suppliers and vendors, product procurement, workforce management and security training, inventory management, theft prevention, security monitoring, transportation).

Pacific Northwest
NATIONAL LABORATORY

CSP
CHEMICAL SECURITY PROGRAM

CRDFGLOBAL
INSPIRED BY PEOPLE | DRIVEN BY SCIENCE

CSIR • INDIA

CONNECTING SCIENCE & TECHNOLOGY
NEIST
FOR A BRIGHT TOMORROW

CSIR-CLRI

Indo-US

Workshops on

Strengthening Supply Chain Security in the Pharmaceutical Industry

VIRTUAL WORKSHOP

WORKSHP PROGRAM

Day - 1 November 30, 2020

Theme: Awareness of Supply Chain Security Issues

09h00 - 09h50: 50 min		Opening Ceremony	50 min
		■ Welcome Remarks and Greetings from US and Indian Organizers	
		■ Purpose, Structure and the Goals of the Workshop	
		■ Introduction of Instructors and Participants	
		■ Perspectives and Overview on the Security of Dual-Use Chemicals (Europe, India and USA)	
09h50 - 09h55:		Break	05 min
09h55 - 10h55:		**Technical Session - 1**	60 min
09h55 - 10h25: 30 min	L1	Examples of Security Risks in Supply Chain and Customer Vetting ● Sabotage, theft, diversion, and loss of sensitive information	
10h25 - 10h55: 30 min	L2	Threats and Consequences ● Insiders, criminals, terrorists, nation states, and other external threats ● Types of attacks: physical, cyber, and blended ● Confidentiality, Availability, and Integrity Impacts ● Ways to enhance security: Predict, Prevent, Detect, and Respond to attacks	
10h55 - 11h00:		Break	05 min
11h00 - 12h30:		**Technical Session - 2**	90 min
11h00 - 11h25: 25 min	L3	Exercise - A ● Given the characteristics of an example pharmaceutical company and the capabilities of an identified adversary -- identify potential security issues.	
11h25 - 11h55: 30 min		Supply Chain Security and Customer Vetting ● Similarities and differences between traditional supply chain security and what is needed to safeguard hazardous chemicals ● Customer vetting/Know-your-customer	
11h55 - 12h20: 25 min		Exercise - B ● For the pharmaceutical company in the previous exercise, identify potential practices that can be adopted to better secure the chemical supply chain.	
12h20 - 12h30:		Questions & Answers and Discussions	10 min

Indo-US
Workshops on
Strengthening Supply Chain Security in the Pharmaceutical Industry
VIRTUAL WORKSHOP
WORKSHP PROGRAM

Day - 2	December 1, 2020	9h00 - 12h30

Theme: Security vulnerabilities and engineering

09h00 - 10h10:		**Technical Session–3**	70 min
09h00 - 09h10:		Review of Day 1 / Introduction to Day 2	
09h10 - 09h40: 30 min	L4	Security Vulnerabilities in the Supply Chain ● Security vulnerabilities may exist throughout all the stages in the product lifecycle. Review potential supply chain security vulnerabilities.	
09h40 - 10h10: 30 min		Exercise - B ● For the pharmaceutical company in the previous exercise, identify potential vulnerabilities in their supply chain.	
10h10 - 10h15:		Break	05 min
10h15 - 11h25:		**Technical Session-4**	70 min
10h15 - 10h45: 30 min	L5	Security Engineering ● Supply chains can be securely engineered to prevent abuse and crime. ● Security approaches: strategic, tactical, and their integration. ● Layered defences, building security into equipment, incident response, and event reporting.	
10h45 - 11h25 40min		Exercise C(& D) For the pharmaceutical company in the previous exercises, identify potential vulnerabilities in their supply chain.	
11h25 - 11h30:		Break	05 min
11h30 - 12h05:		**Technical Session-5**	35 min
11h30 - 12h05: 30 min		Social Engineering for Chemical Security Techniques used by adversaries to manipulate organization staff	
12h05 - 12h30:		**Questions & Answers and Discussions**	25 min

Indo-US
Workshops on
Strengthening Supply Chain Security in the Pharmaceutical Industry
VIRTUAL WORKSHOP

WORKSHP PROGRAM

Day - 3	December 2, 2020		9h00 - 12h30
Theme:	Chemical security and supply chain security maturity model		
09h00 - 10h55:	**Technical Session- 6**		55 min
09h00 - 09h10:	Review of Day 2 / Introduction to Day 3		10 min
09h10 - 09h55: 45 min	L7	Assessing Supply Chain Security ● Assessment methods ● Introduction to maturity models ● Discuss modeling the maturity of chemical security programs ● Introduce the freely available Chemical Security Maturity Model.	
09h55 - 10h00:	Break		05 min
10h00 - 11h15:	**Technical Session- 7**		75 min
10h00 - 10h30: 30 min		Exercise - E Exercise to apply chemical security maturity model.	
10h30 - 11h15: 45 min	L8	Assessing Supply Chain Security (cont.) ● Assessing supply chain security costs ● Introduction of the Chemical Security Supply Chain Maturity Model ● Balancing risks and costs	
11h15 - 11h20:	Break		05 min
11h20 - 12h30:	**Technical Session - 8**		70 min
11h20 - 12h05: 45 min		Exercise - F Group Activity: Exercise to apply Chemical Security Supply Chain Maturity Model.	
12h05 - 12h30: 25 min		Conclusions and Closing Remarks (Both the teams)	

The Workshop Organizers

The U.S. partners at the workshop are Pacific Northwest National Laboratory (PNNL), CRDF Global, and their work is sponsored by the U.S. Department of State's Chemical Security Program (CSP). The Indian workshop partners include the CSIR-North East Institute of Science and Technology (CSIR-NEIST) and CSIR-Centre for Leather Research Institute (CSIR-CLRI). This workshop is a follow-up to the chemical security vulnerability assessment workshops conducted 2016 in Hyderabad; 2017 in New Delhi, Ahmedabad, and Hyderabad; 2018 in Chandigarh and Visakhapatnam and 2019 in Ahmedabad and Hyderabad.

Patrons and Advisory Committees

Patrons

Dr. Shekar Mande

Director General, CSIR, New Delhi, India

Dr. G. Narahari Sastry

Director, CSIR-NEIST, Jorhat, India

Dr. K.J. Sreeram

Director, CSIR-CLRI, Chennai, India

Mr. Jack Dishner

Chemical Security Program, Depart 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. R. L. Goswamee

Senior Principal Scientist, CSIR-NEIST, Jorhat, India

Dr. M. Surianarayanan

Senior Principal Scientist, CSIR-CLRI, Chennai, India

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

India

Dr. G. Narahari Sastry
Director, CSIR NEIST
Jorhat, Assam, India
Tel: +91 99635 82996
director@neist.res.in
gnsastry@gmail.com

Dr. Lakshi Saikia
Senior Scientist,
CSIR NEIST, Jorhat, Assam, India
Tel: +91-9957031635
lsaikia@neist.res.in
l.saikia@gmail.com

Dr. Manas Ranjan Das
Senior Scientist
CSIR NEIST
Tel: +91-9957178399
mrdas@neist.res.in

Dr. K.J. Sreeram
Director,
CSIR-Central Leather Research Institute
Adyar, Chennai, Tamil Nadu, India - 600 020
Phone: +91 - 44 - 24910897
Email:director@clri.res.in,

Dr. M. Surianarayanan
Senior Principal Scientist,
CSIR-Central Leather Research Institute
Adyar, Chennai, Tamil Nadu, India - 600 020
Tel: +1 509-375-2166
E-mail: clrimsn@gmail.com

USA

Dr. Clifford Glantz
Chief Scientist, PNNL
Tel: +1 509-375-2166
cliff.glantz@PNNL.gov

Dr. Radha Kishan Motkuri
Senior Principal Scientist, PNNL
Tel: +1 509-371-6484
radhakishan.motkuri@pnnl.gov

Dr. John Cort
Senior Principal Scientist, PNNL
Tel: +1 509-371-6334
john.cort@pnnl.gov

India (Proposed NACS)*

Prof. V.K. Jain
Gujarat University
Tel: +91-7926300969
drvkjain@hotmail.com

Prof. S. K. Mehta
Panjab University, Chandigarh
Tel:+91 944 080 2808
surinder.sk1961@gmail.com

Dr. G. V. M. Sharma
Yajushi Labs., Hyderabad
Tel: +91-944 080 2785
sharmagvm@gmail.com

Mr. 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

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

*NACS: National Association for Chemical Security (NACS)

During the Indo-US workshop in 2018/2019, the organizers from both the USA and India, planned to establish an Association for Chemical Security at the National level, to popularize the concept on Chemical Security amongst all the Academia and Industry, along with all other stake-holders. In 2020, the above team has formed a General Body and went ahead for the registration of NACS, National Association for Chemical Security. The details will be released by the time of the proposed 5th Indo-US workshop (Virtual).

Pacific
Northwest
NATIONAL LABORATORY

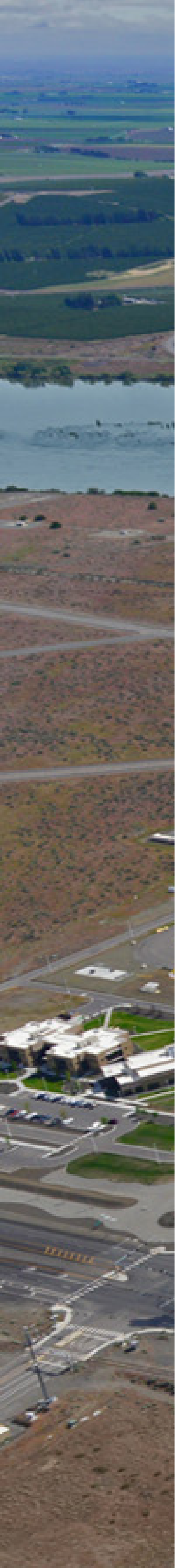
Lesson 1: Examples of Security Risks in Supply Chain and Customer Vetting

Cliff Glantz, John Cort, and Radha K Motkuri

Pacific Northwest National Laboratory (PNNL)
Richland, WA, 99352
USA

U.S. DEPARTMENT OF
ENERGY BATTELLE

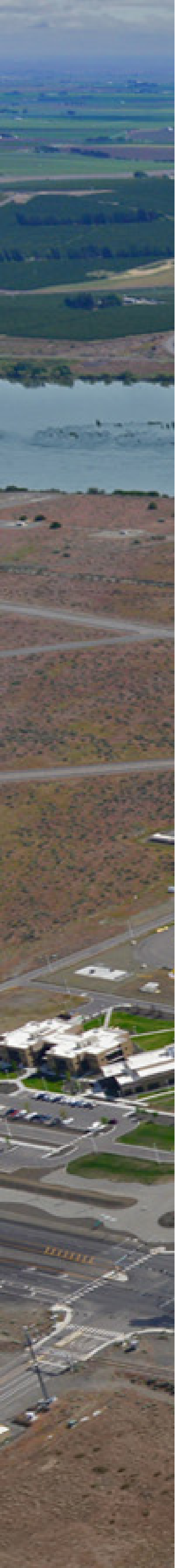
PNNL is operated by Battelle for the U.S. Department of Energy



Outline of this Presentation

I will present:

- A few hypothetical scenarios involving chemical life-cycle and supply chain security problems that could befall pharmaceutical and specialty chemical companies – and could potentially involve **dual-use chemicals**.
- Real world examples of actual security incidents that have affected companies – including chemical, pharmaceutical, and other critical infrastructures.
- The purpose of this presentation is to raise awareness of potential ways your supply chain can be attacked – through physical and cyber techniques. -

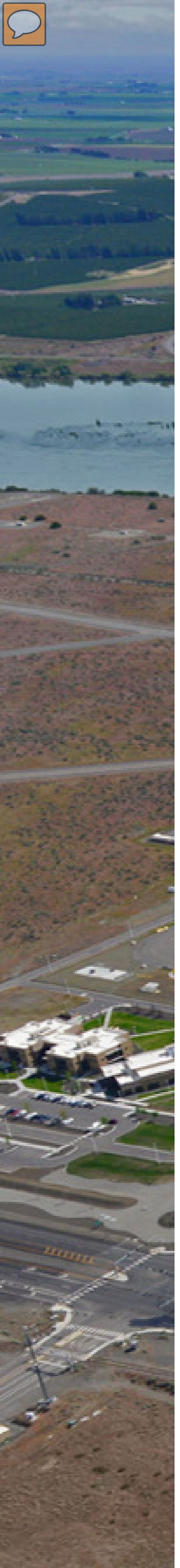


Pacific Northwest
NATIONAL LABORATORY

Cliff Glantz

- 38 years as a scientist and project manager at Pacific Northwest National Laboratory
- Expertise in emergency management, risk management, critical infrastructure protection, cybersecurity, and blended cyber-physical security
- Five years supporting chemical and nuclear security projects in India for the U.S. Department of State
- India cybersecurity engagement coordinator for the U.S. Office of International Nuclear Security.

Indo-US
Workshop on
Safeguarding Dual-Use Chemicals
Application of Vulnerability Assessment Tools and Risk-Based Security Enhancements
2018
July 16-17, 201
t of SAIF/CIL, Panjab
digarh
SP
CSIR - Indian Institute of Chemical Technology
Hyderabad, India
in association with
Pacific Northwest National Laboratory
U.S. Department of State's Chemical Security Program
Indo-
Worksho
Vulnerability Ass
Weaponizable Dual Pur
icals
July 28-
CSP



Consider a Few Hypothetical Examples: Case 1

Customer Vetting

- The sales office of your pharmaceutical 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.
- The product is prepared and is ready to ship 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.

FREE YOUR LOGO

Sales Order

COMPANY NAME
1st Main Street
City, State Zip
123-456-7789

Sales: S/O#: 0001 Date:

Company Name: Terms: Ship Via:

Bill to: Attn:	Ship to: Attn:
Street:	Street:
City: State: Zip:	City: State: Zip:
Tel: Fax:	Tel: Fax:
E-mail:	E-mail:

Item Number	Description	Quantity	Unit Price	Total
			Total:	

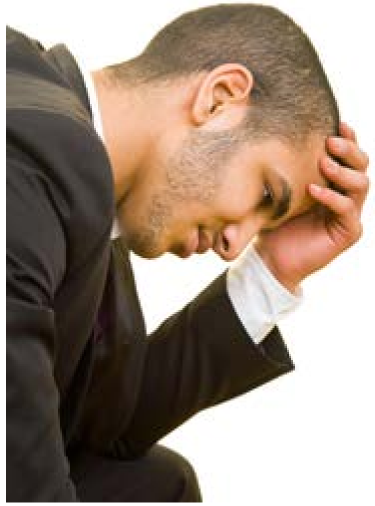
Credit Card #: Exp: CVV#:

Authorized Signature: Date: / /

Case 2

Cyberattack and Customer Vetting

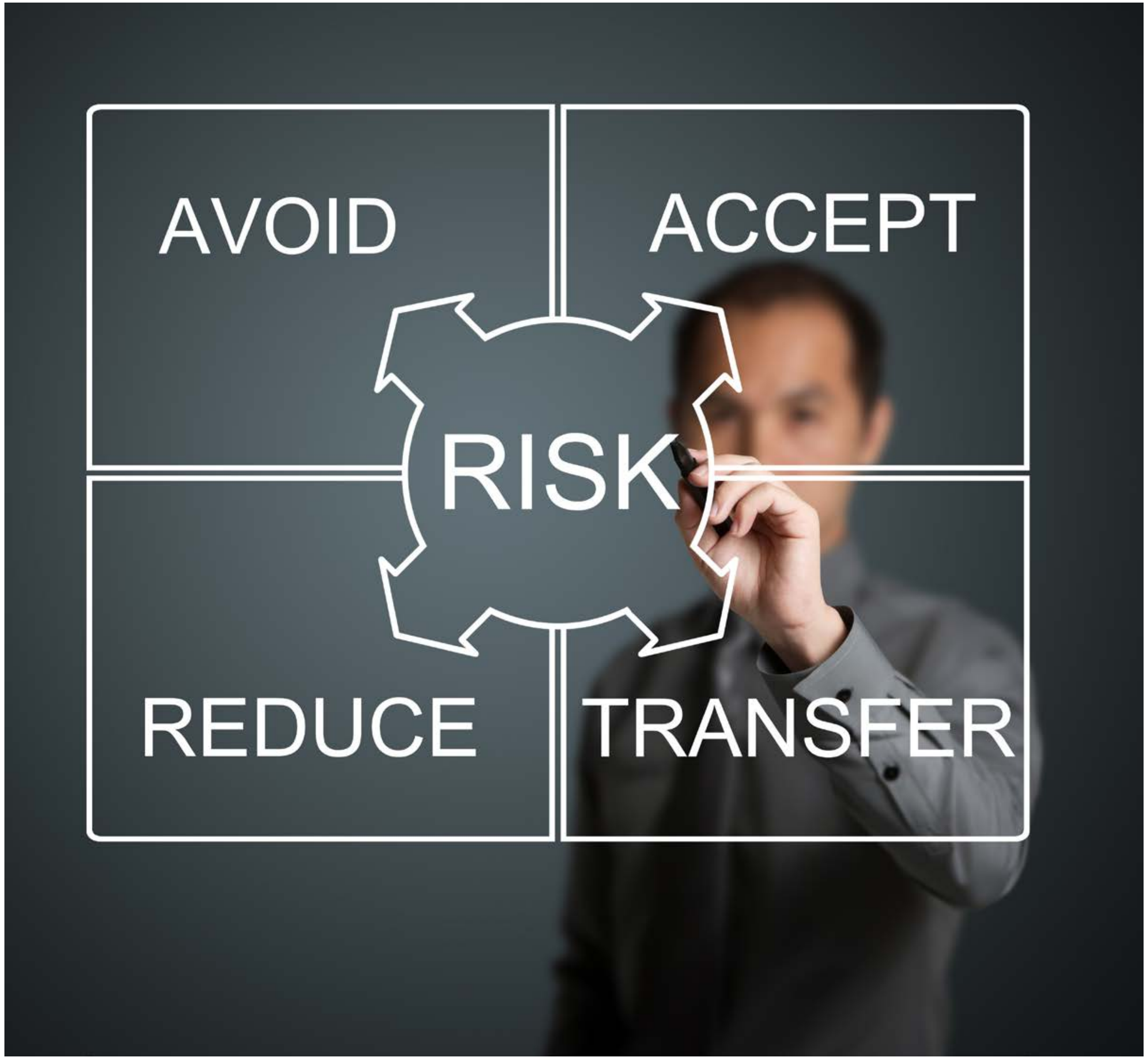
- A regular customers submits an order to your chemical company for a dual-use chemical.
- A terrorist organization mounts a successful **cyber intrusion into your shipping system**.
- They **change the delivery address** for a legitimate order from your customer's facility to their warehouse.
- The product is shipped to the terrorists instead of the intended recipient.
- This mistake is not detected until the legitimate customer inquires as to the location of their order. By then, the product is gone and the warehouse where it was delivered is abandoned. -



Case 3

Sabotage through a Cyberattack

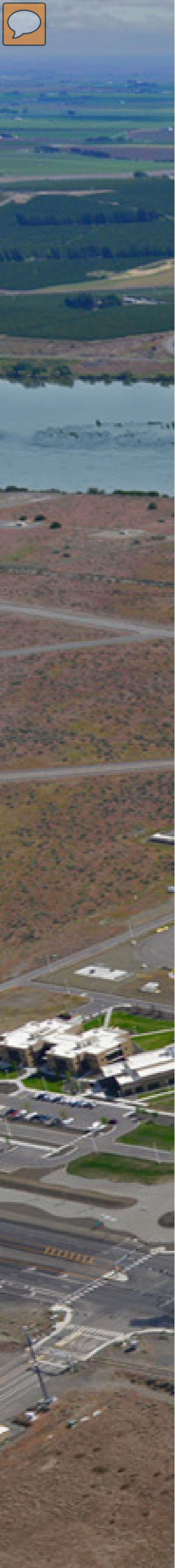
- A criminal organization obtains a **username and password to your industrial control systems network**.
- They break into the network and map the functions of several chemical manufacturing processes.
- They **threaten sabotage** that could cause an explosion if your company does not pay a **ransom**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


AVOID
ACCEPT
RISK
REDUCE
TRANSFER

Case 4

International Purchases

- A company from a country that is in conflict with your country offers your company a digital control system at a price that is lower than offered by other international suppliers.
- Do you buy it?
- That “hostile country’s” spy agency has engineered a **backdoor into that control system.**
- When in service, this control system can be accessed via an internet connection to provide information on its operations
- The **product can be reprogrammed** by the supplier to malfunction if a conflict escalates between their country and your country.



Case 5

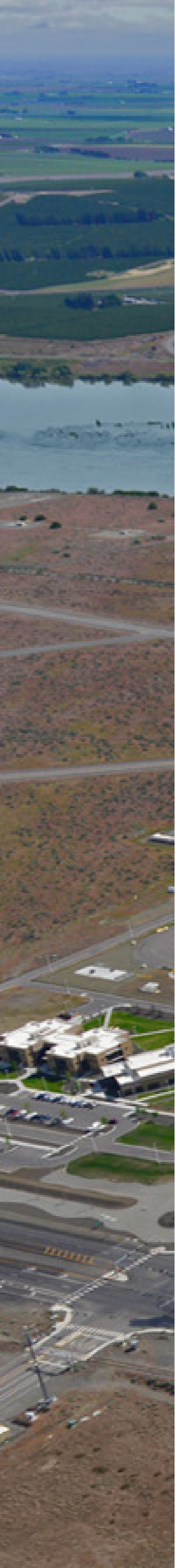
<u>Loss of Intellectual Property</u>

- A supplier has access to your company’s **inventory database**.
- An employee of the supplier uses their access to search for **information** on your database that they could sell to a competitor.
- They might also maliciously attempt to **escalate their privileges** and search for intellectual property on other company computers in your network.

Case 6

Loss of Intellectual Property

- An employee uses an **insecure Wi-Fi connection** to access your company’s business network.
- The employee’s **login credentials are stolen**.
- The stolen credentials are used to enter your company network and **steal product design information**.
- Sometime later, your company finds its markets being flooded by cheap, counterfeit, cut-rate versions of its products using your logo.
- Your customers begin contacting your company with complaints, believing the cut-rate counterfeit products are from your company. -



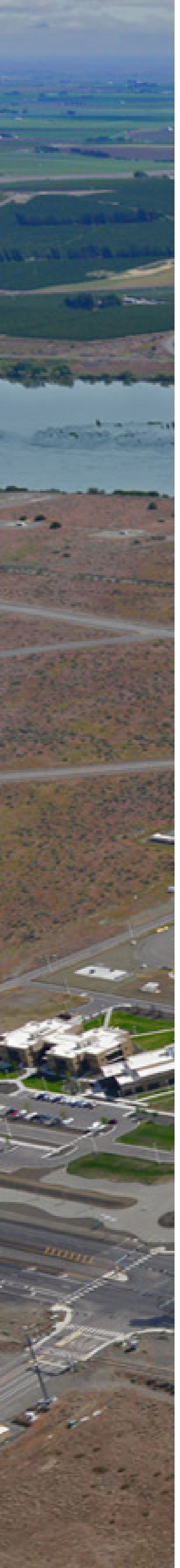
Real World Incidents

- Our hypothetical examples were all based on real-world events or attacks demonstrated to be plausible.
- Emphasized cyberattacks as components of these hypothetical attacks because they are **new**, **affordable**, and our current defenses are often inadequate.
- Physical attacks are better understood and their risks are more easily recognized.
- Let’s now look at some documented real-world attacks against companies, their supply chains, products, and assets.

Eli Lilly Warehouse Theft (2010)

- In the U.S., an **organized crime group** collected operational information about an Eli Lilly warehouse.
- 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 this pharmaceuticals heist and committed similar million-dollar warehouse jobs.
- Eventually caught and sentenced to prison.

http://www.courant.com/news/connecticut/hc-lilly-heist-ringleader-1206-20161205-story.html



Target Attack (2013)

- Target **lost sensitive customer payment data**
- The attackers hacked their way into Target's corporate network by compromising a third-party HVAC vendor (Fazio Mechanical).
- A phishing email duped at least one Fazio employee, allowing malware to be installed on Fazio computers.
- With the malware in place, and undetected by antivirus software, the attackers waited until the malware provided what they were looking for – Fazio’s login credentials to Target’s business network.
- Target later addressed the exploited vulnerabilities:
  - Require vendors to use appropriate anti-malware software.
  - Require two-factor authentication to access Target systems.
  - Bulked up internal firewalls

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

This was a cyberattack on an industrial control system that resulted in physical damage.

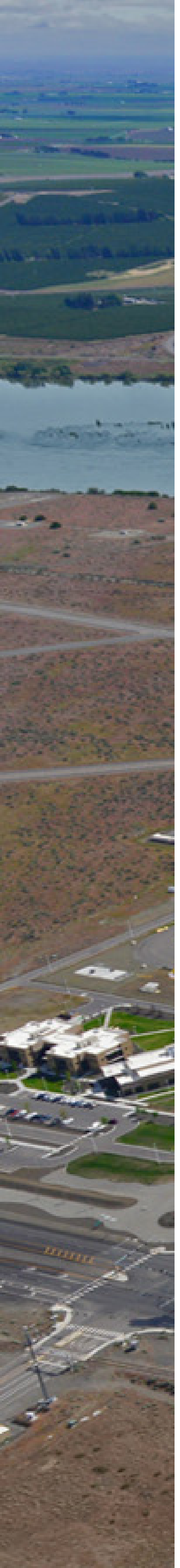
Ukraine Power Grid Attack (2015, 2016, and 2017)

Event: Cyberattack and exploitation of SCADA system for Ukraine power grid. Involved an “advanced and persistent threat” (APT).

Consequences: Power outages at 3 regional electric power distribution companies impacted about 225,000 people.

Specifics:

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



Pacific Northwest NATIONAL LABORATORY

Cyberattack on Saudi Arabia Petrochemical Plant (2018)

- A cyberattack on a petrochemical company “was not designed to simply destroy data or shut down the plant… 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 attackers compromised Schneider’s Triconex controllers – products 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

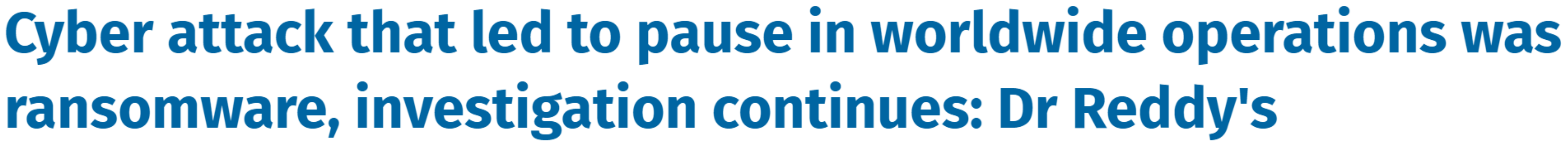
The New York Times

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.

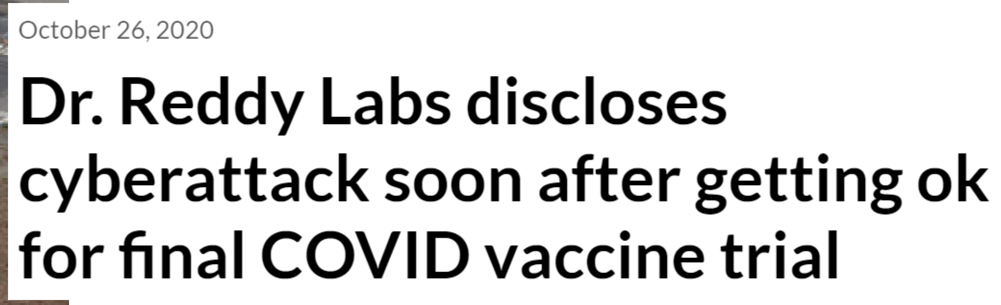
Cyberattack on Dr. Reddy’s - 2020

- "On 22nd October 2020, we experienced an information security incident and consequently isolated the impacted IT services. This incident involved a ransomware attack. We promptly engaged leading outside cybersecurity experts, launched a comprehensive containment and remediation effort and investigation to address the incident."

“…Recovery and restoration of all applications and data is underway. All critical operations are being enabled in a controlled manner."

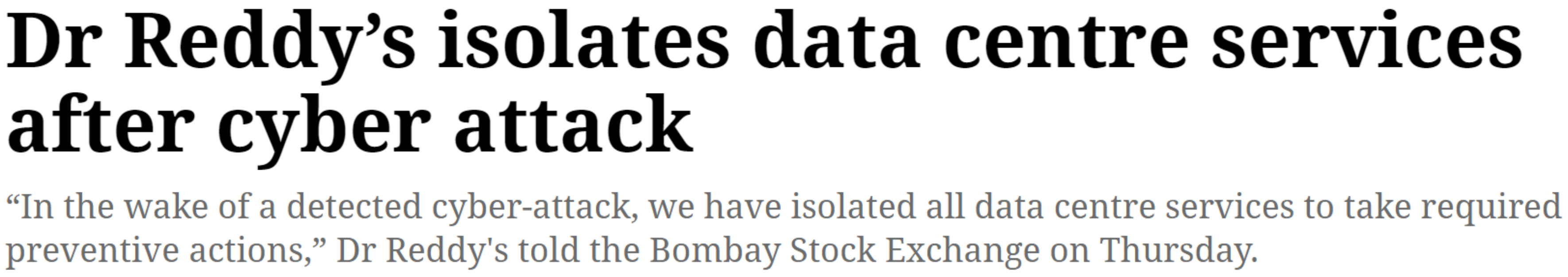


Cyber attack that led to pause in worldwide operations was ransomware, investigation continues: Dr Reddy's



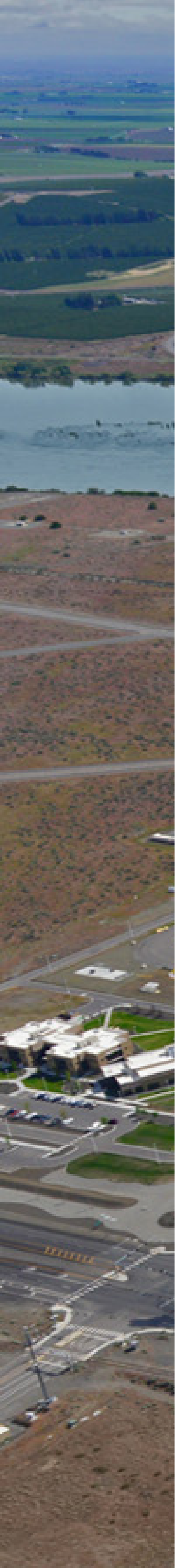
October 26, 2020

Dr. Reddy Labs discloses cyberattack soon after getting ok for final COVID vaccine trial



Dr Reddy’s isolates data centre services after cyber attack

“In the wake of a detected cyber-attack, we have isolated all data centre services to take required preventive actions,” Dr Reddy's told the Bombay Stock Exchange on Thursday.

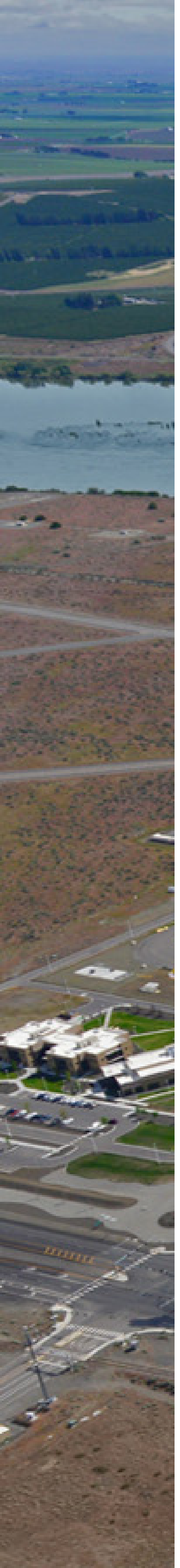


Pacific Northwest NATIONAL LABORATORY

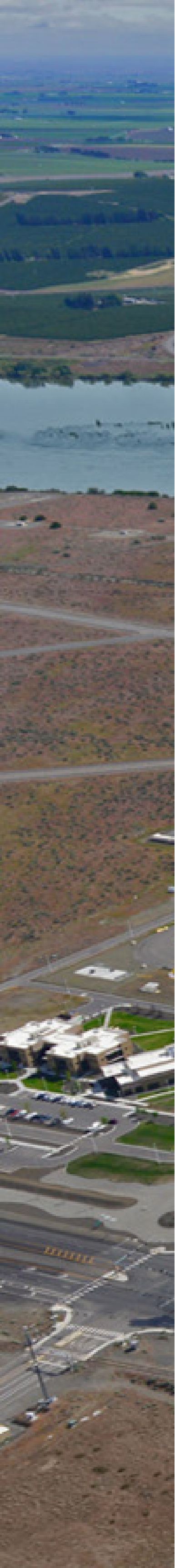
Summary

- All these “real-world” attacks were big – too big to be hidden from the public and government regulators.
- Public corporations in the U.S. are required by the Security and Exchange Commission to publicly report major security events.
- Many supply chain incidents involving sabotage, theft, or diversion are too small and “quiet” to get media attention.
- Observation: There are security threats and vulnerabilities involving the life cycle of dual use chemicals, supply chains, and other practices that can have implications for public safety and company profitability. -

Pacific Northwest
NATIONAL LABORATORY



Thank you



Pacific Northwest NATIONAL LABORATORY

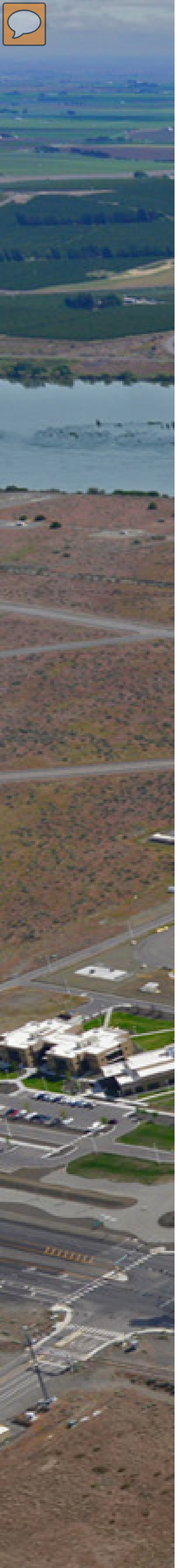
Lesson 2: Threats and Consequences

**Cliff Glantz, John Cort,
and Radha Kishan Motkuri**

Pacific Northwest National Laboratory (PNNL)
Richland, WA, 99352
USA

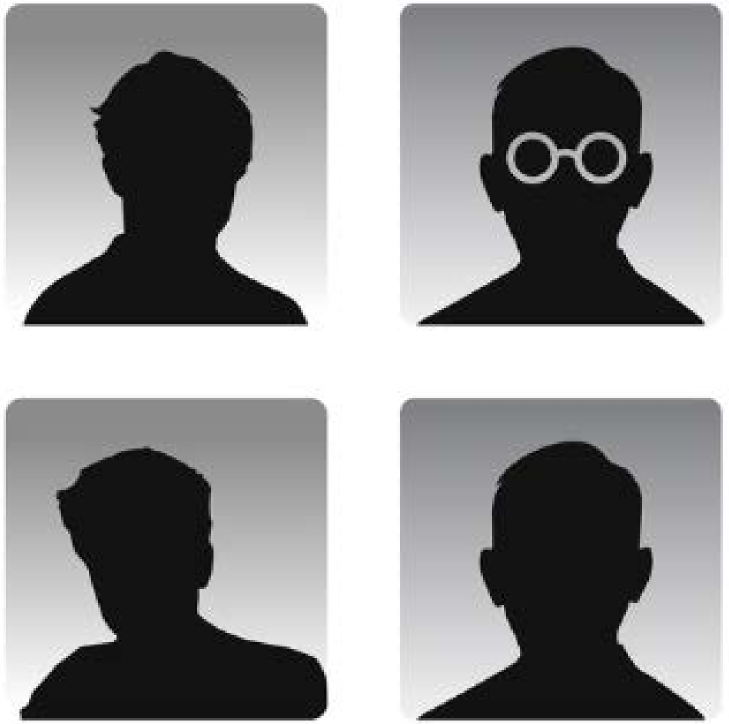
U.S. DEPARTMENT OF ENERGY BATTELLE

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



Potential Threat Agents/ Adversaries

- External threat agents
  1. Criminals
  2. Terrorists
  3. Nation states
  4. Antisocial individuals



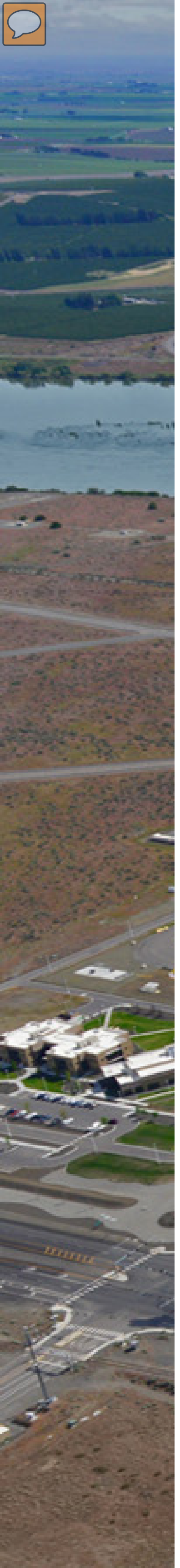
- Internal threat agents: “Insiders”
  - dissatisfied or mentally ill employees
  - former employees
  - external threat agents working within the organization

The Objectives of Threat Agents

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

Types of Adversaries: Insiders

- Access:
  - May have **detailed knowledge** of facility operations, including critical systems.
  - May have **direct physical access** to the facility and its systems.
  - May have **electronic access** to plant information and control systems – including security systems and intellectual property.
- By working inside defenses they can increase the success of an attack.

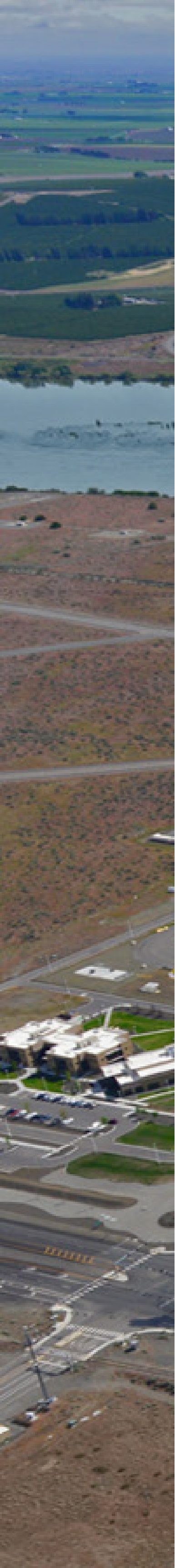


Types of Adversaries: Insiders

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

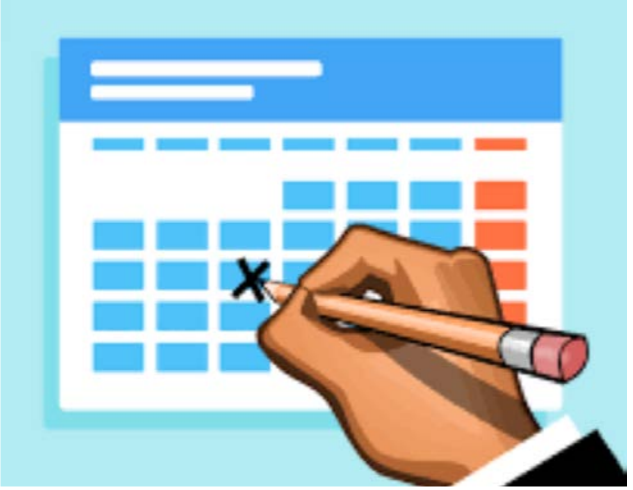
Motivations for Malicious Behavior

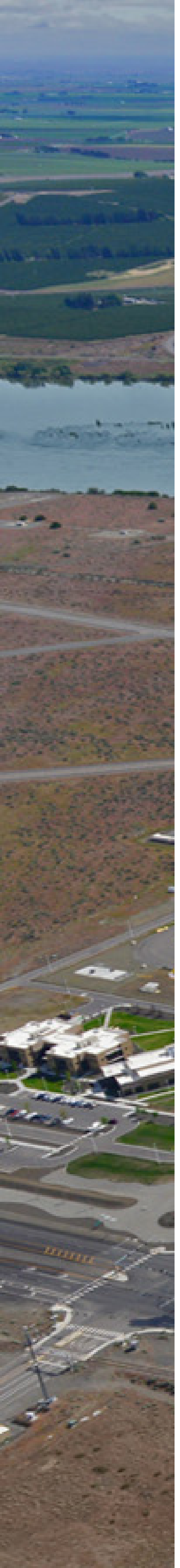
- **Disgruntled** – Want to harm the company, management, co-workers because of past slights or other events
- **Profit** – hired to work for attackers, steal products, sell information
- **Political/Cultural** – want to make a political statement or advance the agenda of a certain group
- **Mental illness**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



Malicious Intentions Can Lead to Bad Outcomes

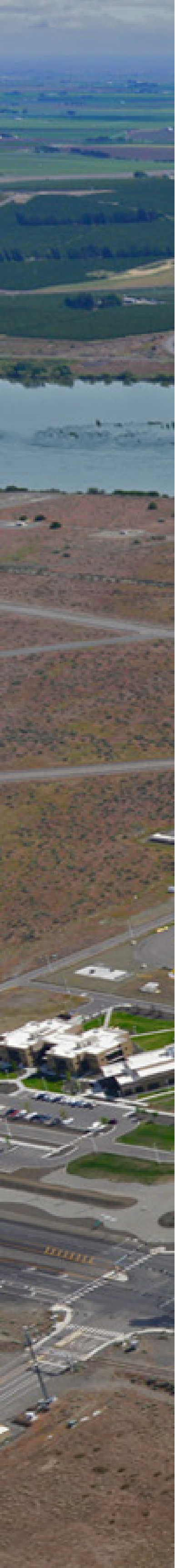
- Insiders possess **system knowledge** that can be used to their advantage
- Insiders are permitted to **access sensitive** systems and areas in the facility
- Insiders can **choose the best time** to commit a malicious act. Can have adverse consequences occur long after the insider leaves the facility.
- Insiders can take actions to reduce the likelihood that their malicious actions will be **traced back** to them. -





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
  - Increasingly likely to employ cyber attacks or mount combined **cyber-physical attacks**.

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. Increasingly likely to combine a physical and cyber attack.
- **Numbers:** Individuals to large groups
- **Resources:** Limited to extensive -

Pacific Northwest NATIONAL LABORATORY

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.") -

Types of Adversaries: Nation States

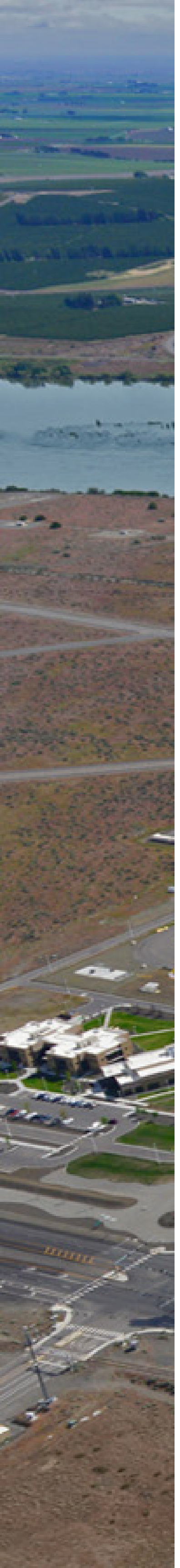
- **Intentions**: Ranges from information gathering to the intentional destruction/disabling of critical infrastructure.
- **Motivation**: Political influence, defense, preparation for potential future conflicts (military or non-military). May need to act with stealth.

Types of Adversaries: Nation States (cont)

- **Numbers**: Typically, extensive, well-organized, highly trained groups
- **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 Adversaries: Antisocial Individuals

- **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 like-minded groups
- **Resources** are limited by the intensity of their motivation and financial constraints.



Pacific Northwest
NATIONAL LABORATORY

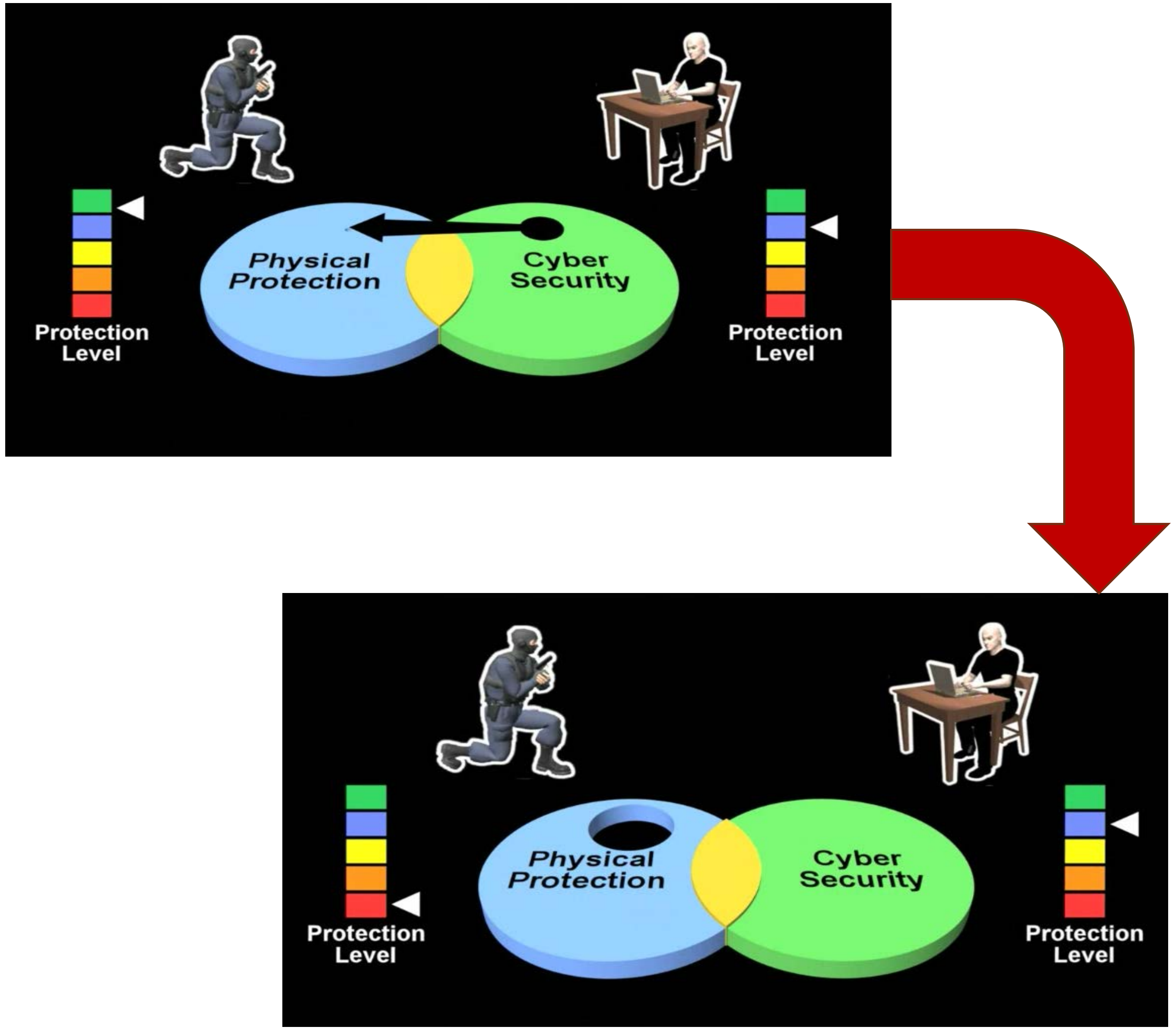
Types of Adversaries: Antisocial (Cont'd)

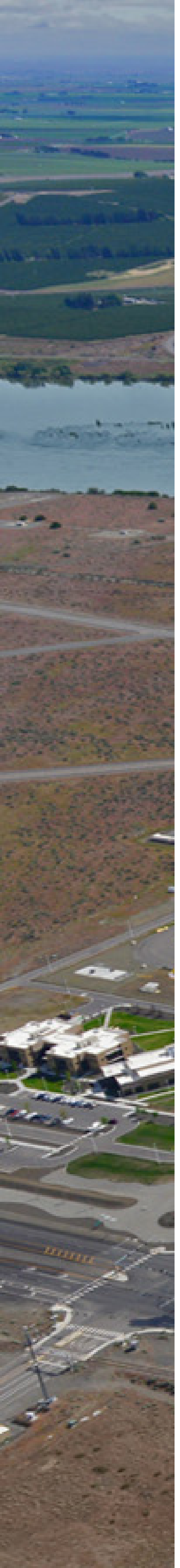
- Capabilities:
  - Their skill level may range from relatively **low to highly sophisticated**.
- Example -- cyber capabilities:
  - At the **low level**: May rely exclusively on off-the-shelf (including commercial) hacking technologies
  - At the **high level**: May develop their own sophisticated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

Pacific Northwest
NATIONAL LABORATORY

Types of Attacks

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

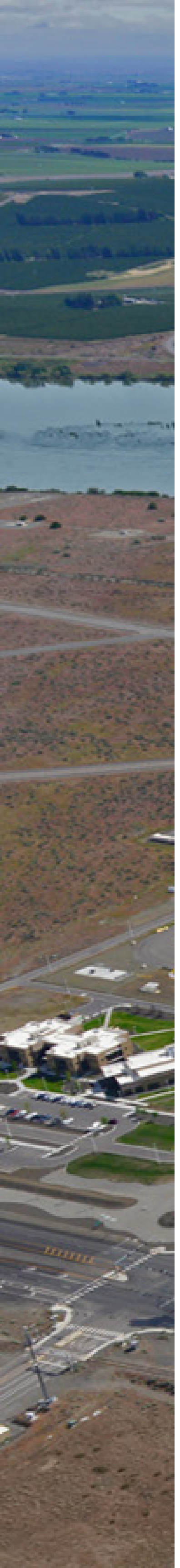




Design Basis Threat

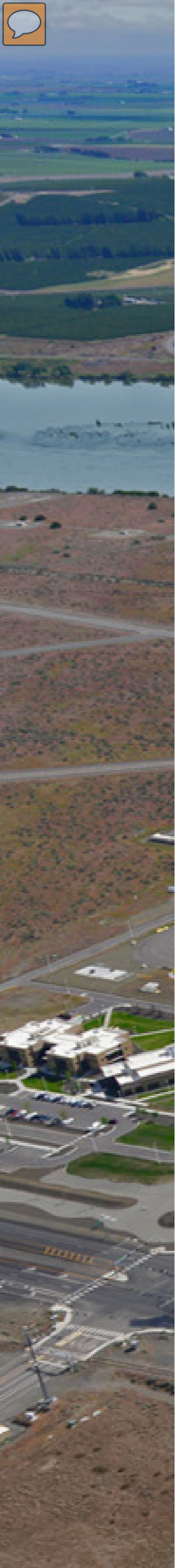
- No organization and facility can protect itself from all threats.
- To understand what types of threats the organization needs to design its security program to stop, it is helpful to determine an applicable Design Basis Threat (DBT).
- A Design Basis Threat (DBT) is:

> *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.* -

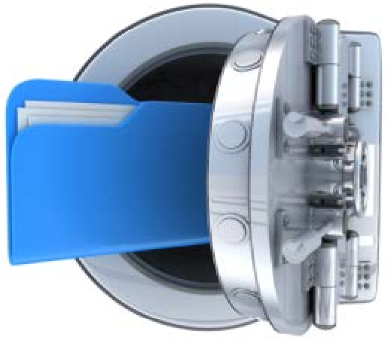


Design Basis Threat Example

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

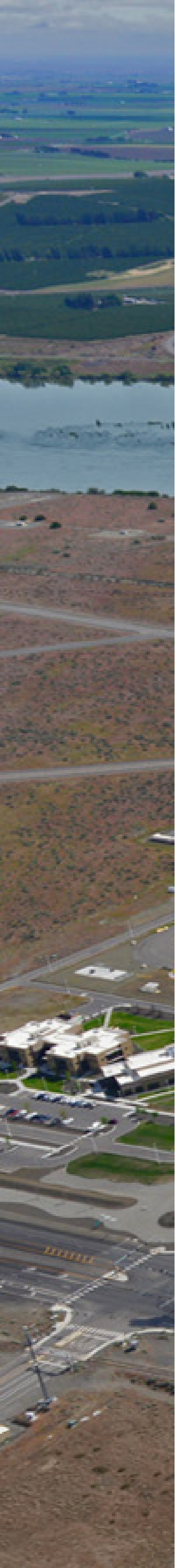


Types of Consequences



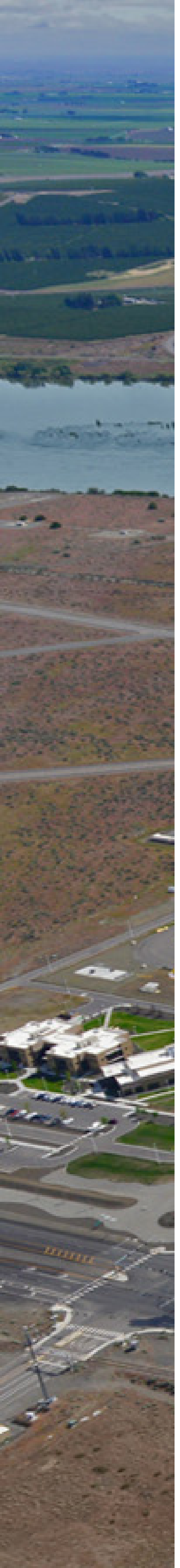
Consequences Fall into Three Categories:

1. Loss of Confidentiality
   - Theft of data, plans, information, etc.
2. Loss of Integrity
   - Data is altered or compromised
   - Facility systems are operating but adversaries can alter system operation.
3. Loss of Availability
   - Theft or diversion of material or products
   - System becomes inoperative or ineffective



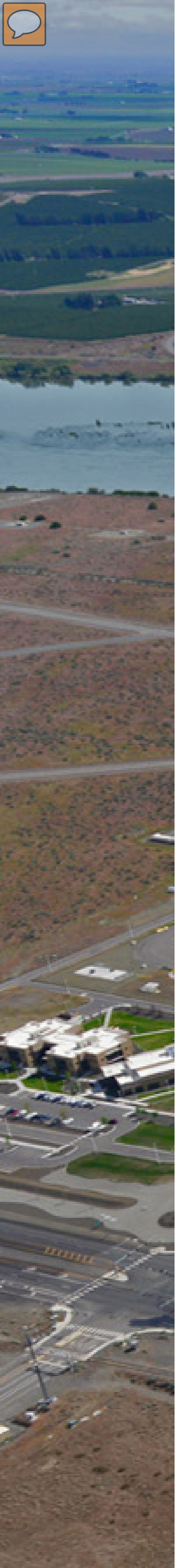
Loss of Confidentiality

- Loss of sensitive information. Examples include the loss of:
  - Staff **personnel records**
  - **Access control information** such as computer system usernames and passwords or security gate access information.
  - **Intellectual property** such as chemical formulations and processing information
  - **Shipping information** such as the scheduling and destination for the offsite transportation of dual-use chemicals
  - **Business information**, such as pricing and sales information -



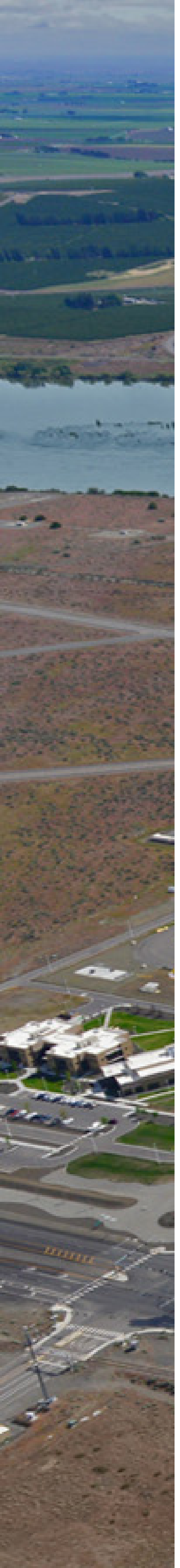
Loss of Availability

- Loss of ability to access data, systems, products, or facilities. Examples include:
  - Destruction or damage to chemical **manufacturing assets or storage facilities**
  - **Theft** of equipment or products.
  - Inability to access automated **security systems** requiring the facility to rely on manual systems.
  - Reduced ability to **monitor** some plant operations.
  - Reduction or elimination of **communications** within the facility or with the outside world.



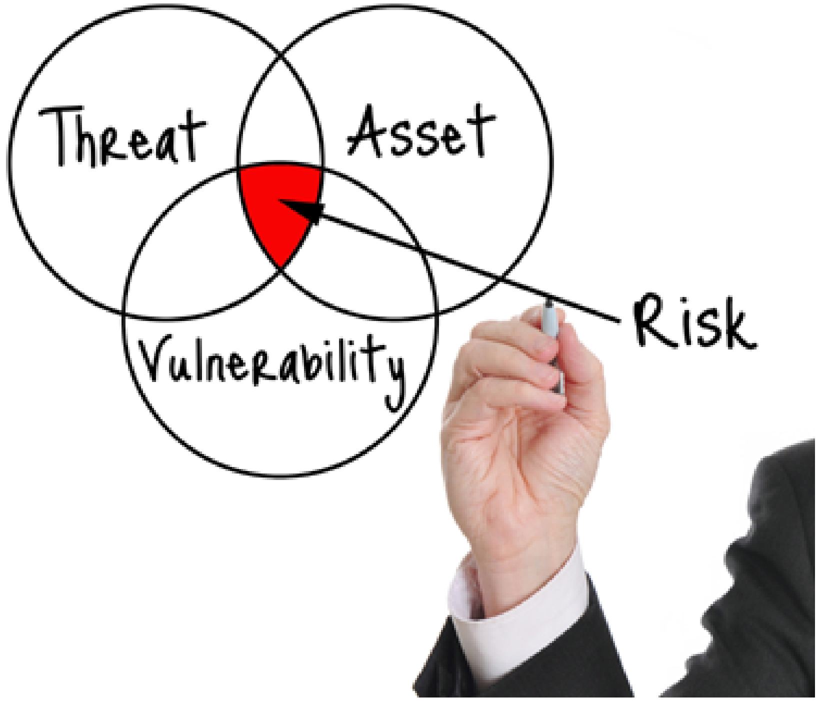
Loss of Integrity

- Loss of control over processes – including critical control systems – or products. Examples include:
  - Physical or digital **manipulation of the operation of chemical or pharmaceutical manufacturing or storage systems**. May involve taking control of plant automated processes and feeding false data to plant systems and system operators.
  - **Altering data in company systems**. The may involve changing order, shipping, pricing, and formulation data.
  - **Manipulate data in security systems**. This can include shutting off alarms, feeding security cameras false images, changing physical access authorizations, or data tampering.



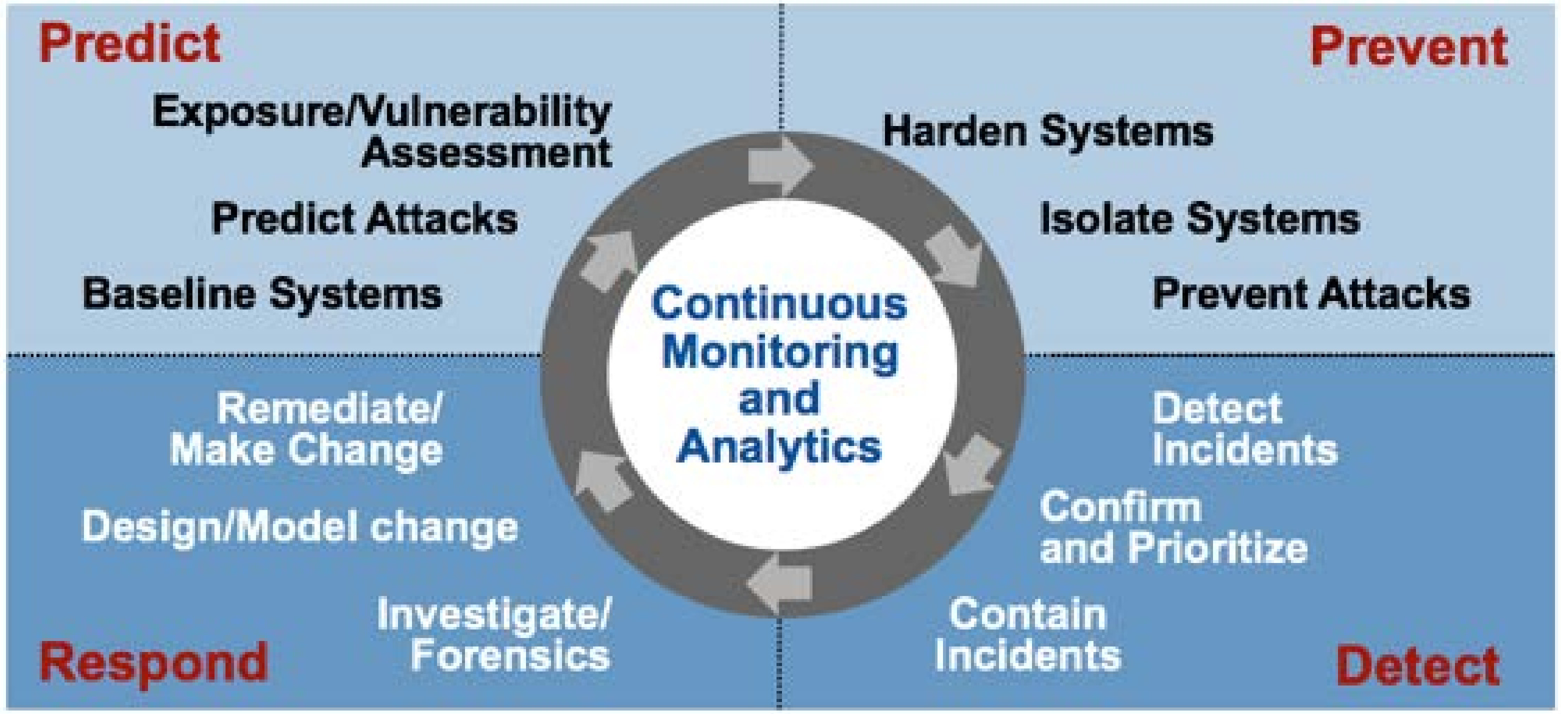
Threat and Vulnerability Information Support Risk Assessments

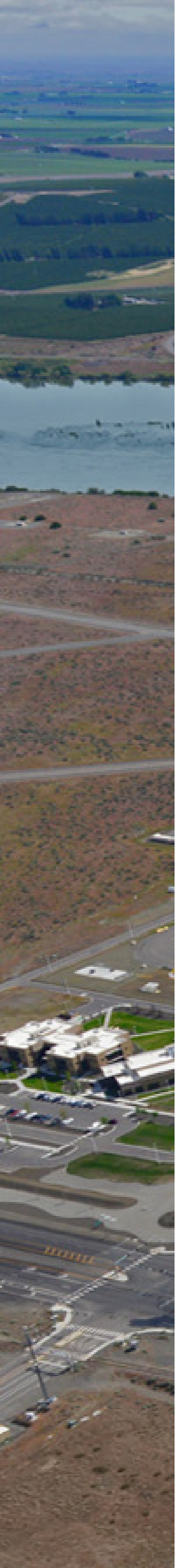
- Risk = Consequences x Probability of occurrence
- Probability can involve a number of factors:
  - Probability an attack will occur
  - Probability of it succeeding
  - Probability of worst-case consequences occurring (failure of safety systems, resiliency, etc.) -



Enhancing Security

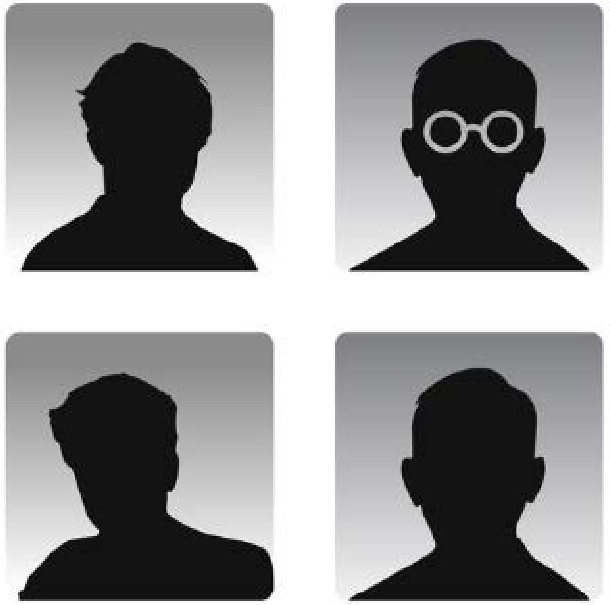
- Steps to take to enhance security.
  - **Predict**
  - **Prevent**
  - **Detect**
  - **Respond**





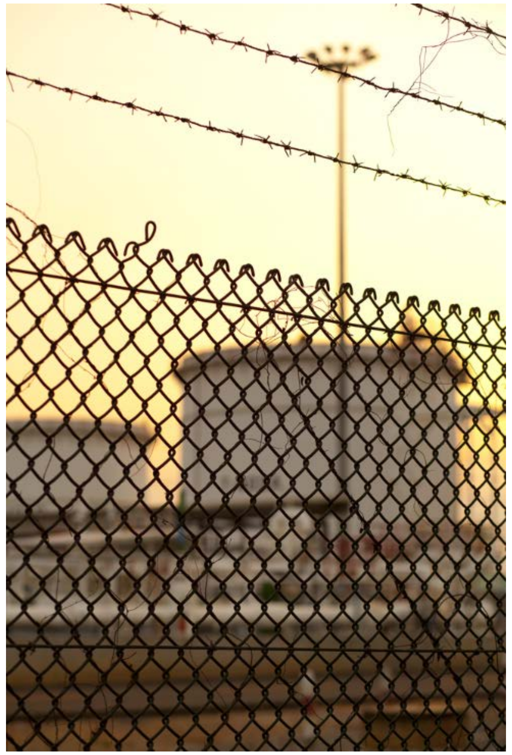
Predict

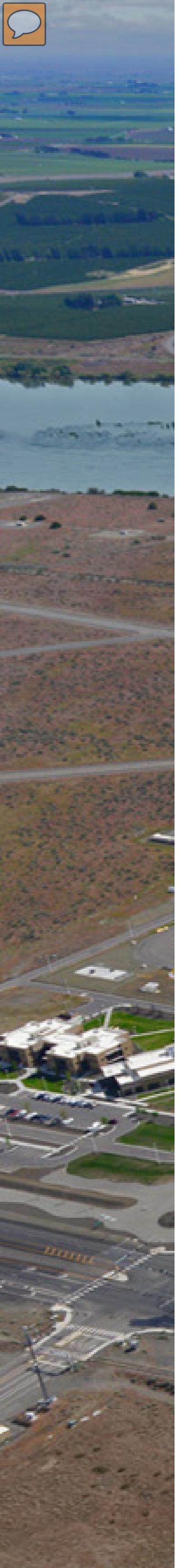
- Understand the threat environment
- Understand potential security vulnerabilities
- Understand the consequences of potential security incidents.



Prevent

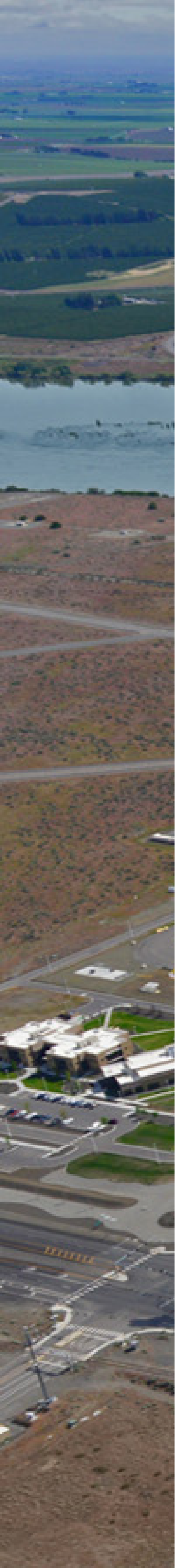
- Address security throughout the product lifecycle
- Implement cost-effective security controls to **deter** attackers (so as not to be seen as an easy target)
- Address, **delay**, and thwart attacks up to and including the design basis threat





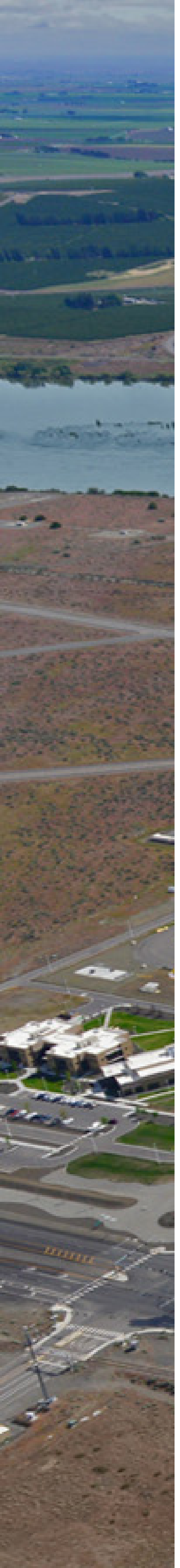
Detect

- 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 your staff on what to do.
- Plan to be resilient – to lessen the consequences.
- 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.



Pacific Northwest
NATIONAL LABORATORY

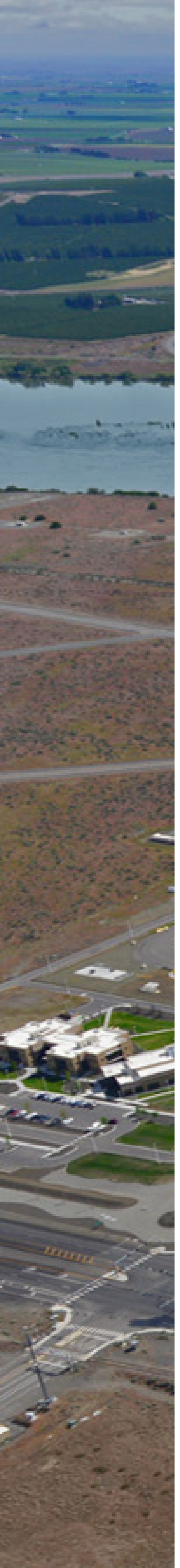
Thank you

Exercise A: Identifying Potential Security Threats along the Supply Chain -

Alpha Chemicals & Pharmaceuticals

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

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



In this exercise,

- We will introduce a Pharmaceutical and Specialty Chemical manufacturing facility and laboratory
- Will provide the facility details as well as its location, mission and background
- Details on supply chain steps
- Example scenarios and then identifying security threats….

Pacific Northwest
NATIONAL LABORATORY

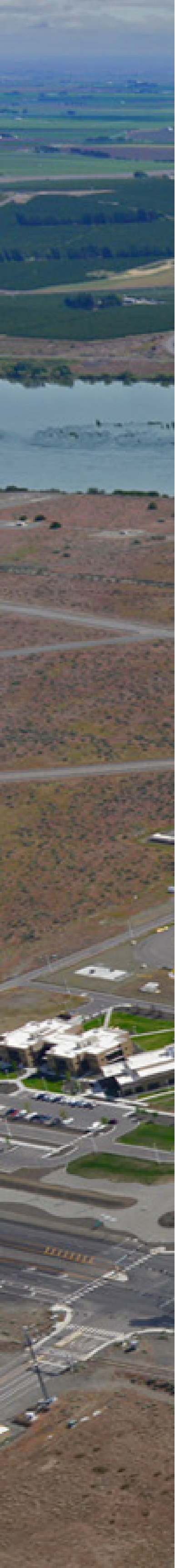
Dr. Radha Kishan Motkuri
Senior Principal Scientit

- 13 years at PNNL working in nanoporous materials, catalysis, sensing and security. (Ph.D. from CSIR-IICT/UH in 2003 with Dr. K.V. Raghavan)
- Five years supporting chemical and nuclear security projects in India/Bangladesh for the U.S. Department of State
- Published
  - **~92 peer-reviewed publications, >90** presentations.
  - **>3100 citations** with **H-index 28** (Google scholar)
- **15 international patents (9** USA patents/applications), 2 licences
- Received **2017 R&D 100 Award** in 2017 for thermal vapor-compression cooling technology.
- An editorial board member for the prestigious inorganic and material journals:

Inorganic Chemistry
including bioinorganic chemistry

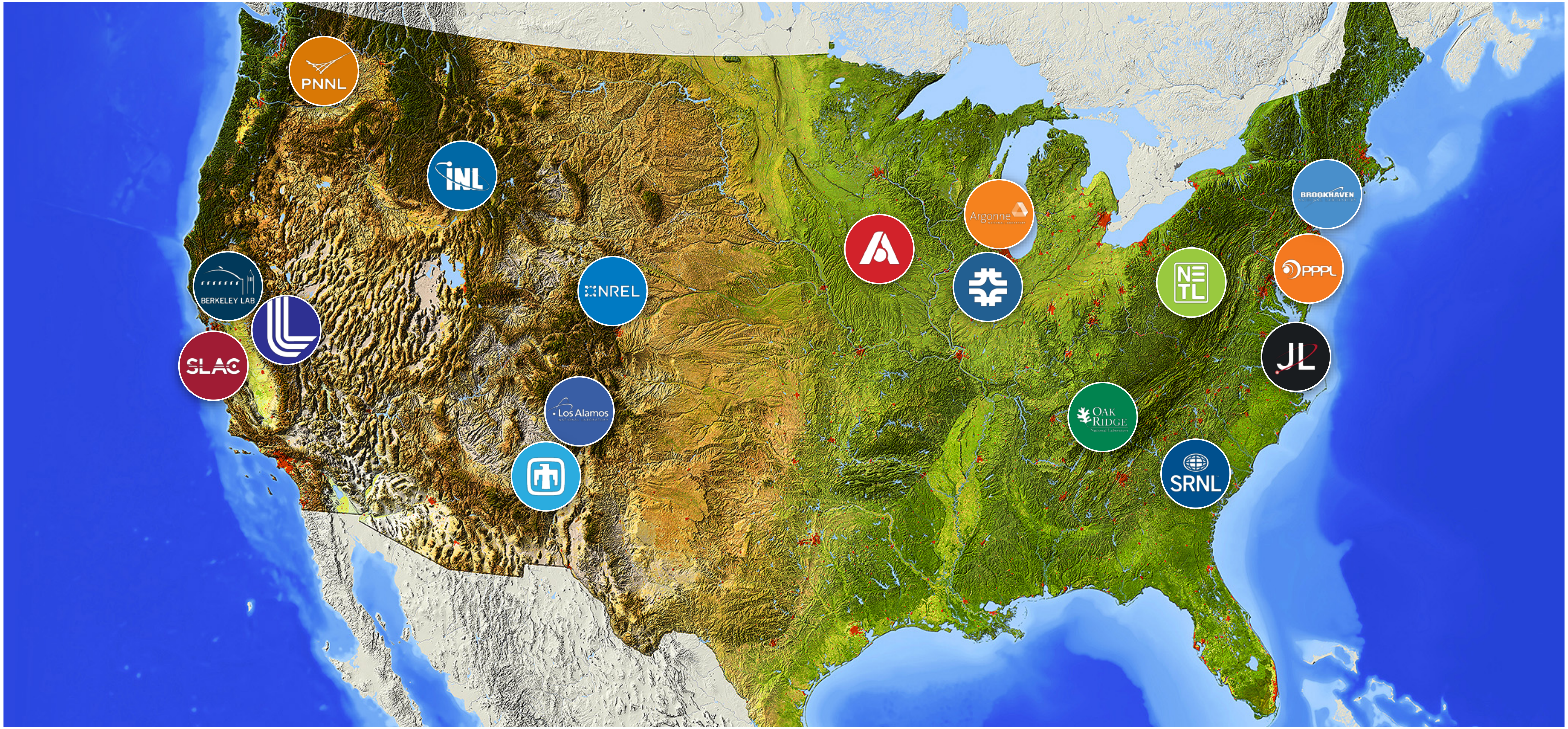
SCIENTIFIC REPORTS
nature publishing group npg

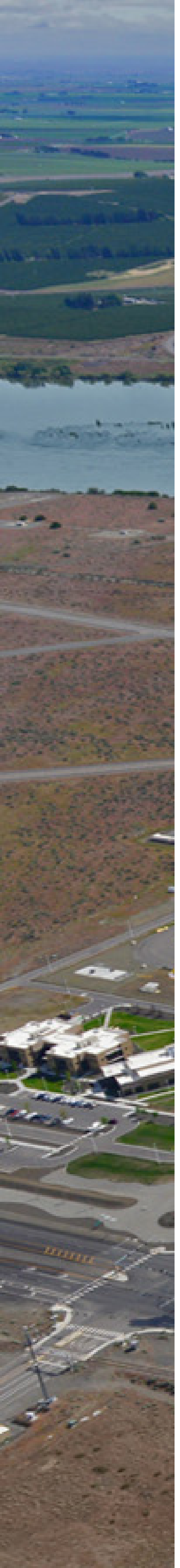
Inorganica Chimica Acta



Pacific Northwest
NATIONAL LABORATORY

PNNL is one of DOE’s 17 **national laboratories** that tackle critical scientific challenges





Pacific Northwest
NATIONAL LABORATORY

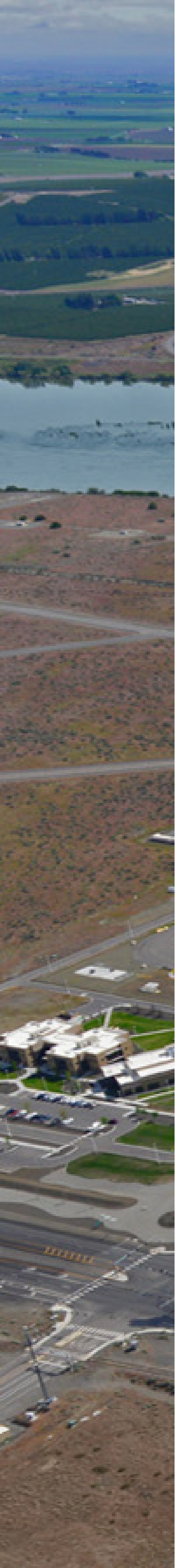
We are a regional, national, and international **scientific resource**

$1B Spending

4,700 Staff

265 Invention disclosures

1,193 Peer-reviewed publications



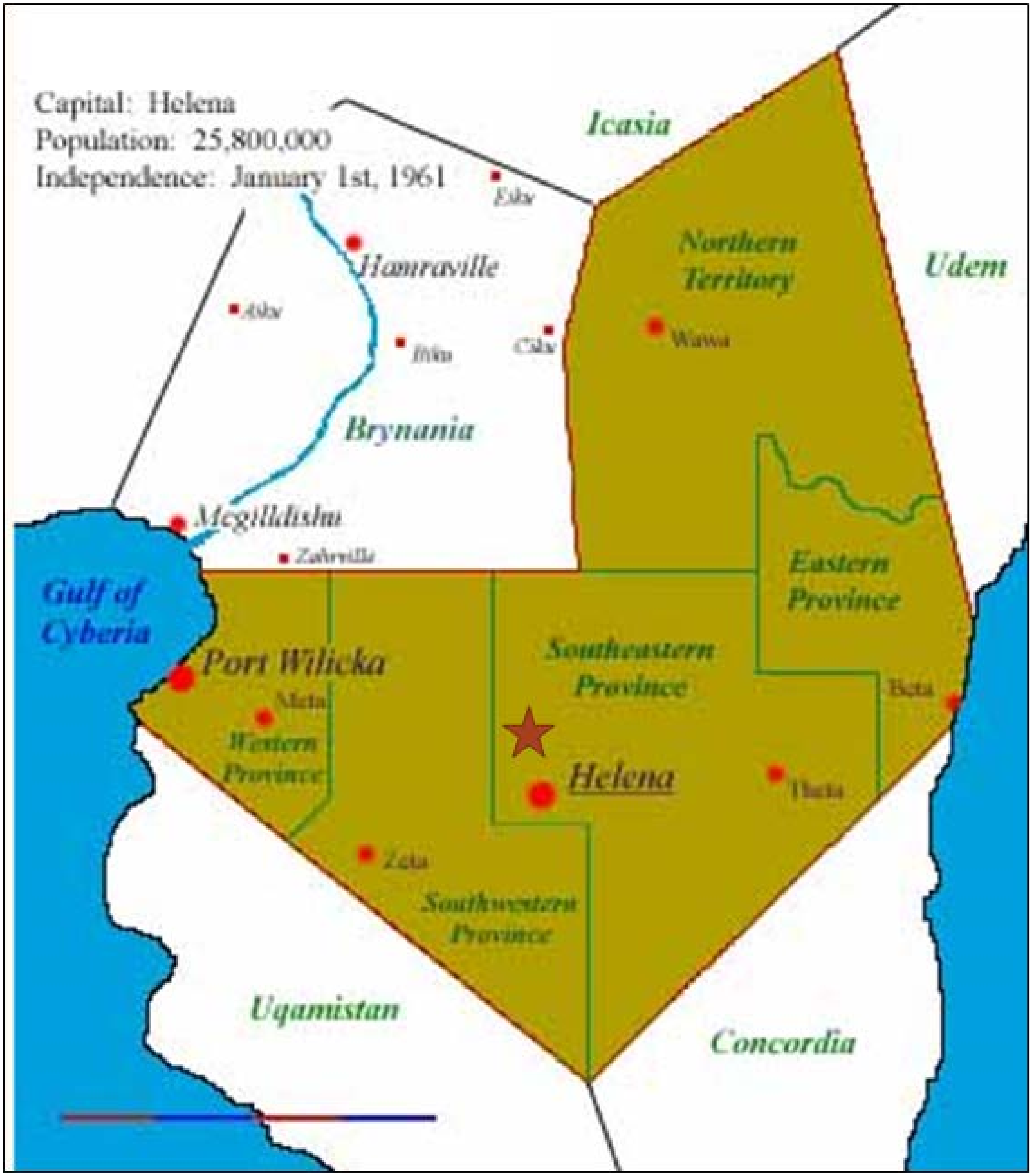
Welcome to Plant Alpha Chemicals & Pharmaceuticals

Plant Alpha

A Pharmaceutical and Specialty Chemical manufacturing facility and laboratory

Serving Norland and our community with distinction since 1923

Welcome to Alpha Chemicals & Pharmaceuticals : Background Information



- Located In the country of "Norland"
- Plant founded in 1923. 15 years ago it launched it's "21st Century" initiative.
- Motto: "*Putting Technology to Work to Benefit the People of Norland*".
- Employs 570 people.

Welcome to Alpha Chemicals & Pharmaceuticals:
Mission

Plant Alpha produces:

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

Welcome to Alpha Chemicals & Pharmaceuticals : Supply Chain

Plant Alpha

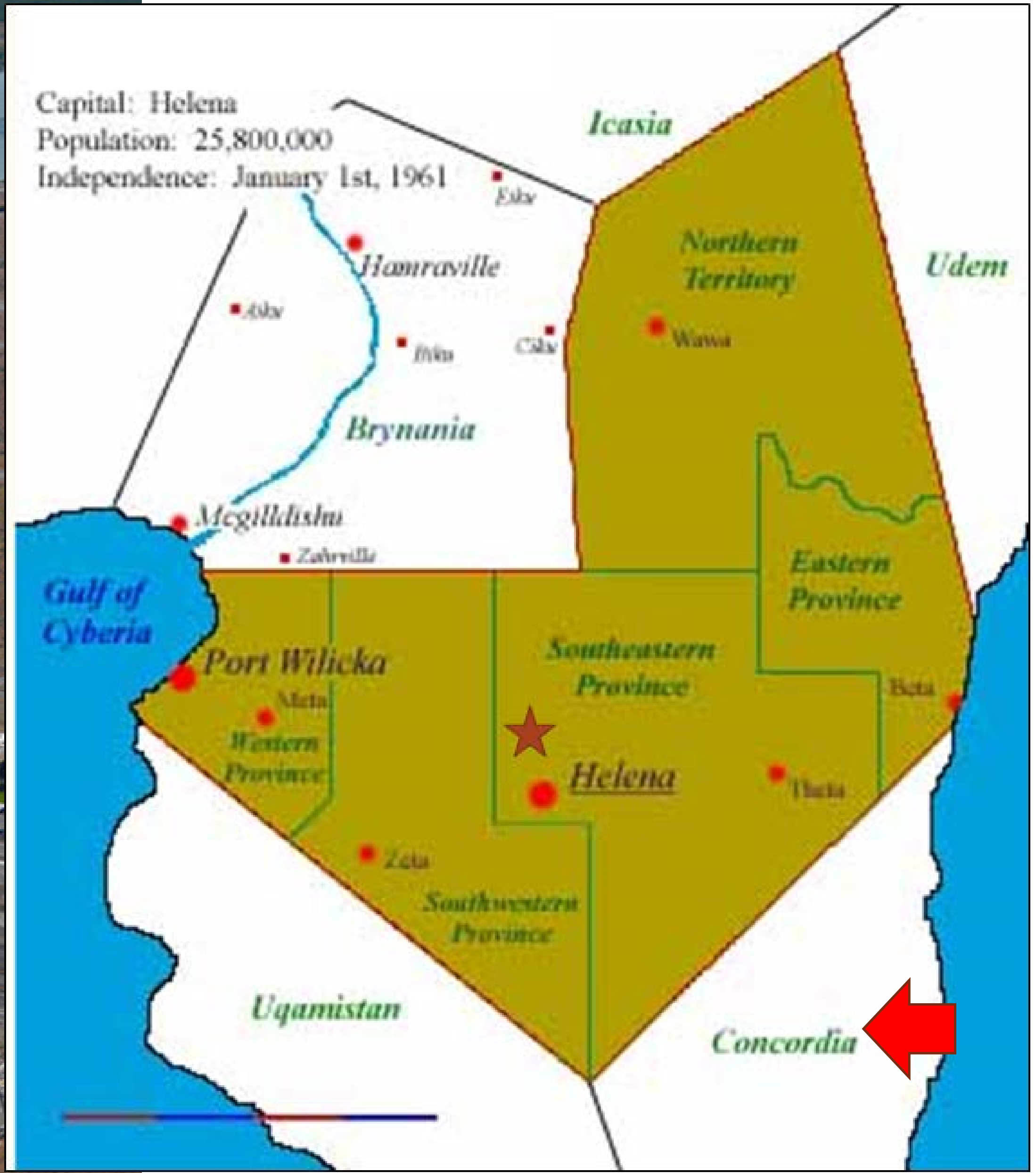
- manufactures and stores an array of pharmaceutical and chemical products.
- manufactures specialty/fine/custom/intermediate chemicals for its industry customers.
- This also includes dual-use, hazardous chemicals.
- Also, bulk materials, including hazardous chemicals, are shipped to Plant Alpha for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

Welcome to Alpha Chemicals & Pharmaceuticals : Supply Chain (Contd.)

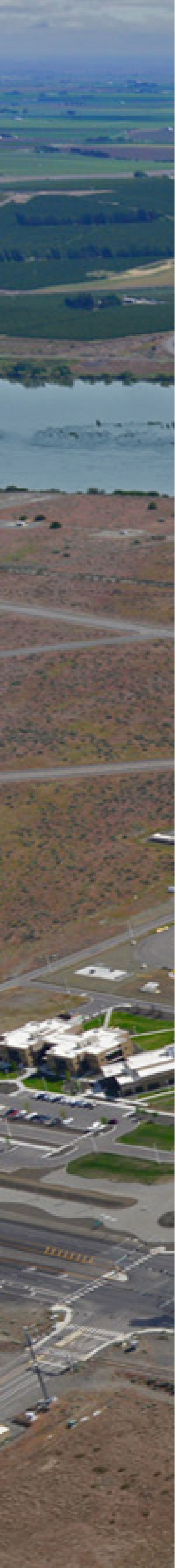
Pharmaceuticals and specialty chemicals (including dual-use chemicals), are shipped to customers for further processing and packaging.

- In the company office:
  - Procurement of products,
  - hiring,
  - sales of finished products,
  - billing and accounts receivable,
  - inventory management,
  - shipping, and
  - other business functions are performed

NORLAND : Relationships



- Norland has good relationships with most (but not all) of it neighbouring countries, including free trade agreements.
- Relationships with Concordia are strained,
- There is a serious dispute over offshore oil and gas resources in the waters bordering both countries.
- Trade with Concordia is very limited.
- Concordia’s military and national police may actively support Norland opposition groups based in Concordia, including a suspected terrorist organizations
- Organized crime groups are active in both Norland and Concordia.
- Smuggling from Concordia is a major problem. Smuggled items include drugs, electronics, and refugees.



Pacific Northwest NATIONAL LABORATORY

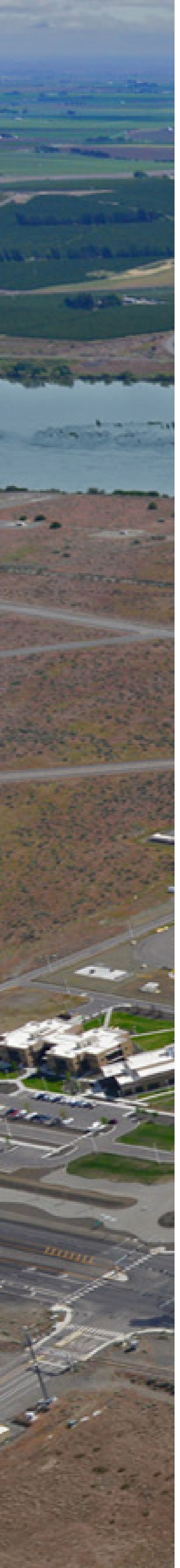
What are the Security Threats Facing Plant Alpha?

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

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

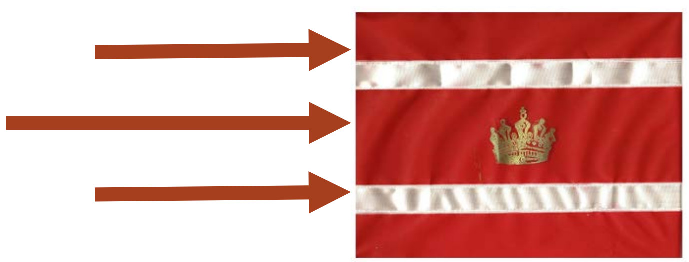
Supply Chain Steps

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



Pacific Northwest NATIONAL LABORATORY

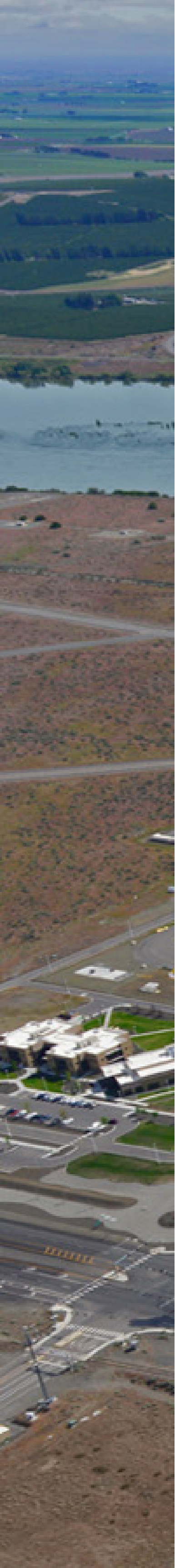
Example Scenario



A nation state mounts a cyberattack to sabotage the Plant Alpha during the manufacturing process, with the intention of destroying production and releasing hazardous materials into the environment.

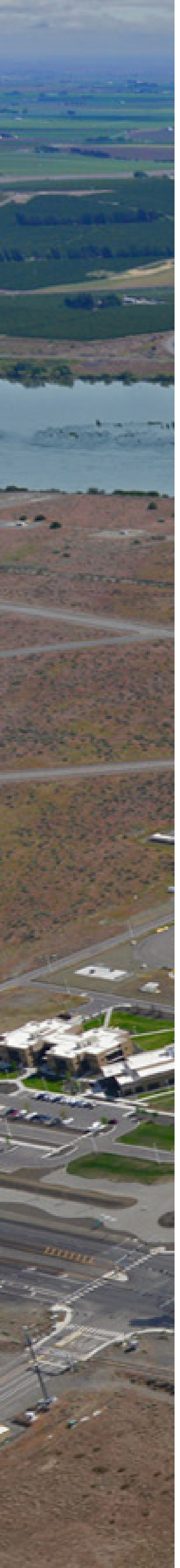
Step # **Activity**

1. The attackers recruit an experienced hacker
2. They acquire control system malware from the dark web
3. They send spear phishing emails to company executives
4. They wait for malware to be transferred to a Plant Alpha control system.
5. The malware "calls home" to let the attackers know it is installed.
6. The attackers activate the malware and maliciously operate the system
7. An explosion, fire, and chemical release occurs…



Scenario – You design the attack

- **Criminals want to hijack a shipment of pharmaceutical chemicals during their transport from Plant Alpha to a customer.**
- You are the leader of the criminal gang!
- You have to plan, and carry out the attack using the available threats or attack paths that you decide upon
- Put on your black hat and get ready to be the bad guy!



First Step – Potential Attack Scenarios

Option 1. Personnel Attack

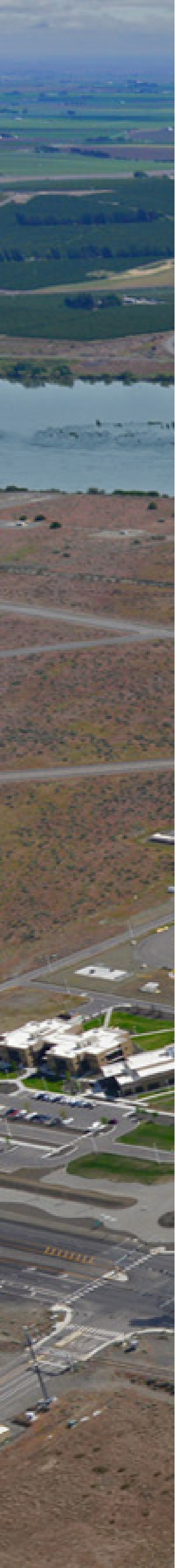
- Research public records for information on plant employees
- Identify a vulnerable plant employee
- Bribe/threaten a staff member to obtain information on the planned shipment of chemicals

Option 2. Cyberattack

- Recruit a hacker or hackers
- Obtain malware and mount a cyberattack and obtain access to shipping information
- Examine records to obtain information on the shipment of chemicals to customers

Option 3. Physical attack

- Break into the company offices at night
- Find the file cabinet with shipment information and search hardcopies
- Search hardcopies and obtain information of the shipment of chemicals to customers



Second Step in the Attack

Option 1. Personnel Attack

1a) Follow the truck as it leaves the plant

1b) Approach the driver at a rest stop

1c) Bribe/threaten the driver to transport the shipment of chemicals to your warehouse

Option 2. Cyberattack

2a) Alter the delivery address for a future the shipment

2b) Set up a plausible delivery location for the shipment (e.g., a small packaging facility)

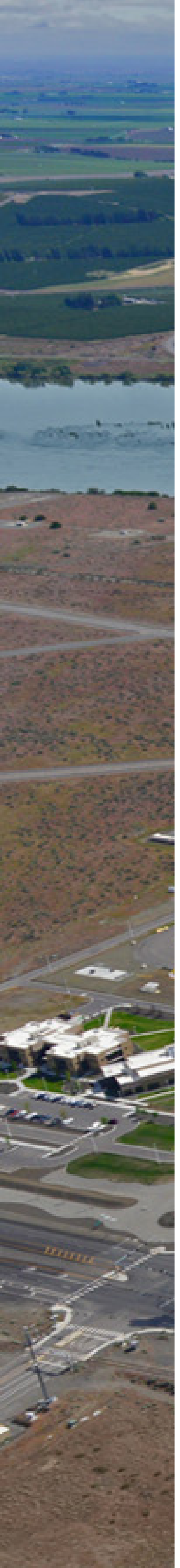
2c) Receive the shipment at your location.

Option 3. Physical attack

3a) Follow the truck as it leaves the plant

3b) Disable the driver when he stakes a rest break, take his keys, and steal the truck.

3c) Drive the shipment to your secret location



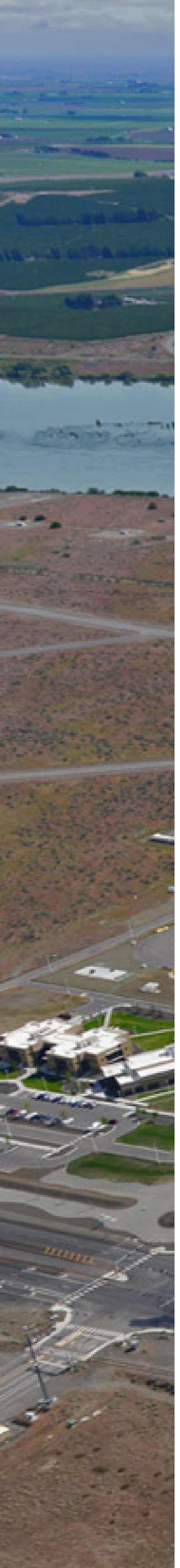
Final Step Questions – What Next?

What do you do with the stolen chemicals?

- Option 1: Sell them on the regional black market to another chemical company
- Option 2: Smuggle them out of the country
- Option 3: Ransom them back to the chemical company you stole them from

Closing Thought…

- **Thinking like an attacker** is a productive way to start identifying vulnerabilities, potential consequences, and types of security enhancements that may lower risks.
- This can help safeguard your pharmaceutical chemicals, your facility, your staff, and protect the safety and health of the public.



Pacific Northwest
NATIONAL LABORATORY

Thank you

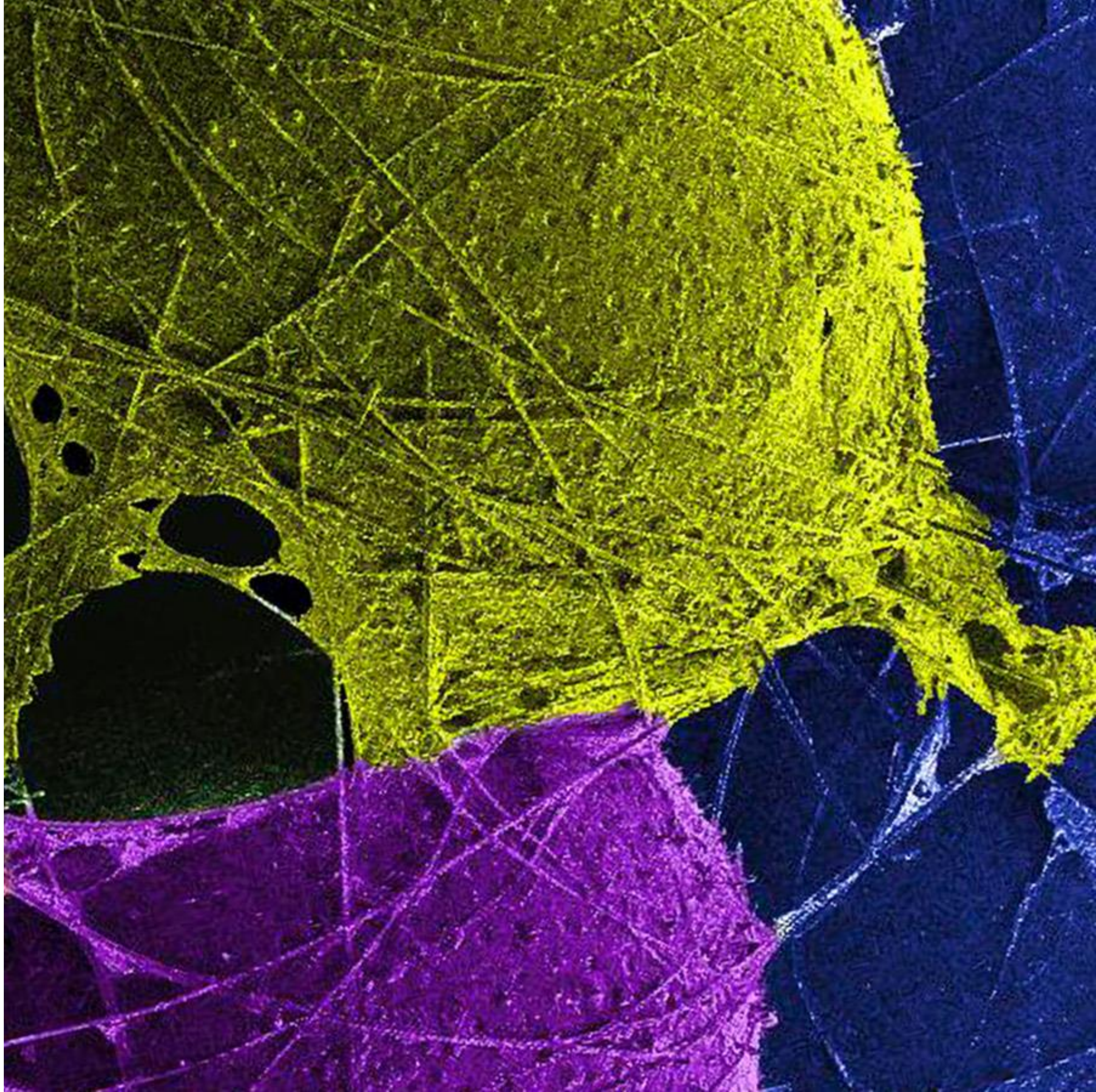
If you have any further questions:
Dr. Radha Kishan Motkuri
Radhakishan.Motkuri@pnnl.gov

L3:
Supply Chain Security and Customer Vetting

Part 1:
Background

John Cort
Cliff Glantz
Radha Kishan Motkuri
Pacific Northwest National Laboratory

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



Supply Chain Security and Customer Vetting: Background

- **Outline (Part 1, background)**

A. Background

- What is *supply chain security*? simple model vs. reality
- *Supply chain* ***security*** contrasted with *supply chain* ***management***.
- What are security requirements?
- What is customer vetting?
  - "Know your customer"
  - Understand *you* are the customer of your supplier

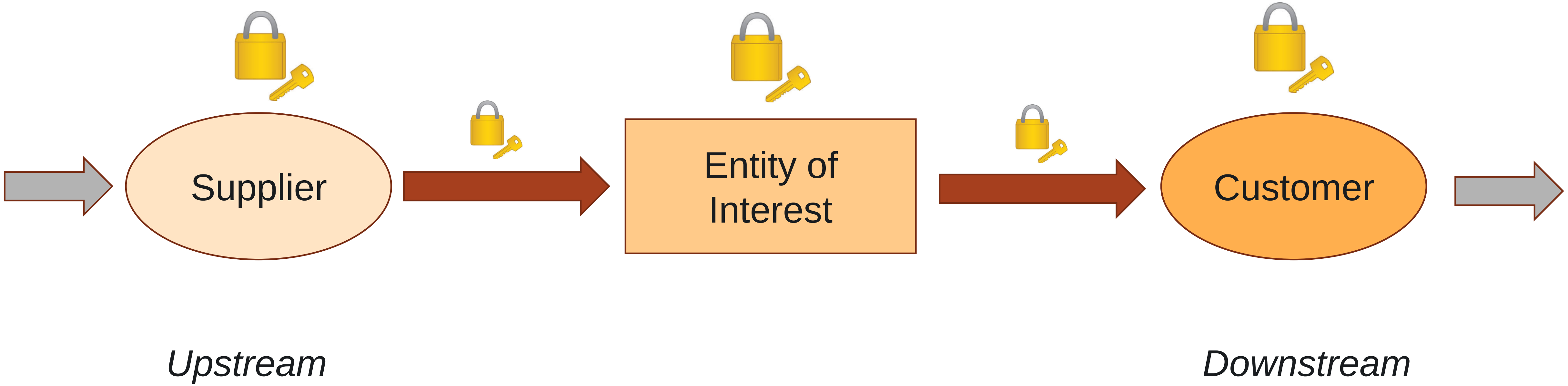
B. Case Studies

About the presenter

- **John R. Cort**
  - Senior Research Scientist (Chemist), Biological Sciences Division, PNNL, Richland, Washington, USA (since 1998).
  - Associate Research Professor, Washington State University, Institute of Biological Chemistry.
  - PhD in Organic Chemistry, University of Washington, Seattle, Washington
  - In addition to chemical security, research interests include:
    - Biomolecular NMR spectroscopy (structure/function elucidation of proteins, peptides, and other biological molecules)
    - Structure determination, chemical diversity, and biosynthesis of plant phenylpropanoids and other natural products
    - Characterization of biomass and the chemistry of biomass conversion processes
    - Biophysical characterization and metabolism of heterogeneous macromolecular pharmaceuticals

Supply Chain Security and Customer Vetting: Background

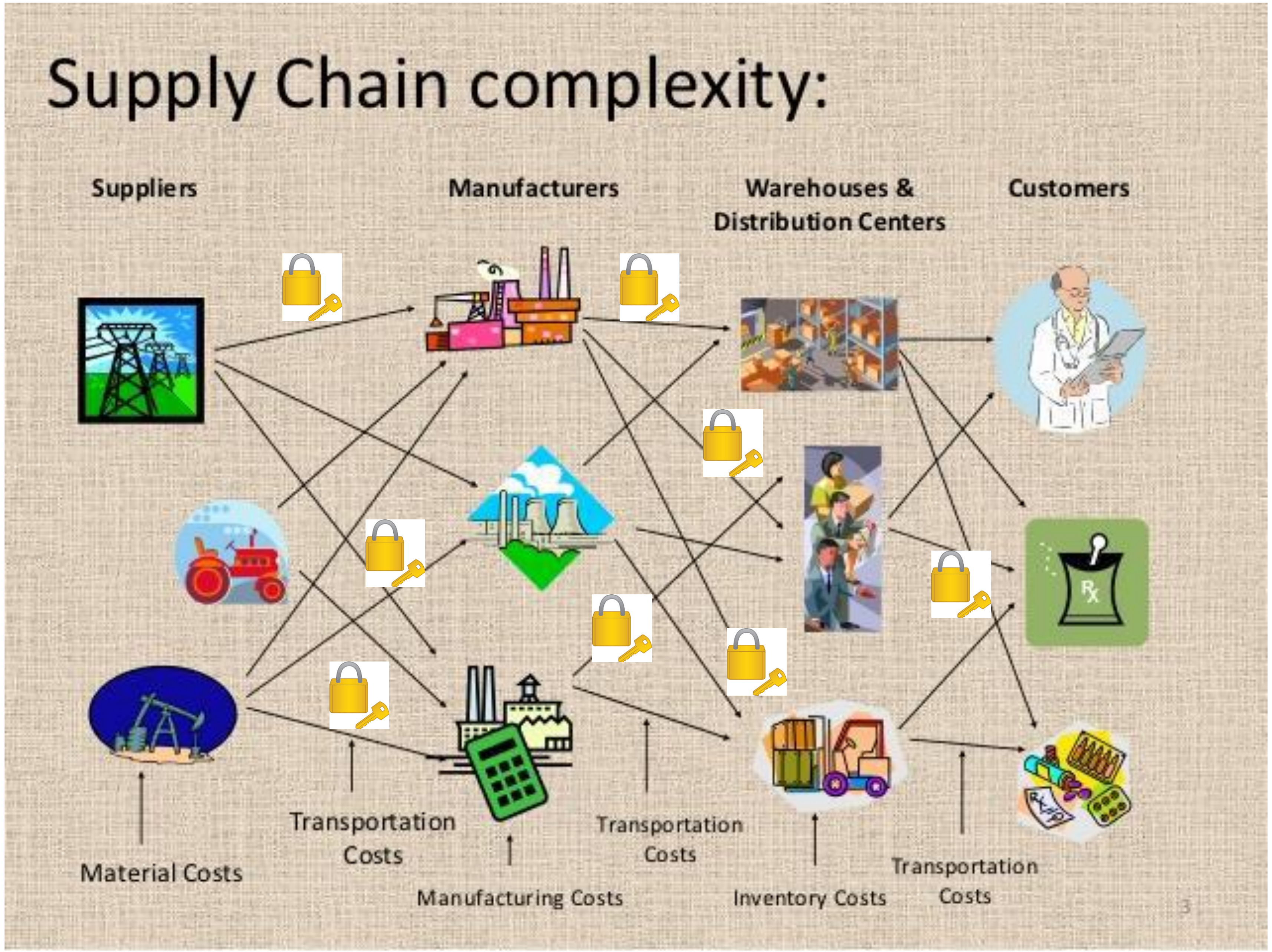
Simplified supply chain



Supply Chain Security and Customer Vetting: Background

Real supply chain:

Dynamic, complex network of relationships



Pacific Northwest NATIONAL LABORATORY

Supply Chain Security and Customer Vetting: Background

- **What is supply chain security? What is supply chain management?**
  - **Definition**: Supply chain ***security*** in this context is the maintenance of control over chemicals and materials at or transiting to/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.

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)

Supply Chain Security and Customer Vetting: Background

- **Why might an individual or group disrupt the supply chain or divert chemicals?**
  - Supply chain disruption / diversion:
    - Economic sabotage
    - Criminal mischief
    - Unintentional / accident / incompetence / negligence
    - Theft
    - **To obtain specific chemicals (or products, e.g. pharmaceuticals) of interest,** apart from their market value

Supply Chain Security and Customer Vetting: Background

- **Disruption**
  - Economic sabotage
  - Criminal mischief / vandalism
  - Unintentional / accident / incompetence / negligence

Supply Chain Security and Customer Vetting: Background

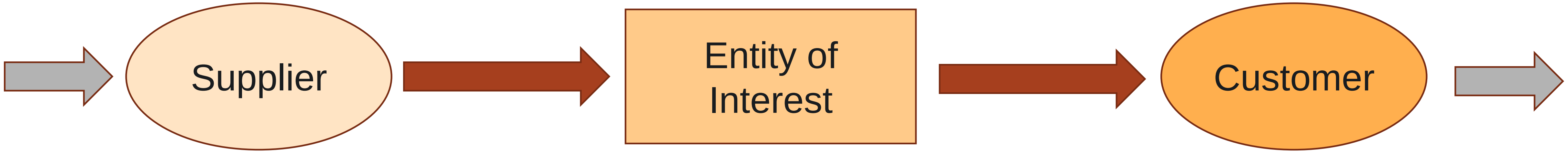
- **Diversion**
  - Unintentional / accident / incompetence negligence
  - Theft—chemicals have value and can be resold on the market; many are commodities and are not *easily* traceable.
  - Illicit activity—purchasing some chemicals in legitimate markets may be difficult or impossible for some parties, 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
    - Exchange (buy/sell) on open or lightly-regulated markets

Supply Chain Security and Customer Vetting: Background

- **What is customer vetting?**

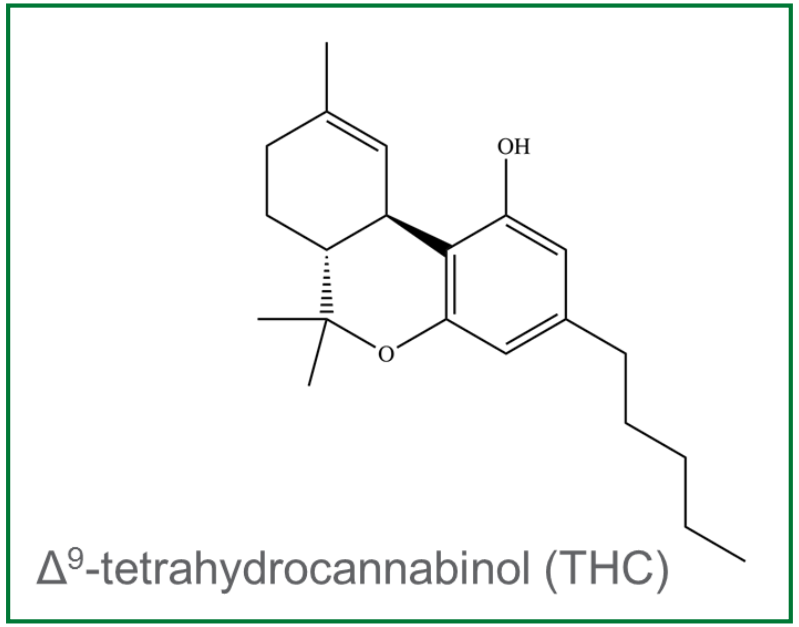
  (definition: vetting = *evaluating for approval or acceptance*)

  - Know the customer; recognize sometimes you are the customer
  - Why is the customer purchasing this chemical
  - Costs and benefits of vetting
  - Short-term vs. long-term benefits



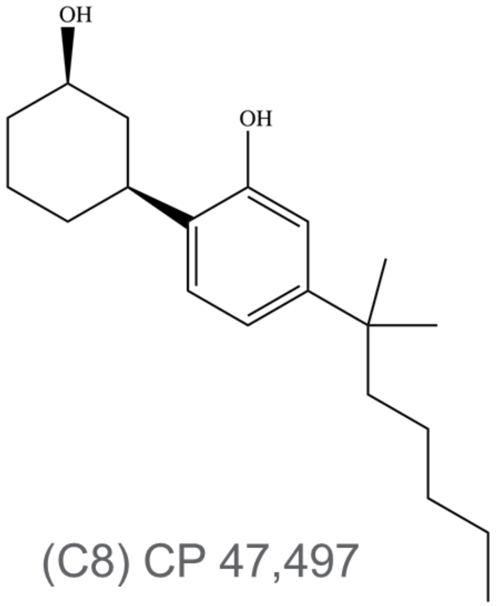
- A few case studies are presented here: synthetic cannabinoids, brodifacoum, fentanyl
- Best Practices for customer vetting covered in part 2 of this presentation

Case Study: Synthetic cannabinoids and other designer drugs

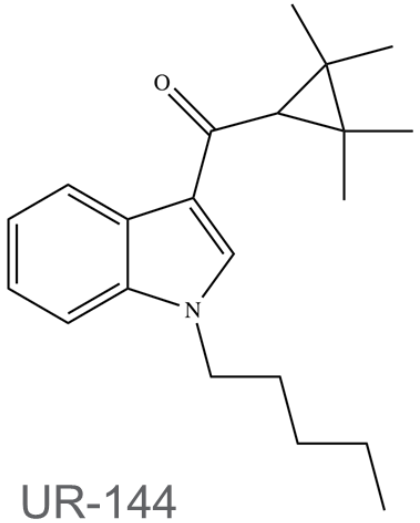


Δ^9-tetrahydrocannabinol (THC)

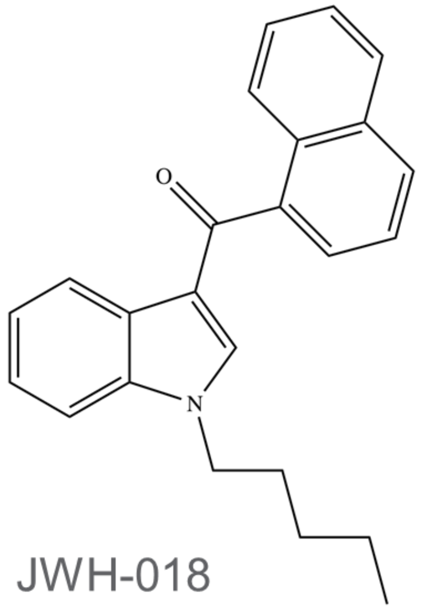
synthetic cannabinoids, no legitimate use



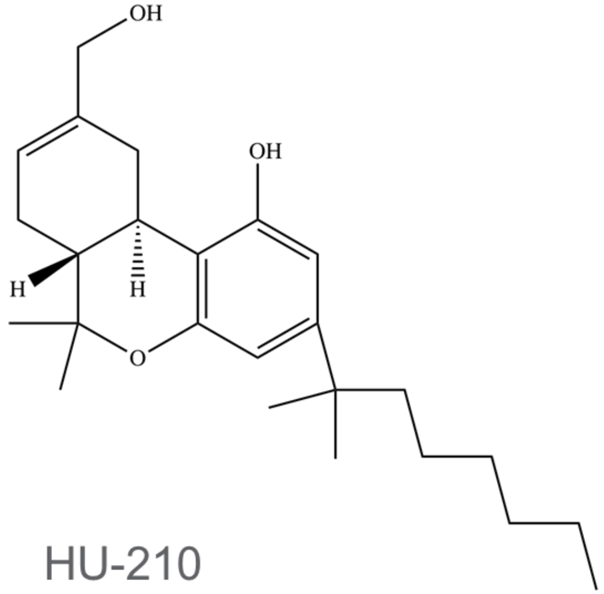
(C8) CP 47,497



UR-144

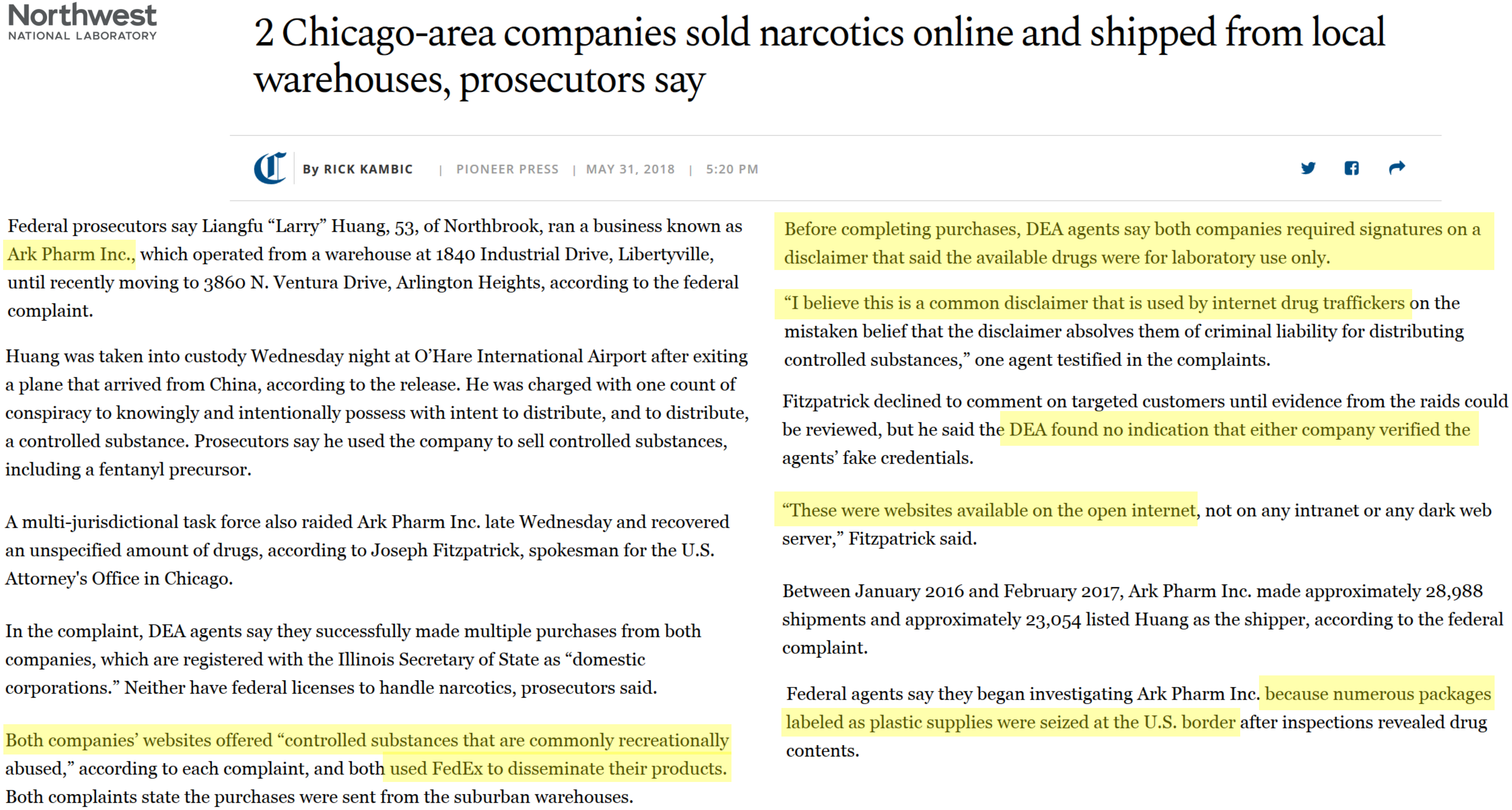


JWH-018



HU-210

Case Study: novel amphetamines (2018)



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

By RICK KAMBIC | PIONEER PRESS | MAY 31, 2018 | 5:20 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.

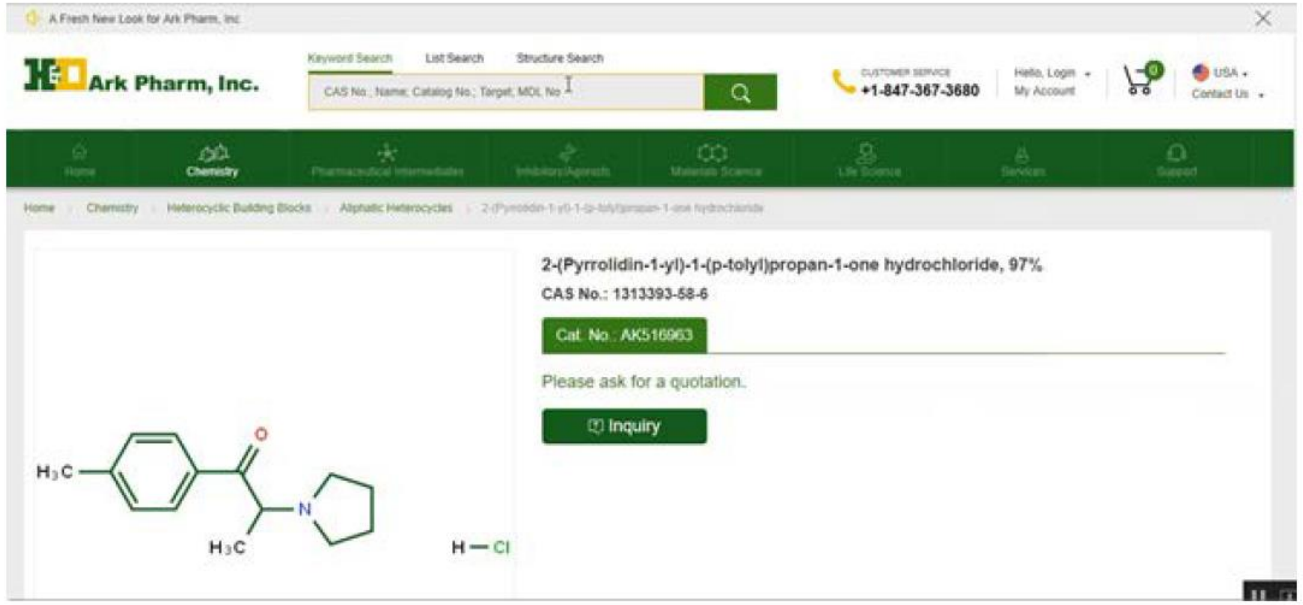
"I believe this is a common disclaimer that is used by internet drug traffickers on the mistaken belief that the disclaimer absolves them of criminal liability for distributing controlled substances," one agent testified in the complaints.

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.

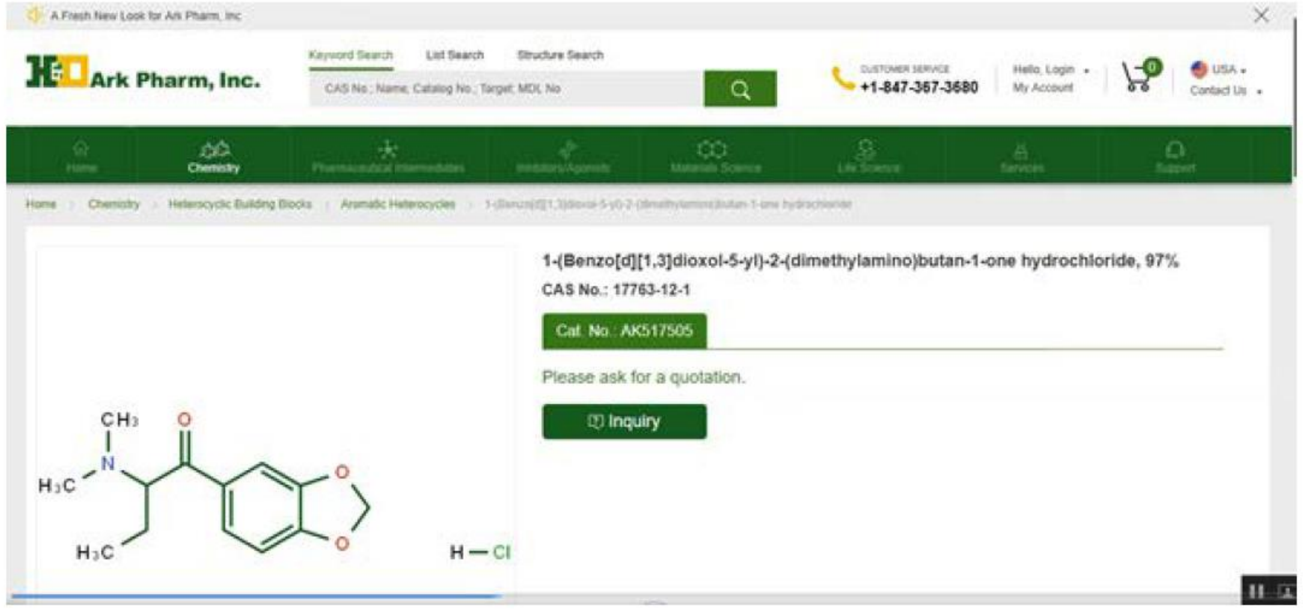


2-(Pyrrolidin-1-yl)-1-(p-tolyl)propan-1-one hydrochloride, 97%

CAS No.: 1313393-58-6

Cat. No.: AK516963

Please ask for a quotation.



1-(Benzo[d][1,3]dioxol-5-yl)-2-(dimethylamino)butan-1-one hydrochloride, 97%

CAS No.: 17763-12-1

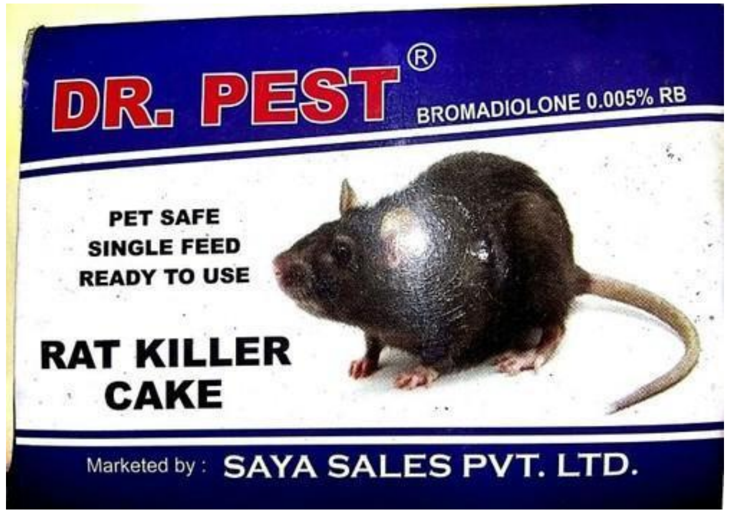
Cat. No.: AK517505

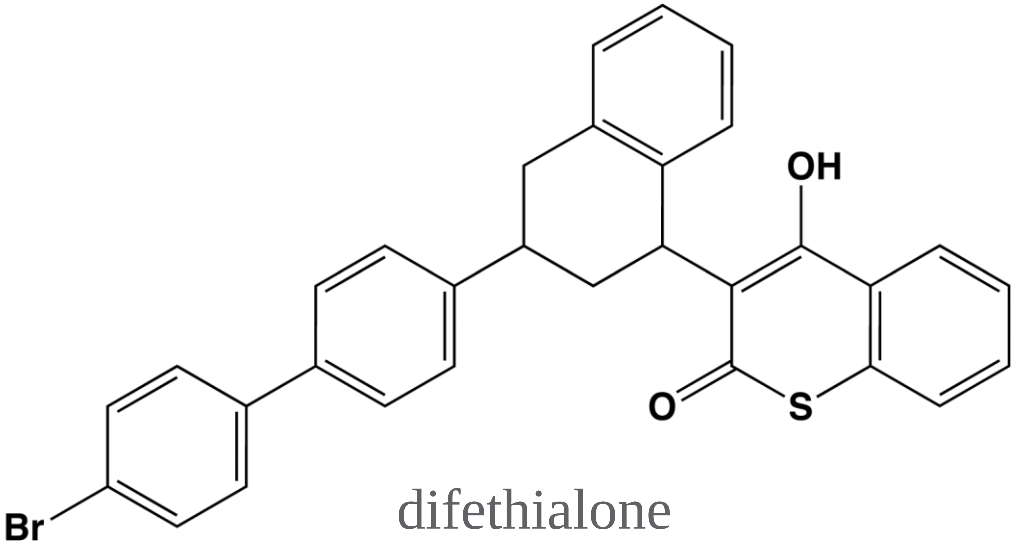
Please ask for a quotation.

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

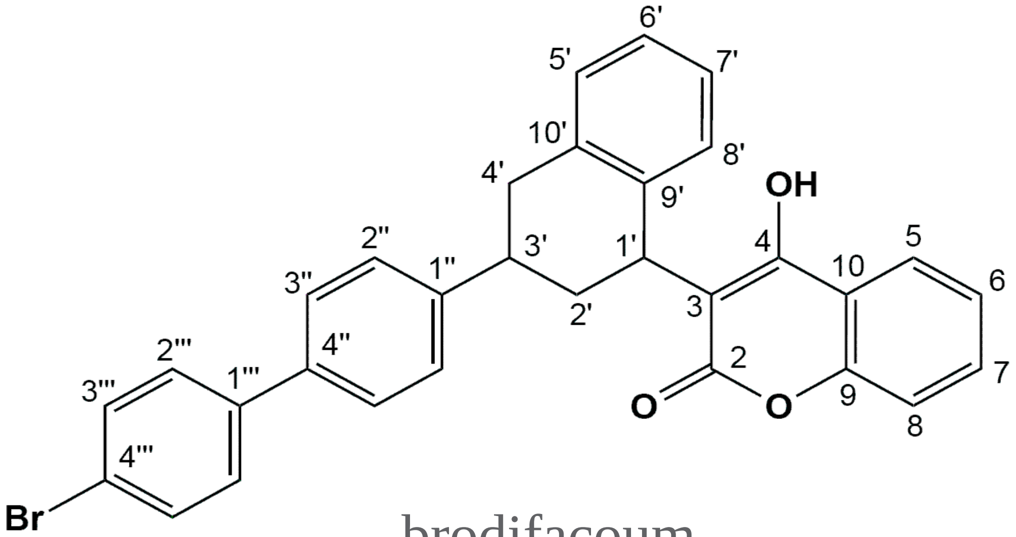
Pacific Northwest
NATIONAL LABORATORY

Case Study: Brodifacoum and superwarfarins





difethialone



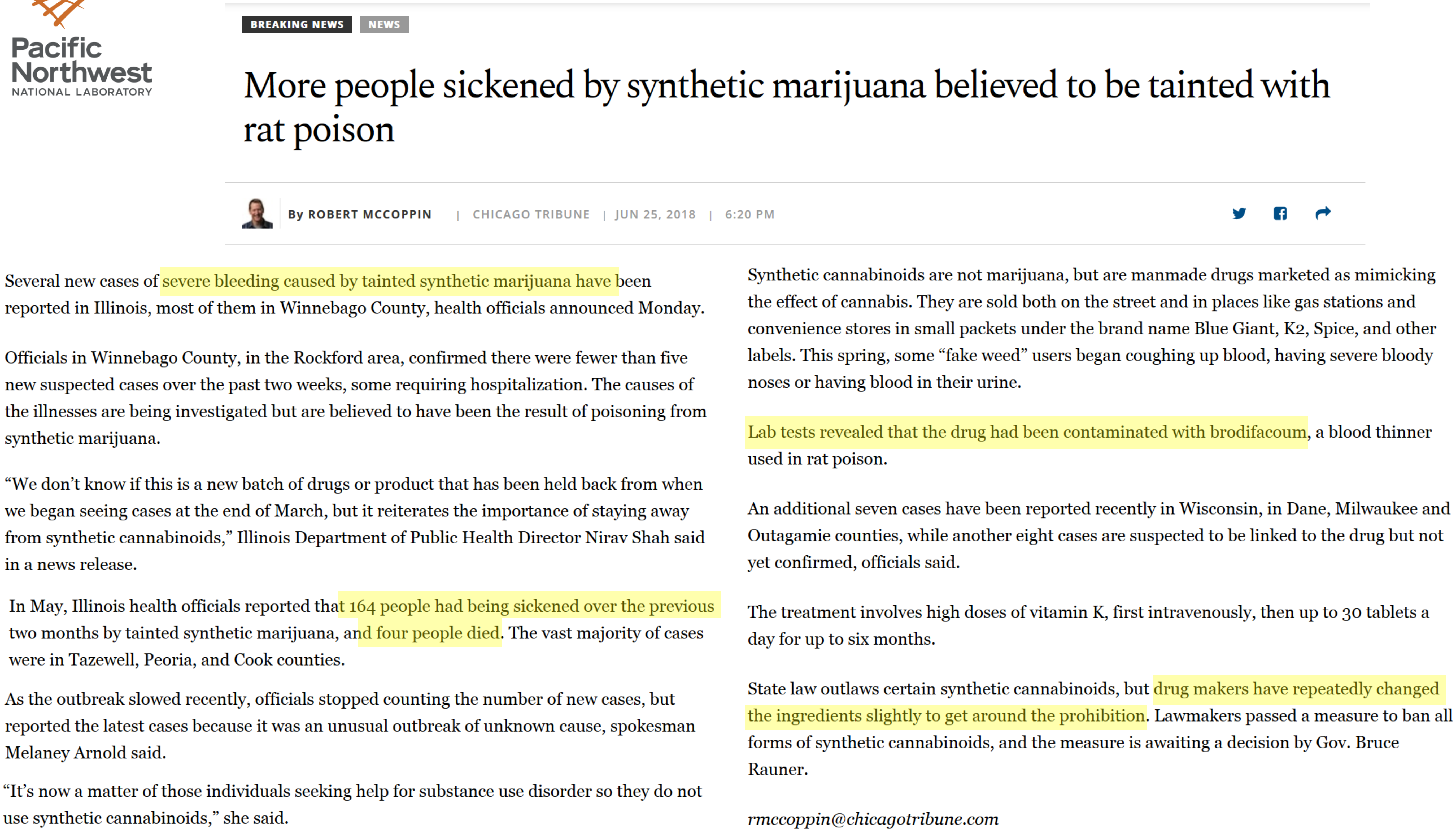
brodifacoum

"superwarfarins":

Highly toxic anticoagulant vitamin K epoxide reductase inhibitors

Very low concentration in baits: 0.005% by weight

Pacific Northwest
NATIONAL LABORATORY



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.

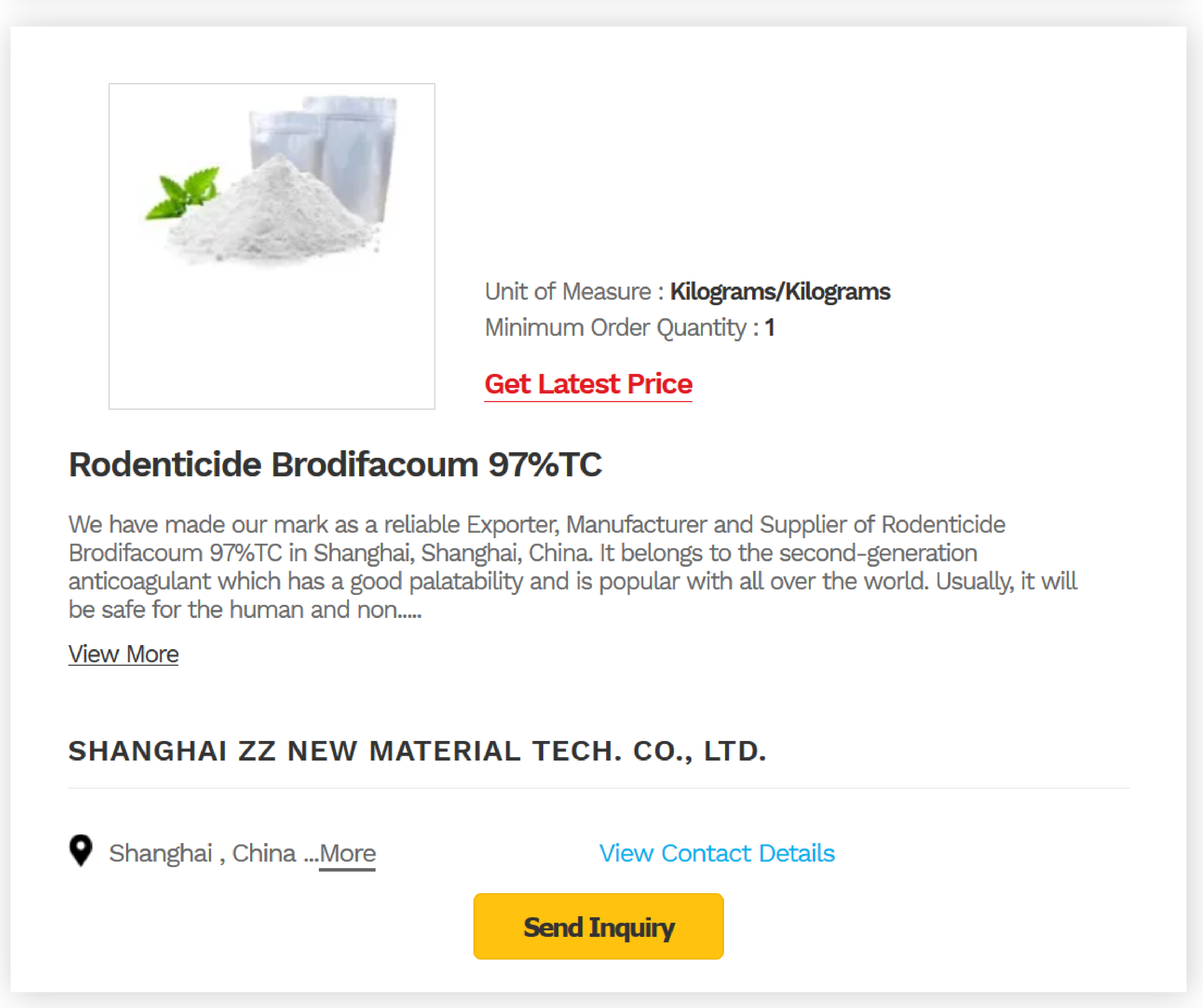
An additional seven cases have been reported recently in Wisconsin, in Dane, Milwaukee and Outagamie counties, while another eight cases are suspected to be linked to the drug but not yet confirmed, officials said.

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

Case Study: Brodifacoum and superwarfarins



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

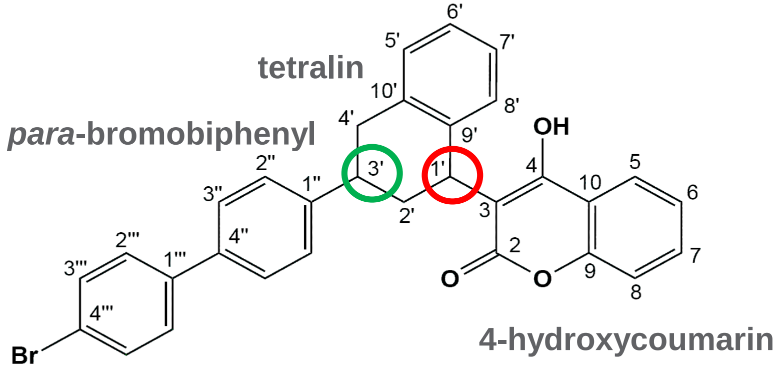
Pacific Northwest NATIONAL LABORATORY

Supply Chain Security and Customer Vetting: Driver for Chemical Forensics and Attribution

- **Traceability of chemicals after diversion**
  - Even pure chemical compounds 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—traceability of chemicals
  - Relies on stable isotope ratios, impurity profiles, stereoisomer distributions, and other intrinsic and extrinsic *attribution signatures*
  - Motivation for development of methods comes from potential outcomes when there are deficiencies in supply chain security

Chemical Forensics of Brodifacoum

- **Chemical Forensics:** tracing chemicals for source attribution and sample matching



Key to sources

△ A: Germany

🟪 B: US

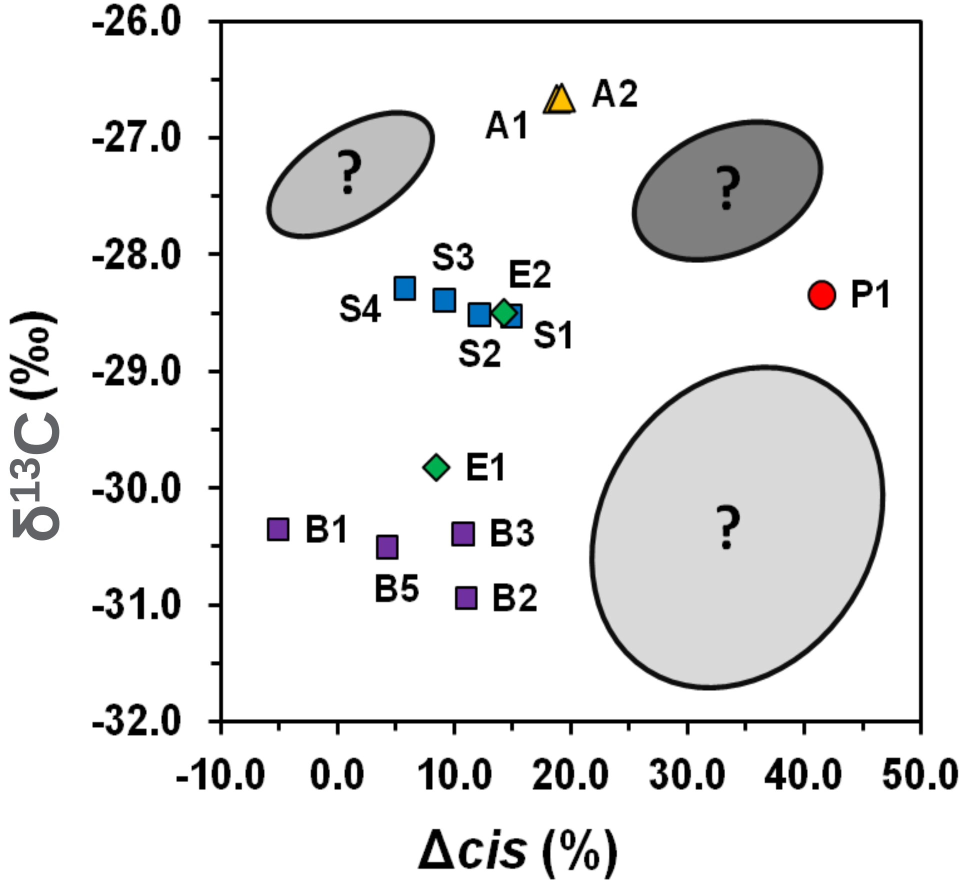
🟦 S: UK

🔴 P: Asia

◆ E: US EPA, attr. to B (US) & S (UK)

(numbers are different batches)

? = *other plausible parameter space*



IRMS: James Moran & Helen Kreuzer, PNNL

Case Study: fentanyl and fentanyl derivatives, dual/multi-use pharmaceuticals

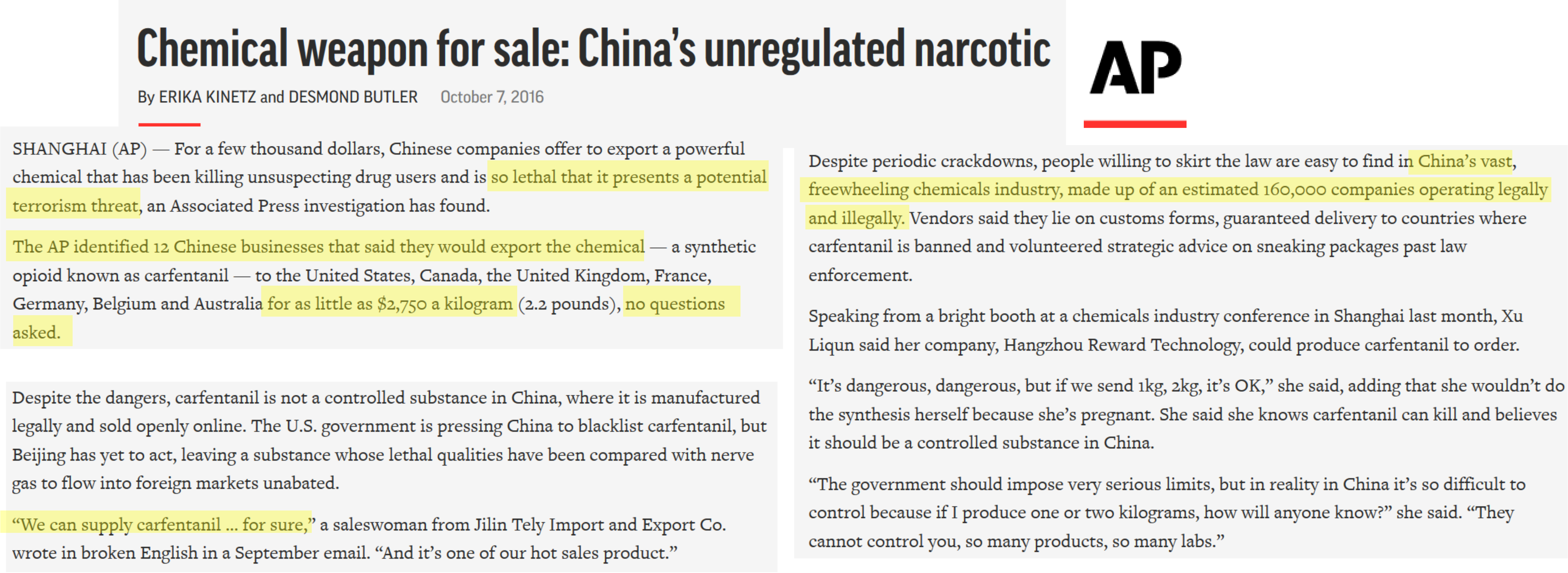
- **Fentanyl and fentanyl derivatives: essential drugs for medicine (anesthesia and analgesia)**

PAR PHARMACEUTICAL
NDC 49884-764-78
℞ only
Fentanyl Transdermal System 100 mcg/h
In vivo delivery of 100 mcg/h fentanyl for 72 hours
Each transdermal system contains: 10 mg fentanyl and 0.4 mL alcohol USP
DO NOT USE IF SEAL ON POUCH IS BROKEN
KEEP OUT OF REACH OF CHILDREN
five (100 mcg/h) systems
ONLY for pain requiring opioid medicine around-the-clock

Pacific Northwest NATIONAL LABORATORY

Case Study: fentanyl and fentanyl derivatives, dual/multi-use pharmaceuticals

- **Fentanyl and fentanyl derivatives: drugs of abuse**
  - ✓ Highly potent and addictive, available through batch custom fine chemical synthesis



Chemical weapon for sale: China's unregulated narcotic

By ERIKA KINETZ and DESMOND BUTLER October 7, 2016

AP

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 12 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.

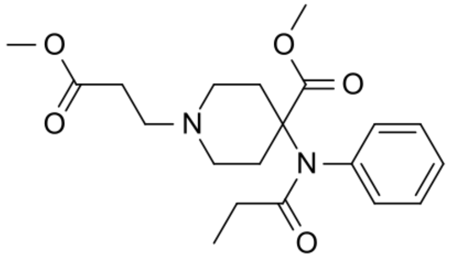
"The government should impose very serious limits, but in reality in China it's so difficult to control because if I produce one or two kilograms, how will anyone know?" she said. "They cannot control you, so many products, so many labs."

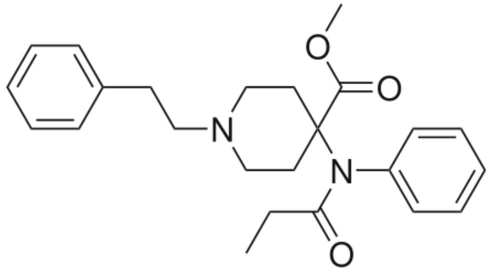
Case Study: fentanyl and fentanyl derivatives, dual/multi-use pharmaceuticals

- **Fentanyl and fentanyl derivatives: weapons / incapacitating agents**

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.

Journal of Analytical Toxicology 2012;36:647–656
doi:10.1093/jat/bks078 Advance Access publication September 20, 2012

Case Report

Analysis of Clothing and Urine from Moscow Theatre Siege Casualties Reveals Carfentanil and Remifentanil Use

James R. Riches, Robert W. Read, Robin M. Black, Nicholas J. Cooper and Christopher M. Timperley*

Detection Department, Defence Science and Technology Laboratory (Dstl), Porton Down, Salisbury, Wiltshire, SP4 0JQ, UK

*Author to whom correspondence should be addressed. E-mail: cmtimperley@dstl.gov.uk

On October 26, 2002, Russian Special Forces deployed a chemical aerosol against Chechen terrorists to rescue hostages in the Dubrovka theatre. Its use confirmed Russian military interest in chemicals with effects on personnel and caused 125 deaths through a combination of the aerosol and inadequate medical care. This study provides evidence from liquid chromatography–tandem mass spectrometry analysis of extracts of clothing from two British survivors, and urine from a third survivor, that the aerosol comprised a mixture of two anaesthetics—carfentanil and remifentanil—whose relative proportions this study was unable to identify. Carfentanil and remifentanil were found on a shirt sample and a metabolite called norcarfentanil was found in a urine sample. This metabolite probably originated from carfentanil.

Introduction

On October 23, 2002, Chechen terrorists seized the Melnikov Street Theatre in Moscow during a sell-out performance of the musical "Nord-Ost," taking over 800 hostages and demanding immediate and unconditional withdrawal of Russian troops from Chechnya. The siege ended in the early morning of October 26 after a Special Forces unit belonging to the Russian Federal Security Service (FSB) pumped a chemical aerosol into the building and stormed it. At least 33 terrorists and 129 hostages died during or shortly after the raid. The terrorists were shot dead after falling unconscious to the effects of the aerosol, explosives strapped to them were removed, and a bomb in the auditorium was deactivated. Two hostages were shot by the terrorists, while 125 died through a combination of the aerosol and inadequate medical treatment following the rescue. Medical treatment of the casualties was complicated because the Russian government did not disclose the composition of the aerosol. The head of the Moscow Public Health Department announced that all but one of the hostages killed in the raid had died of the effects of the gas, which was surmised to comprise an anaesthetic or chemical warfare agent. Foreign embassies in Moscow issued official requests for more information on the aerosol to aid treatment, but were ignored. Armed guards were posted at Moscow hospitals and doctors were ordered not to release any of the casualties. Refusing to disclose the content of the aerosol used, the Russian government informed the United States Embassy on October 28 about some of its effects. Based on this information and examination of some of the casualties, doctors concluded that the aerosol had contained a morphine derivative. On October 30, Russia responded to increasing domestic and international pressure with a statement by its Health Minister, Yuri Shevchenko (1), who identified the aerosol as that of a fentanyl derivative, although the precise composition was not disclosed. Shevchenko stated that fentanyl was an anaesthetic that fell into the category of non-lethal medical preparations and that the troops had not used any substances prohibited by the Chemical Weapons Convention.

After the siege, various hypotheses were proposed to account for the Russian explanation that an aerosolised form of fentanyl had been used: a mixture of fentanyl and the anaesthetic gas halothane (2), or fentanyl alone, for example, but these ideas were soon discredited based on the insufficient potency of these chemicals (2–4). A recent European Court of Human Rights report (5) of a legal case against Russia, lodged by 64 Russians that survived or lost relatives in the siege, provides an authoritative account of events. Therein the Russian Government revealed that the aerosol was a "mixture based on derivatives of fentanyl" and "a composite chemical compound of general narcotic action," suggesting more than one component. However, the composition was not disclosed to the court. This case report provides evidence from the analysis of clothing from two British survivors, and urine from a third survivor with a Russian name, that the aerosol comprised a mixture of two fentanyls, carfentanil and remifentanil.

Case History

Clothing and blood samples from British survivors held in the theatre throughout the siege were received at the Defence Science and Technology Laboratory (Dstl) Porton Down on the afternoon of October 28, 2002, for analysis. A jumper and leather jacket from Casualty 1 (male), a shirt from Casualty 2 (female), and two blood samples from each casualty, were provided. The blood samples had been taken approximately 19 h (Casualty 1) and 12 h (Casualty 2) after the chemical aerosol had been released into the theatre. The casualties had been near an exit door, which appears to have been a major factor in their survival. They were among the first casualties evacuated from the theatre after it was assaulted.

Both casualties were interviewed separately by British police on November 12 and 13, 2002. The following information is taken from these interviews (6): During the morning of October 26, the hostage-takers pointed to a white aerosol that appeared to be emerging silently from the balcony wall. The aerosol—dense, white and cloudy—spread evenly and descended slowly. Casualty 1 claimed it had an indescribable smell, Casualty 2 remembered it as odourless; people were not coughing or spluttering, even on the balcony. Both casualties knelt on the floor and covered their faces with their clothing. From first spotting the aerosol to being overcome by it took "10–30 seconds" for Casualty 1 and "at least 30 seconds" for

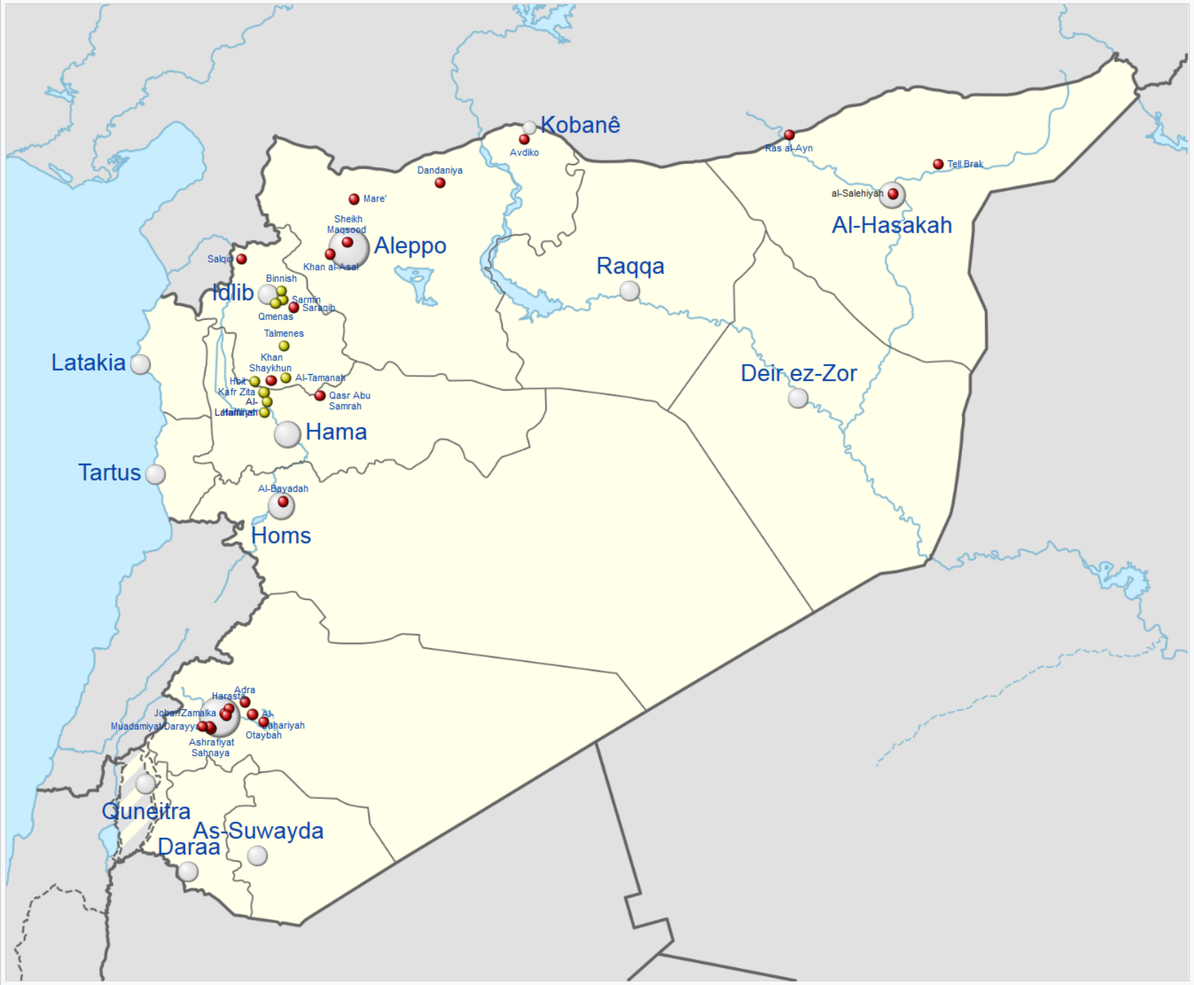
Riches *et al*., Analysis of clothing and urine from Moscow theatre siege casualties reveals Carfentanil and Remifentanil use. *J. Analytical Toxicology*, 2012

Case Study: CWA in Syria

- Alleged use of Sarin and chlorine in Syrian Civil War

- Were chlorine and/or Sarin precursors through the chemical supply chain?

- Hypothetically, could better supply chain security and customer vetting have led to a different outcome?



The map marks the position of reported chemical weapons attacks in the Syrian Civil War. Yellow markers indicate chlorine attacks. Red indicate a more deadly chemical weapon agent.

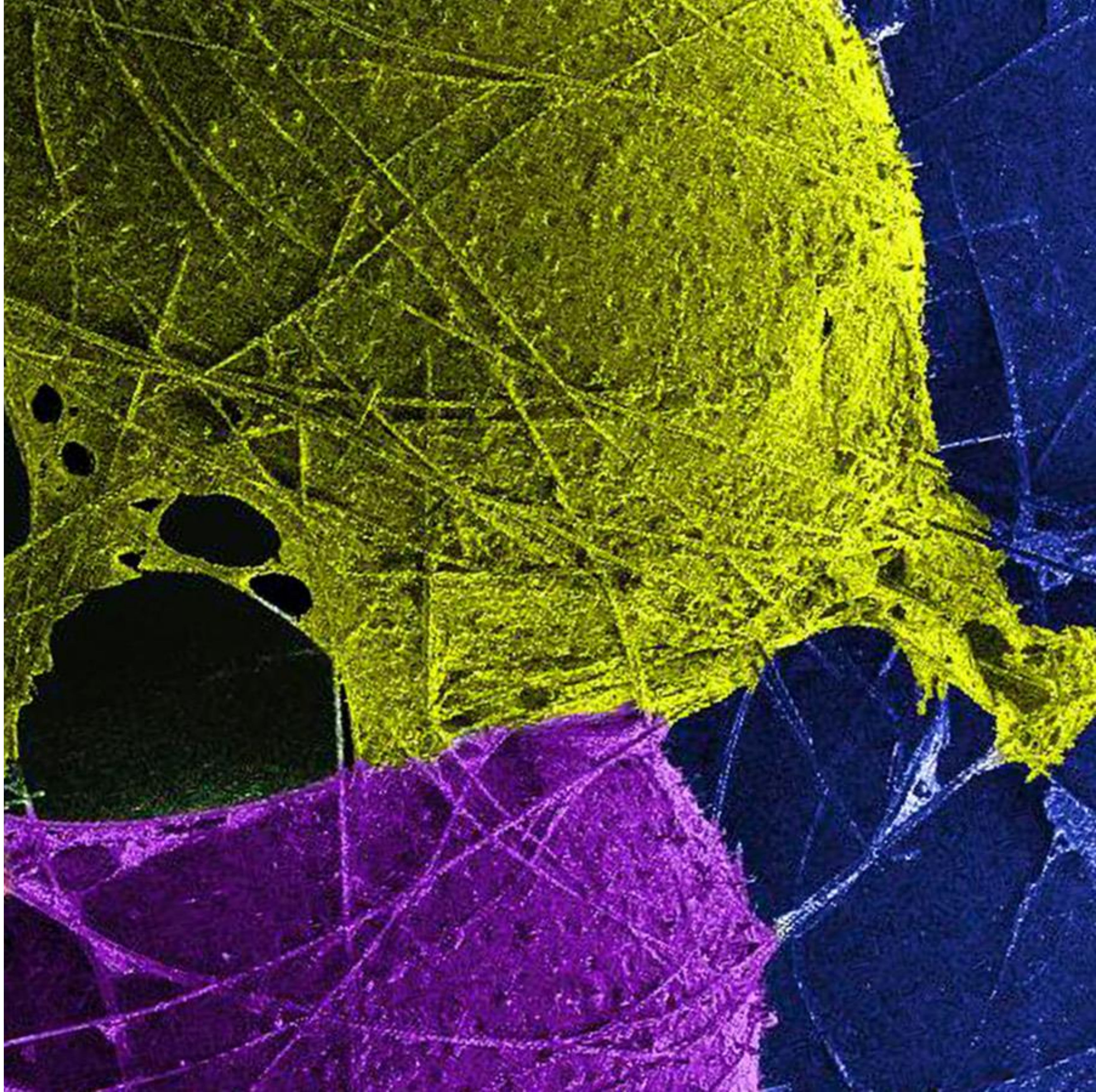
Questions

- What are other examples of chemical/pharmaceutical products or precursors whose characteristics could be attractive to individuals or groups outside of the usual supply chain?

- Could enhancement of supply chain security and customer vetting contribute to the overall level of chemical security for such products or precursors?

L3:
Supply Chain Security and Customer Vetting

Part 2:
Best Practices

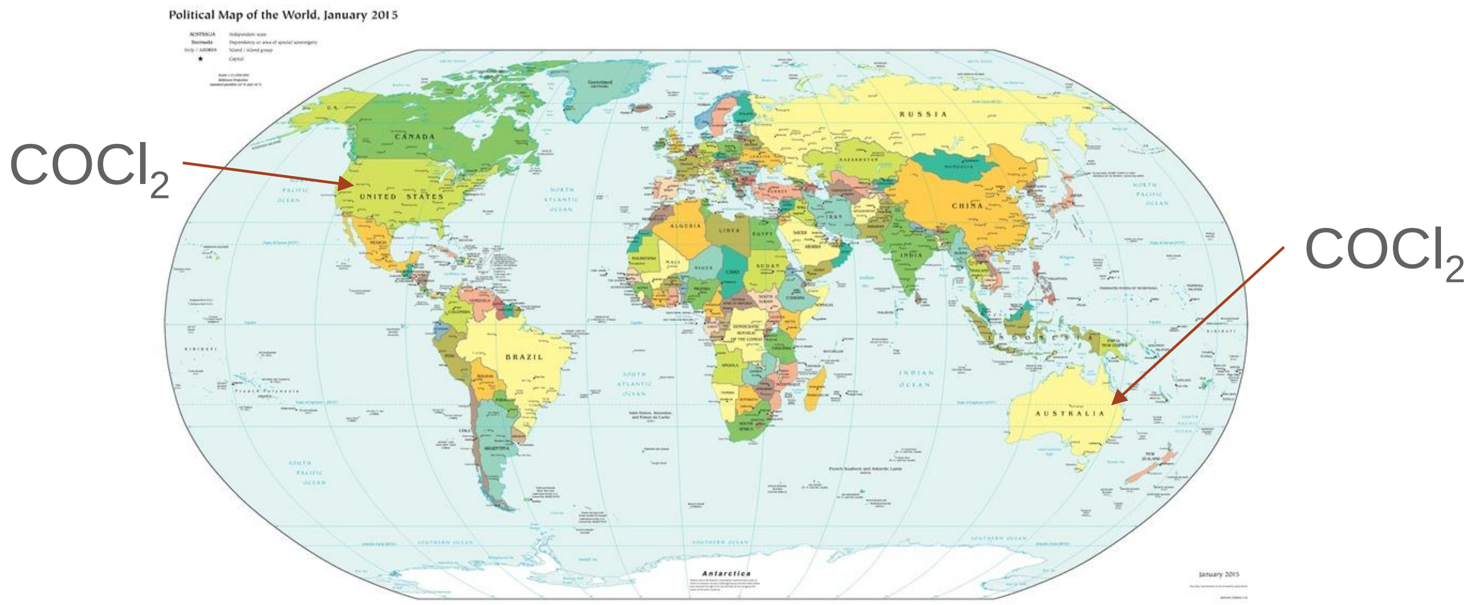


Supply Chain Security and Customer Vetting: Best Practices

- **Outline (Part 2, best practices)**
  - Rationale for increasing supply chain security and customer vetting
  - Examples of best practices
    - Gene synthesis, best practices have been widely adopted *regionally* (US)
    - Custom/contract synthesis as a problem in search of a practice
    - Large chemical vendors
  - Implementation of best practices

Supply Chain Security and Customer Vetting: Best Practices

- **Rationale**
  - Chemical Weapons and TICS are global threats requiring global counter approaches



  - However, regional efforts integrated globally are more easily implemented

Supply Chain Security and Customer Vetting: Best Practices

- **Customer Vetting in Practice:**
  - Custom DNA synthesis
    - In molecular biology, cloning has become less attractive as a means of genetic manipulation.
    - Instead, assembly of synthetic oligonucleotides has become cheaper and more reliable.
    - However: it is possible to assemble entire genomes (with some effort)
    - Smaller genomes are easier to assemble than larger genomes
    - Virus genomes are quite small; horsepox genome synthesis published in *Science* was a wake-up call
    - Some viruses are very bad; 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

Supply Chain Security and Customer Vetting: Best Practices

- **Customer Vetting:**
  - Custom organic synthesis and chemical vendors—is customer vetting ever done?   Often it is not.

    ✓ Numerous vendors online offer custom synthesis services.

    ✓ 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 highly pure—as pure as commercial technical grade material

    ✓ Organic synthesis is moving towards automated determination of the synthetic route (see Sigma’s software) and automation of the synthesis itself.

Supply Chain Security and Customer Vetting: Best Practices

- **Customer Vetting (continued) :**
  - Custom organic synthesis and chemical vendors—is customer vetting ever done?   Often it is not.

    ✓ **Fentanyl**: significant health threat (users, and first responders), many derivatives, all from custom synthesis. China crackdown on Fentanyl.

    ✓ **Synthetic Cannabinoids** (ArkPharm example)

    ✓ **Anabolic steroids**: in WA, USA, steroids were sold to athletes, students, etc., online and delivered by mail through a middleman. Other operations may ship directly from overseas producers to customers. Is the manufacturer aware their product is being sold in this market? Or are chemicals being diverted away from legitimate downstream customers?

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:

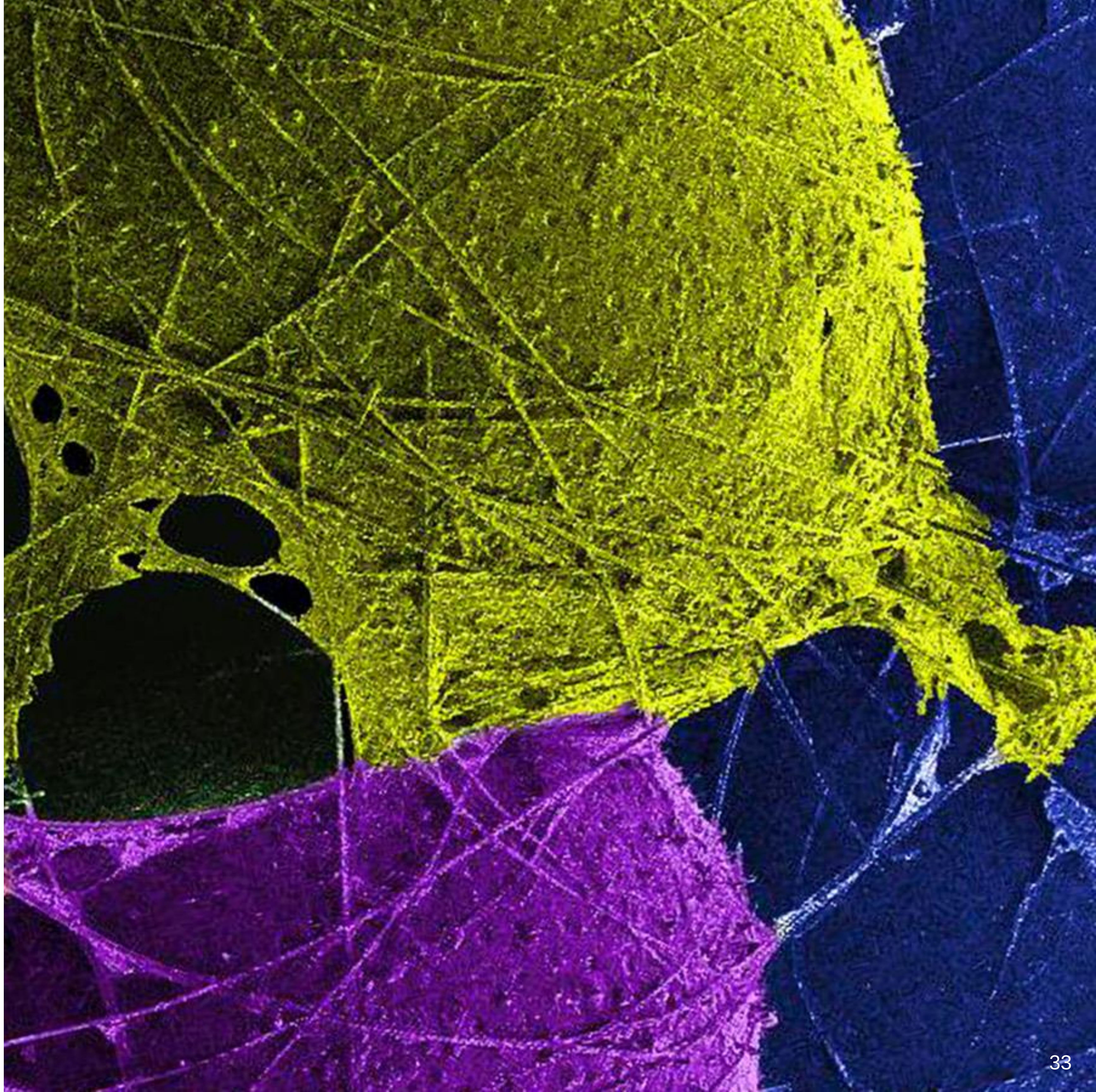
    "…supply the service representative with shipping and billing information. ***The representative will ask some questions about your general business****, along with taking the order. The New Account Department will* ***then verify this information****, as well as* ***validate the intend use of our products****.* ***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."*

Supply Chain Security and Customer Vetting: Best Practices

- **Implementation of Best Practices**
  - Regulations (no consensus) vs. Practices (can reach consensus)
    - Failures of prohibition and traditional concepts of chemical weapons
  - Incentivization of best practices
  - Different best practices are suitable for different types and sizes of firms
  - Addressing People, Processes, Equipment
  - “Supplier Vetting” (see ArkPharm case study)
  - Addressing New Technologies (e.g. RFID chips, digital monitoring, blockchain)
  - Is there justification for an “Association for Chemical Security”, to facilitate consensus-building and sharing of best practices?

Thank you



Lesson 4:
Security Vulnerabilities in the Indian Supply Chain

Dr. M. Surianarayanan & Dr Clifford Glantz

Pacific Northwest
NATIONAL LABORATORY

75 Years of
CSIR Touching Lives

CSIR-CLRI

CISRA

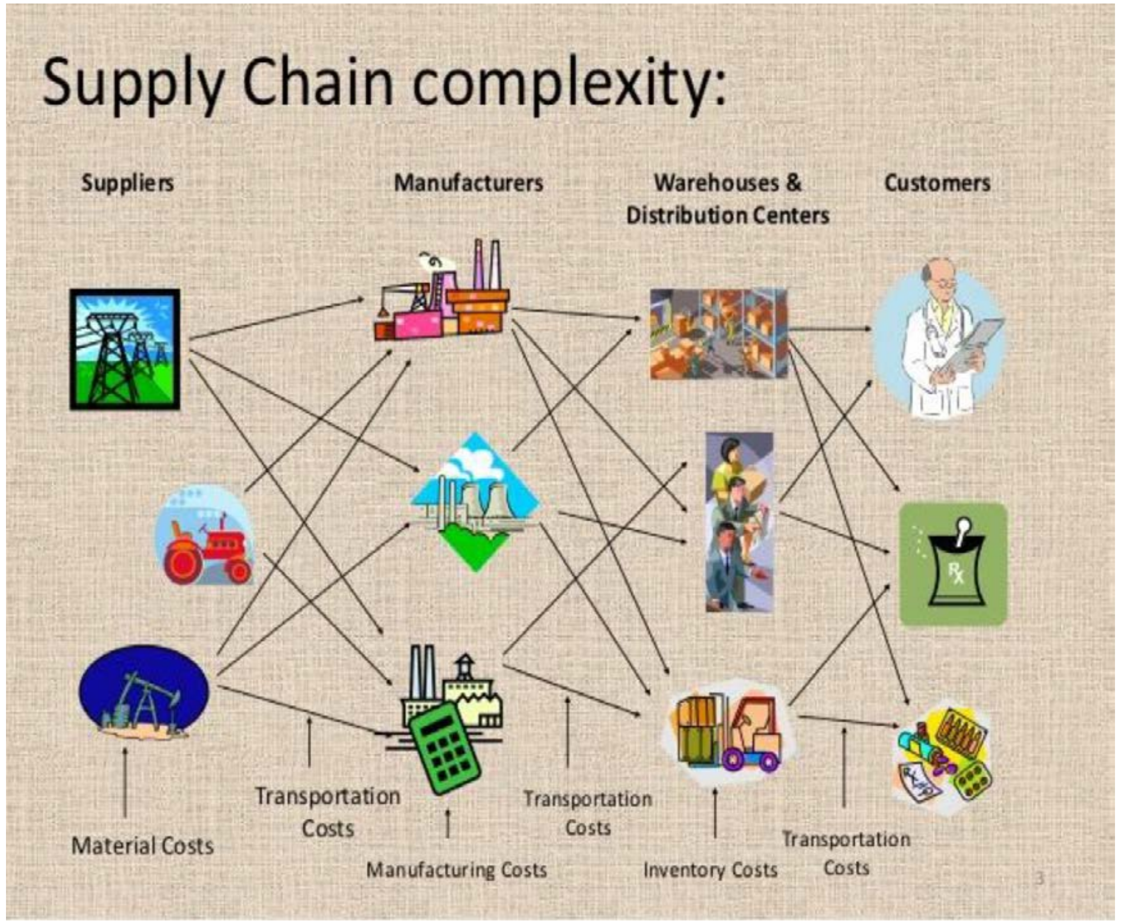
December 8, 2020

Intro to Supply Chain Vulnerabilities

- 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

Vulnerabilities exist in many parts of supply chain operations

Supply Chain Vulnerabilities



- Complex networks of storage and intermodal transport face these challenges
- Longer chains and more actors increase risk.
- Supply chain partners. Third party service providers may not have the same standards or priorities when it comes to security
- 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.

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**
- **Technology**

  With IT systems driving larger parts of supply chains, IT security is a growing issue. IT systems can also be interlinked. Examples are ERP for manufacturing, CRM for sales and operations, and TMS for transport management. Rogue access to one system can lead to access to the next one, and so on.

ERP: Enterprise resource planning, CRM: Customer relationship management, TMS: Transport management System

The Vulnerabilities in the 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.

The Vulnerabilities in the Supply Chain (Cont)

- **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?

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 (cont)

Inadequate protection of physical security-related critical infrastructure:

- Are critical infrastructure assets (e.g., electrical power, water) adequately protected within the facility fenceline?
- 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 (cont)

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 (cont)

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.
- Is monitoring conducted for inappropriate use of plant computer systems?

Potential Supply Chain Vulnerabilities (cont)

- 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 (cont)

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 (cont)

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 (cont)

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?
- Ares suspected attempts to acquire hazardous of dual-use materials reported to the authorities?

Potential Supply Chain Vulnerabilities (cont)

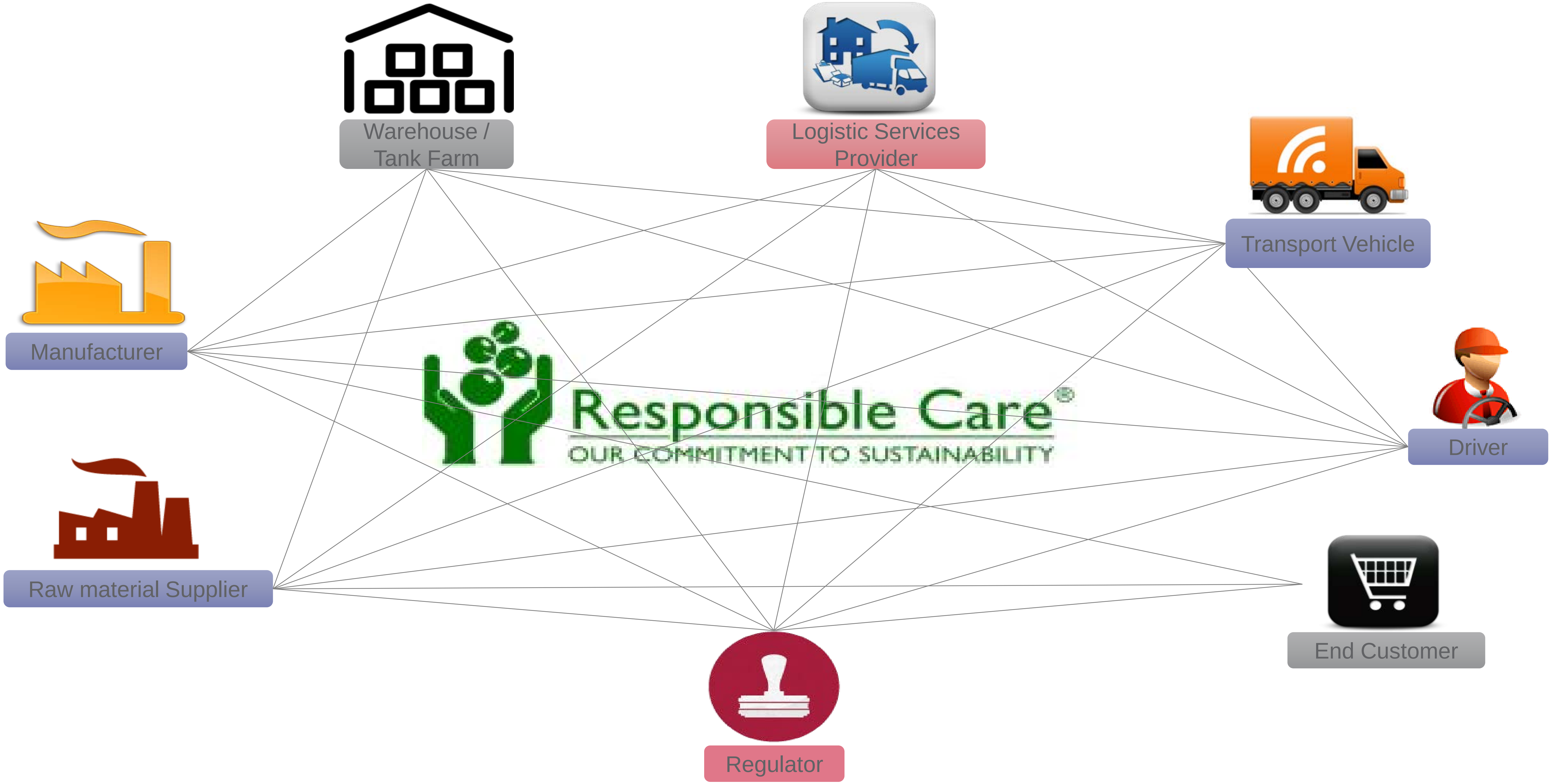
Transport

- 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?

Responsible Care

nicerglobe

Responsible Care® Initiative



Potential Supply Chain Vulnerabilities (cont)

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 requirement 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?

Potential Supply Chain Vulnerabilities (cont)

- 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

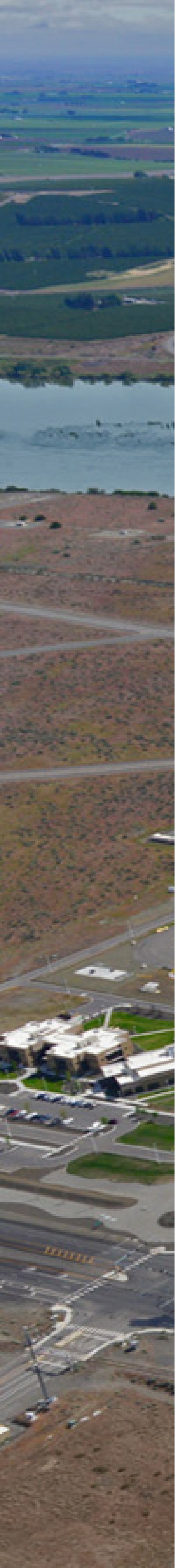
Thank you for the kind attention

email: suri@clri.res.in

Exercise B: Identify Potential Security Practices to Secure Supply Chain

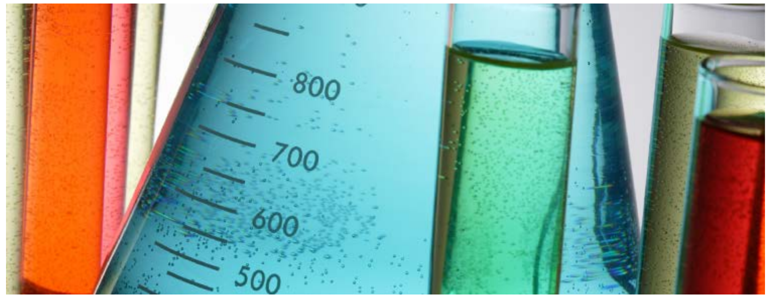
Radha Kishan Motkuri
Cliff Glantz
John Cort
Pacific Northwest National Laboratory (PNNL)
Richland, WA, 99352
USA

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



Pacific Northwest NATIONAL LABORATORY

Instructions



In the previous exercise we discussed an array of attack scenarios with “threat agents” mounting attacks on **Alpha Chemicals & Pharmaceuticals**.

Now shift your attention to the

- physical,
- cyber, and
- personnel security enhancements

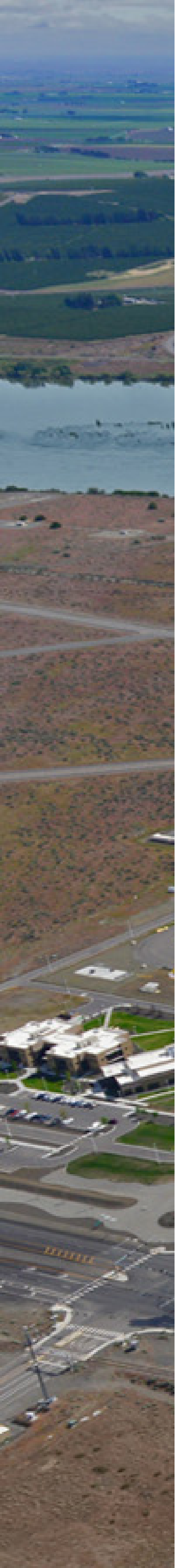
Plant Alpha Chemicals & Pharmaceuticals might implement to reduce or eliminate those attack venues.

Pacific Northwest
NATIONAL LABORATORY

Example Scenario

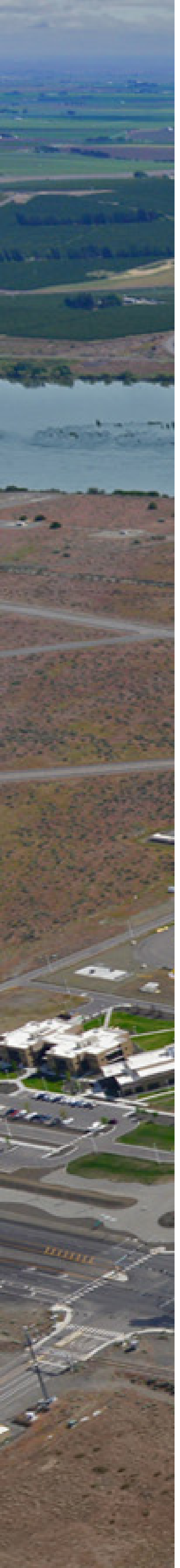
Criminals want to hijack a shipment of pharmaceutical chemicals during their transport from Plant Alpha to a customer.

This time -- you are the defender!



Security Options for Personnel Attack

1. **Information security** (e.g., restrict the public release of information)
2. **Employee assistance program**
   - Offer free mental health, substance abuse, family counseling, etc. to employees
   - Provide financial assistance to employees
3. **Awareness and training**
   - Conduct security training
   - Conduct security awareness programs
   - Offer rewards for reporting security issues
4. **Conduct security checks**
   - Basic screening for new employees and contractors
   - In-depth screening for new and old employees working with high-value or high-risk information, equipment, or materials



Pacific Northwest
NATIONAL LABORATORY

Personnel Security -- Poll 2

Now considering both effectiveness and cost, give the following approaches for prioritizing Plant Alpha’s security investments, which would you choose? (₹13 lakh is budget)

Option A

top

1. ₹1 lakh Information security
2. ₹9 lakh Employee Assistance
3. ₹4 lakh Awareness and training
4. ₹6 lakh Security checks

Bottom

Option B

top

1. ₹1 lakh Information security
2. ₹4 lakh Awareness and training
3. ₹6 lakh Security checks
4. ₹9 lakh Employee Assistance

Bottom

Option C

top

1. ₹4 lakh Awareness and training
2. ₹6 lakh Security checks
3. ₹1 lakh Information security
4. ₹9 lakh Employee Assistance

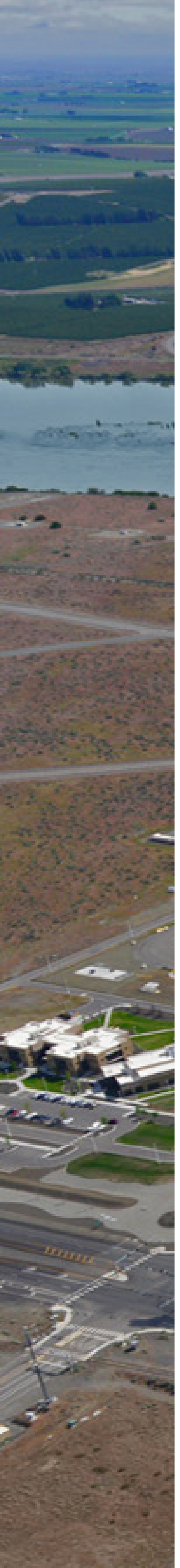
Bottom

Option D

top

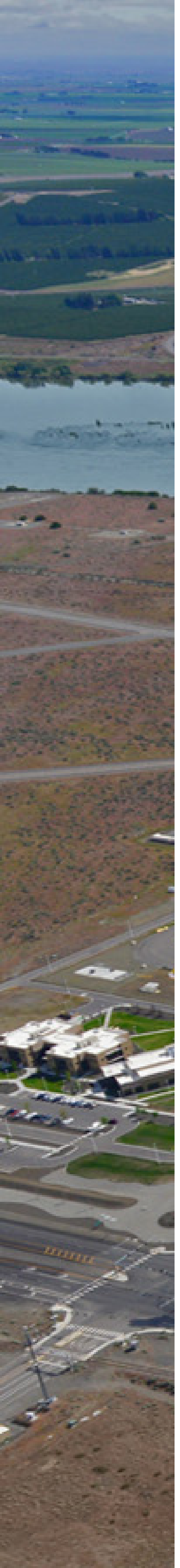
1. ₹6 lakh Security checks
2. ₹4 lakh Awareness and training
3. ₹9 lakh Employee Assistance
4. ₹1 lakh Information security

Bottom



Security Options for Cyberattack

1. **Restrict administrative privileges**
   - The ability to add software or adjust security settings is limited to the system administrators
2. **Require Multifactor Access**
   - To access the network you must have two of the following: something you know, have, or are
   - Example: Password and security token
3. **Secure architecture**
   - Set up zones of increasing security
   - Only allow access to information by authorized personnel
   - Restrict ability to modify data to authorized personnel
4. **Network intrusion and testing with continuous monitoring of logs**
   - Install sensors to continuously monitor for unauthorized access and behavior and alarm if something suspicious is found



Cybersecurity -- Poll 2

Now considering both effectiveness and cost, give the following approaches for prioritizing Plant Alpha's security investments, which would you choose? (₹13 lakh is budget)

Option A

top

1. ₹1 lakh Restrict Privileges
2. ₹4 lakh Multifactor Access
3. ₹6 lakh Secure Architecture
4. ₹9 lakh Intrusion Detection

Bottom

Option B

top

1. ₹1 lakh Restrict Privileges
2. ₹6 lakh Secure Architecture
3. ₹9 lakh Intrusion Detection
4. ₹4 lakh Multifactor Access

Bottom

Option C

top

1. ₹6 lakh Secure Architecture
2. ₹9 lakh Intrusion Detection
3. ₹4 lakh Multifactor Access
4. ₹1 lakh Restrict Privileges

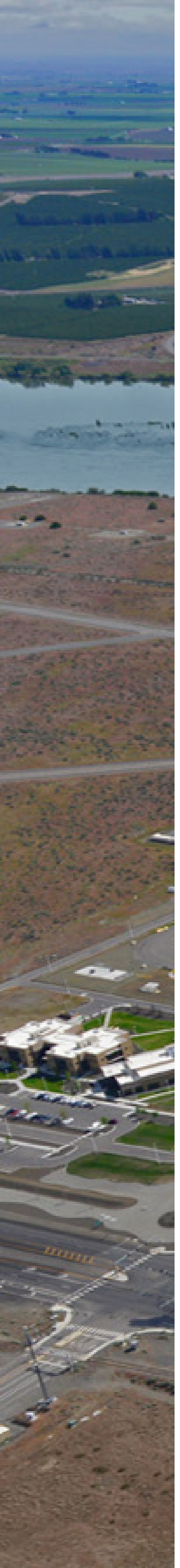
Bottom

Option D

top

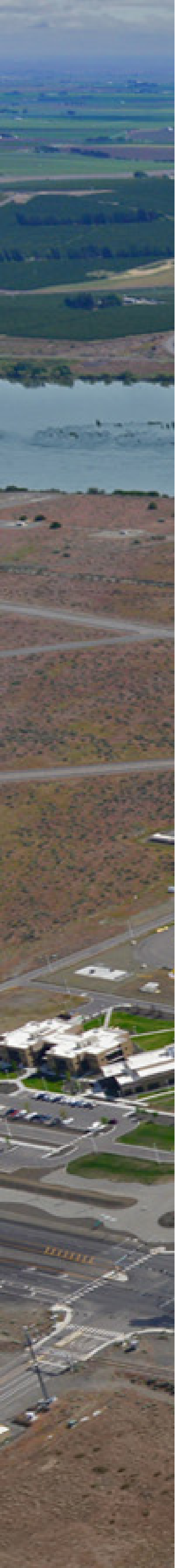
1. ₹9 lakh Intrusion Detection
2. ₹6 lakh Secure Architecture
3. ₹1 lakh Restrict Privileges
4. ₹4 lakh Multifactor Access

Bottom



Physical Security Options

1. **Increase physical security at Plant Alpha**
   - Add guards
   - Install security cameras
   - Install alarms
2. **Install GPS on trucks**
   - Monitor truck location
   - Report a potential problem if there is a significant departure from route
3. **Provide truck drivers with emergency notification devices**
   - A panic button alerts Plant Alpha when a driver believes there is a security threat
   - Includes information of truck location
4. **Label containers with identification numbers to enhance traceability**
   - Only allow access to information by authorized personnel
   - Restrict ability to modify data to authorized personnel



Pacific Northwest
NATIONAL LABORATORY

Physical Security -- Poll 2

Now considering both effectiveness and cost, give the following approaches for prioritizing Plant Alpha's security investments, which would you choose? (₹13 lakh is budget)

Option A

top

1. ₹6 lakh Security at Plant
2. ₹2 lakh GPS on Trucks
3. ₹4 lakh Emergency notification
4. ₹9 lakh Label Containers

Bottom

Option B

top

1. ₹2 lakh GPS on Trucks
2. ₹4 lakh Emergency notification
3. ₹6 lakh Security at Plant
4. ₹9 lakh Label Containers

Bottom

Option C

top

1. ₹4 lakh Emergency notification
2. ₹9 lakh Label Containers
3. ₹2 lakh GPS on Trucks
4. ₹6 lakh Security at Plant

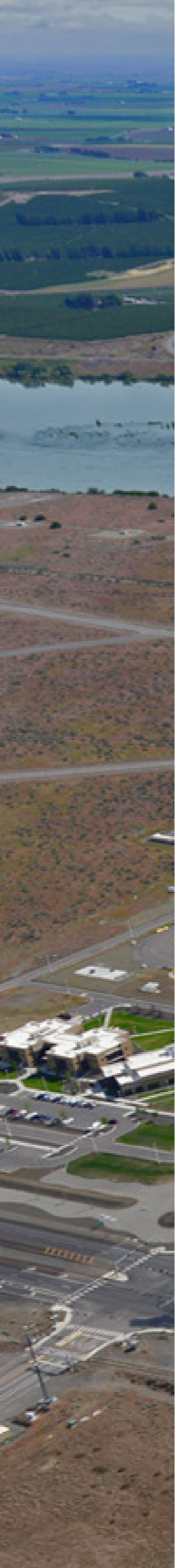
Bottom

Option D

top

1. ₹9 lakh Label Containers
2. ₹4 lakh Emergency notification
3. ₹6 lakh Security at Plant
4. ₹2 lakh GPS on Trucks

Bottom



Pacific Northwest
NATIONAL LABORATORY

Thank you

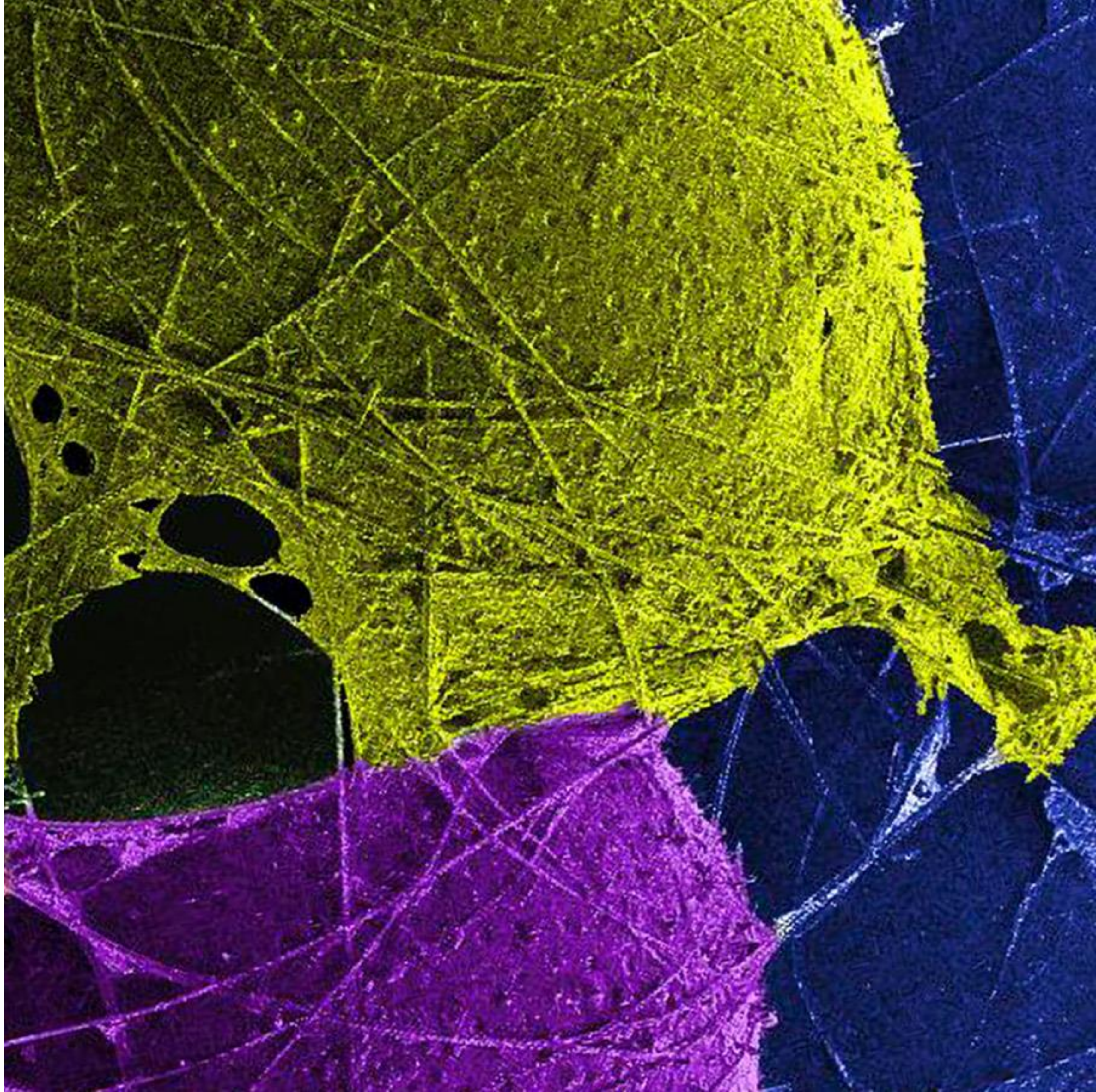
If you have any further questions:
Dr. Radha Kishan Motkuri
Radhakishan.Motkuri@pnnl.gov

L5
Security Engineering

John Cort
Cliff Glantz
Radha Kishan Motkuri

Pacific Northwest National Laboratory

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



REVIEW Supply Chain Security and Customer Vetting: Background

- **Why might an individual or group disrupt the supply chain or divert chemicals?**
  - Supply chain disruption / diversion:
    - Economic sabotage—disruption
    - Criminal mischief—disruption
    - Unintentional / accident / incompetence / negligence—disruption or diversion
    - Theft—diversion
    - **To obtain specific chemicals (or products, e.g. pharmaceuticals) of interest,** apart from their market value—diversion

Pacific Northwest NATIONAL LABORATORY

REVIEW Supply Chain Security and Customer Vetting: Best Practices

- **Implementation of Best Practices**
  - Regulations (no consensus) vs. Practices (can reach consensus)
    - Failures of prohibition and traditional concepts of chemical weapons
  - Incentivization of best practices
  - Different best practices are suitable for different types and sizes of firms
  - Addressing People, Processes, Equipment
  - “Supplier Vetting” (see ArkPharm case study)
  - Addressing New Technologies (e.g. RFID chips, digital monitoring, blockchain)
  - Is there justification for an “Association for Chemical Security”, to facilitate consensus-building and sharing of best practices?

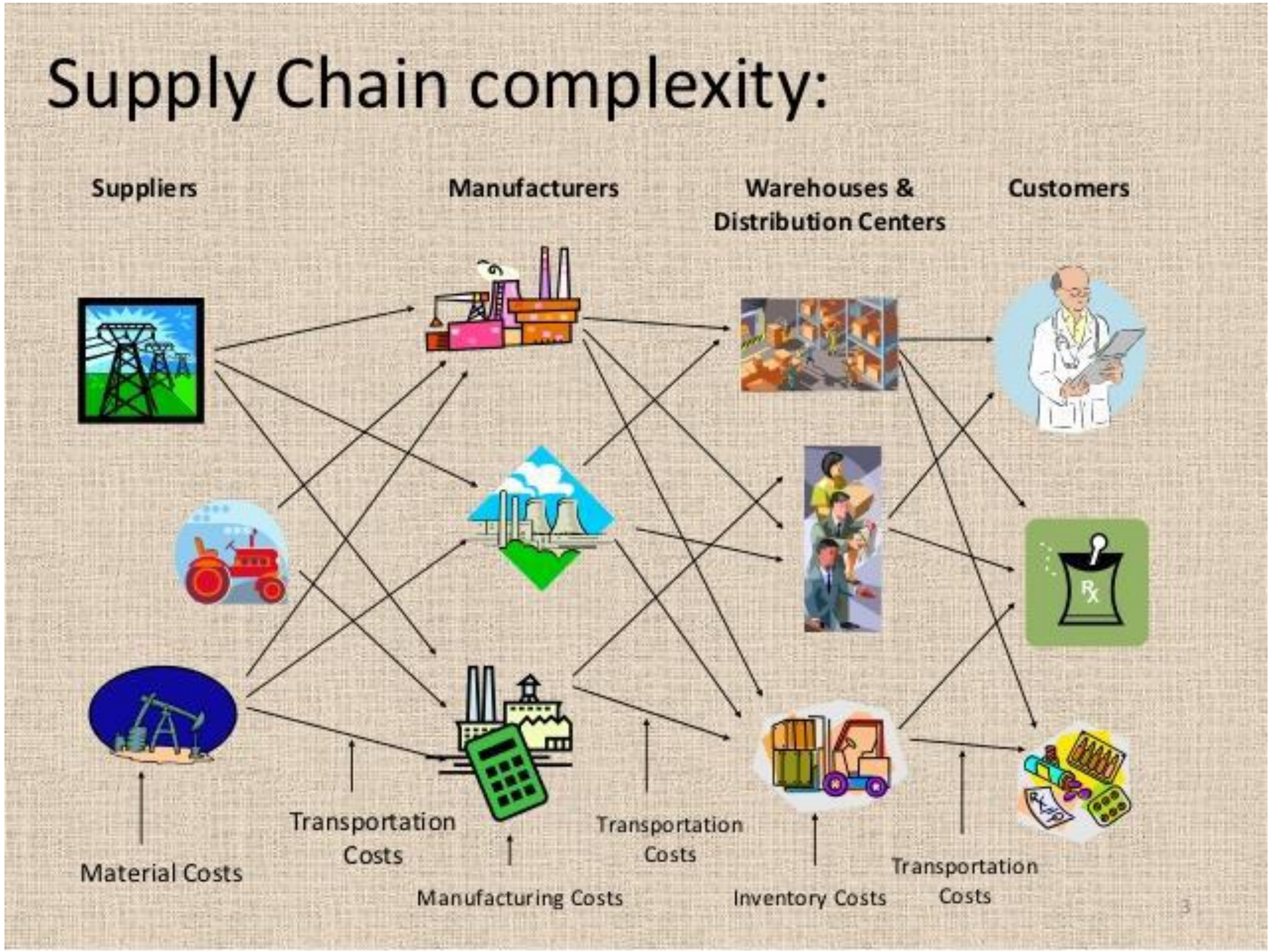
Pacific Northwest
NATIONAL LABORATORY

Security Engineering

- Outline
  - Significant challenges due to a very complex system
  - Supply chains ***can*** be securely engineered to prevent abuse and crime
  - Approaches to reduce risks from threats and vulnerabilities can be <u>strategic</u>, <u>tactical</u>, or both
  - Defense vs. resilience
  - A popular strategy is <u>layered defense</u>
  - Building security into equipment
  - Innovations and new technology are necessary to keep pace with adversaries
  - Ideal for ongoing supply chains that persist for long durations, e.g. product lifecycles
    - ➢ But what about one-off transactions (e.g., custom synthesis)?

Security Engineering

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



Supply Chain complexity:

Security Engineering

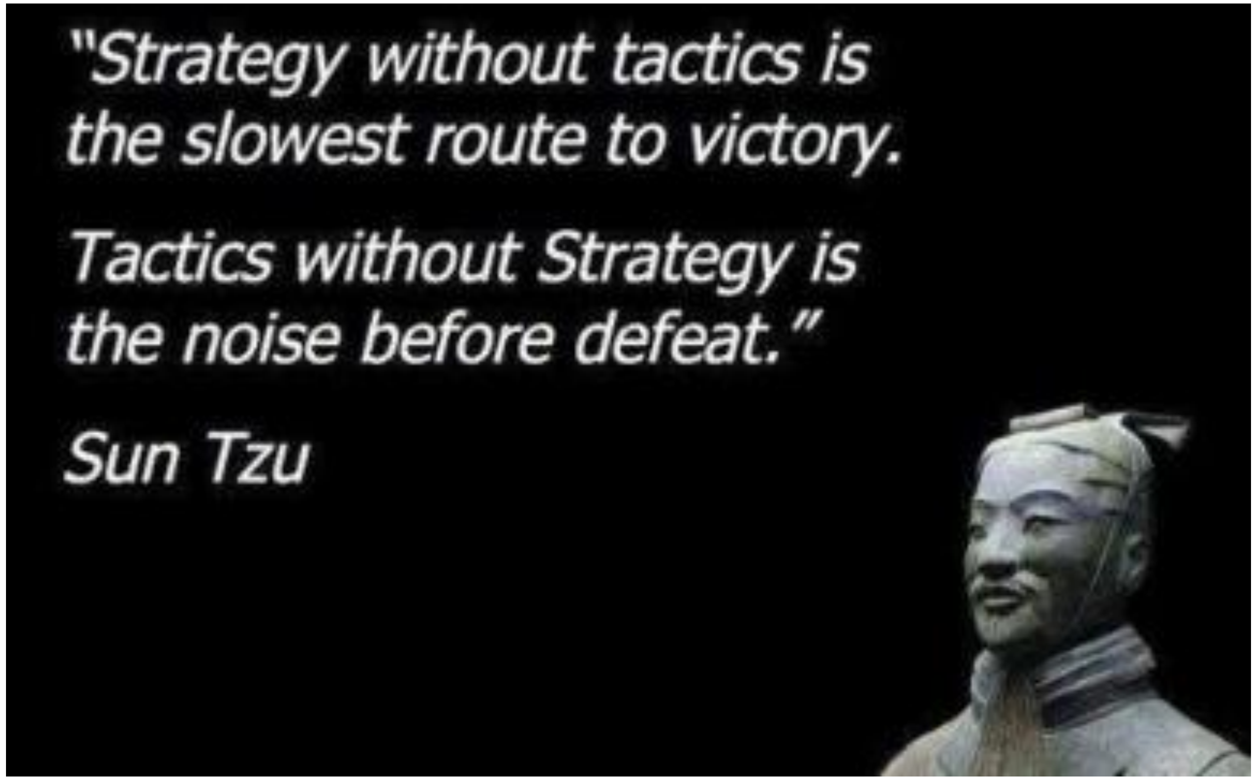
- Complexity does not prevent the problem from being addressed, if we recognize which elements of chemical supply chains are more attractive to adversaries:
  - Chemicals
  - Manufacturing and production facilities
  - Transport and distribution infrastructure
  - Personnel
  - Symbolic nature of the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

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

Security Engineering: Strategies and Tactics

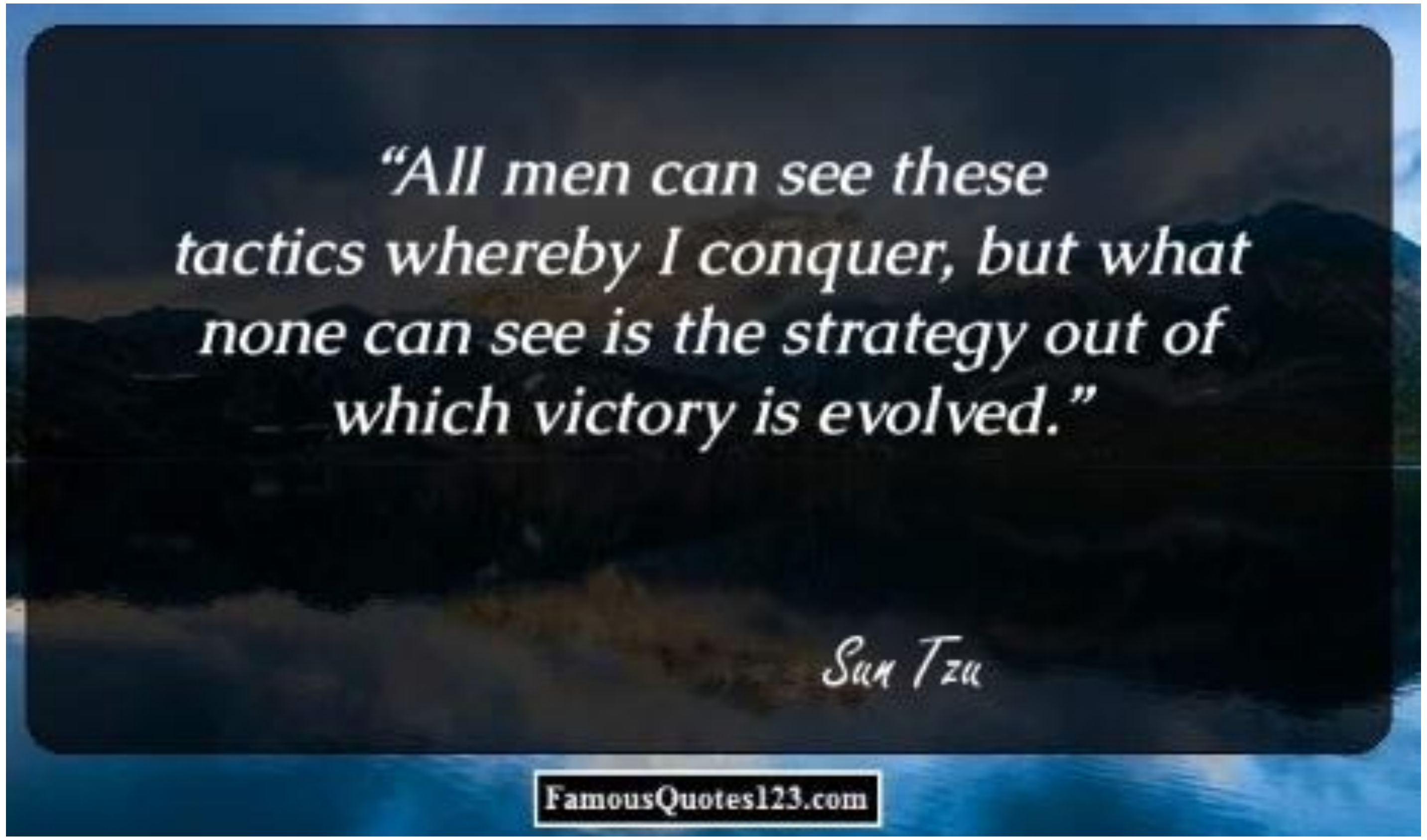
- Approaches to reduce security risks should include both strategies and tactics.
- Strategies are used to define or outline the desired outcome or goal
- Tactics represent the specific actions that are required to implement the strategy
  - What is to be done
  - Order of operations
  - Tools to be 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



"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

Security Engineering: Defense vs. 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
    - 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.
    - Customer Vetting, as an indirect or “soft” defense

Security Engineering: Defense vs. Resilience

- Resilience reduces the impact of a successful attack
  - Reduces consequences without having much of an impact on the probability of the attack

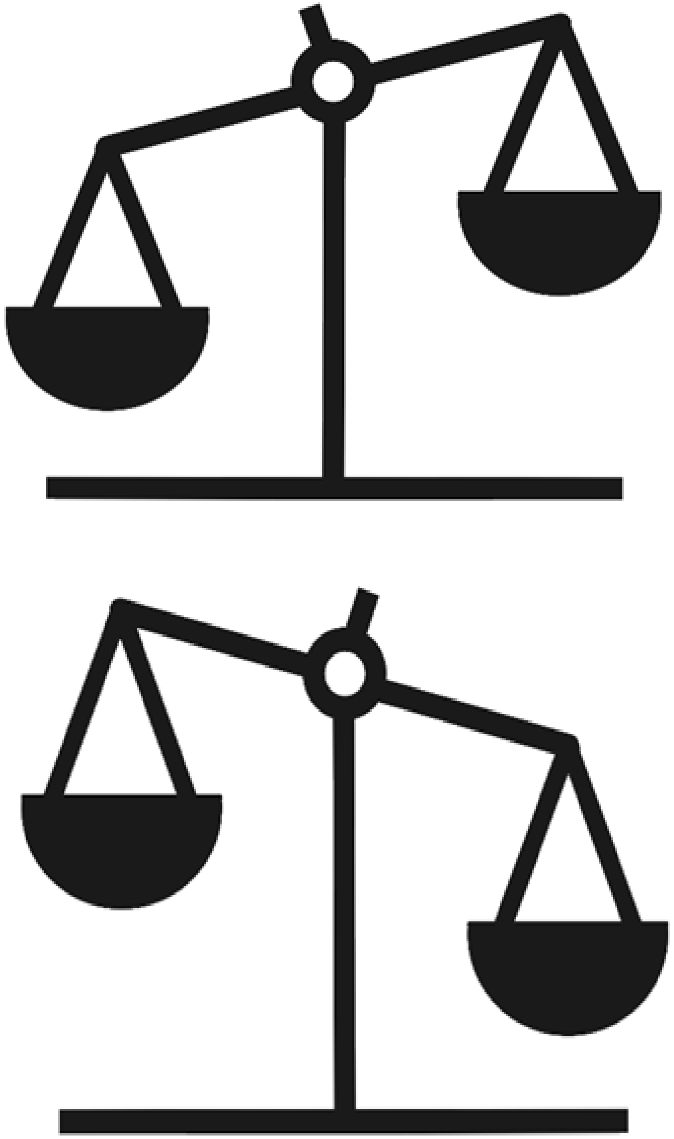
Examples:

- 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 multiple suppliers allows production to continue even if one supplier needs to be fired after providing counterfeit products.

Pacific Northwest NATIONAL LABORATORY

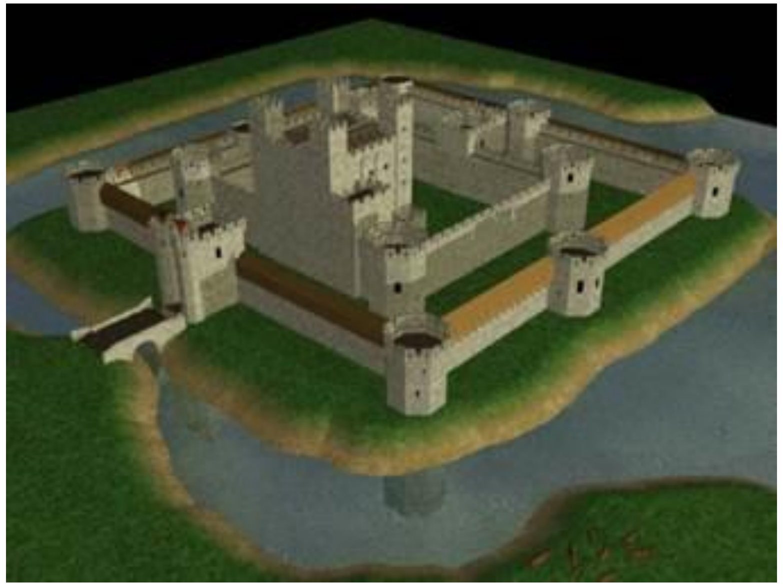
Finding the Right Balance between Defense and Resilience

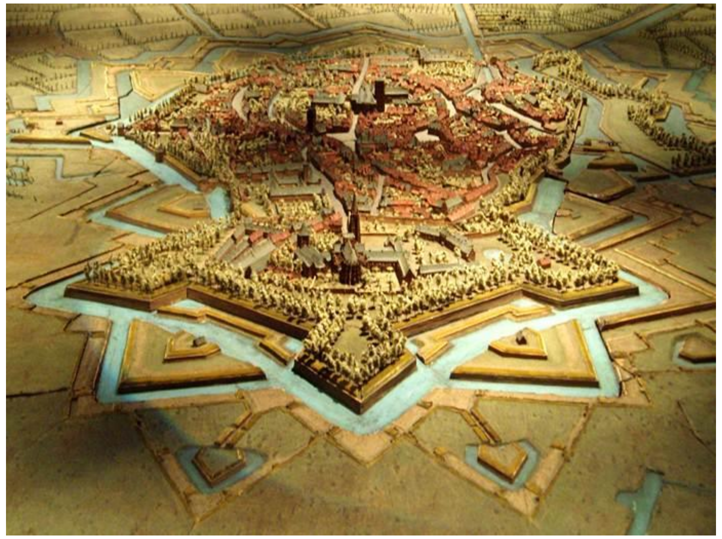
- An effective security program utilizes both defense and resilience to achieve an optimal level of risk management.
- The key is to assess the risks and costs and then find the right balance for your company and circumstances.



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.*



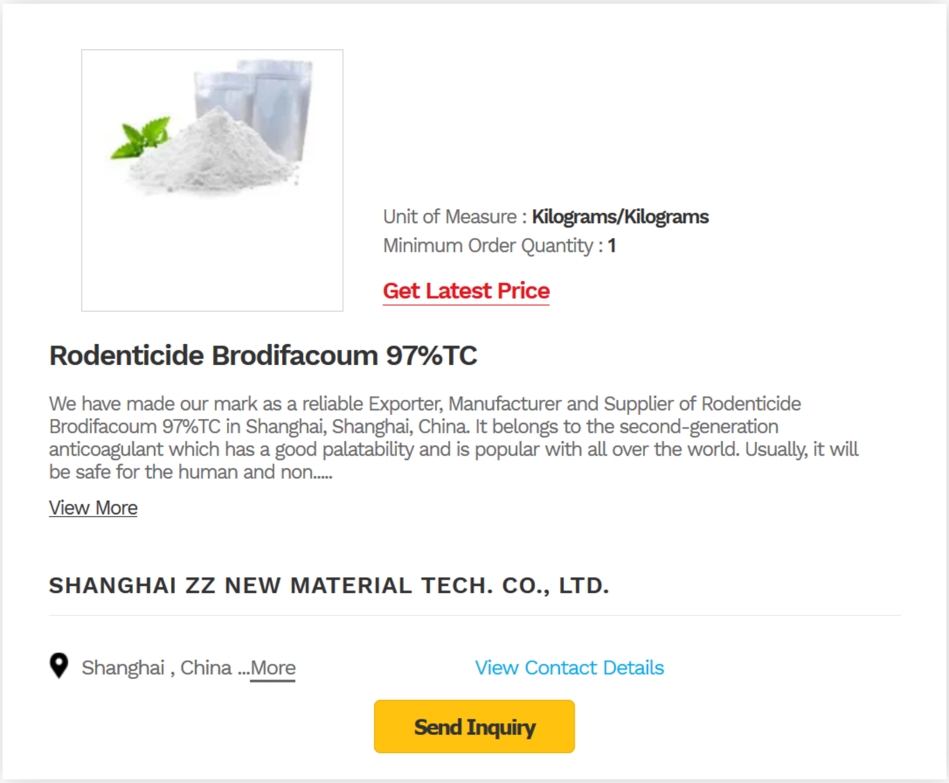


Defense-in-Depth (cont)

- 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.

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 fine chemicals and custom chemical synthesis, where any order/customer is potentially unique or one-time-only.



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

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

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**

Security Engineering—elements

- **Reduction of HazMat shipments**
  - Conversion to less hazardous derivate 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

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 drive 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)

Security Engineering—details

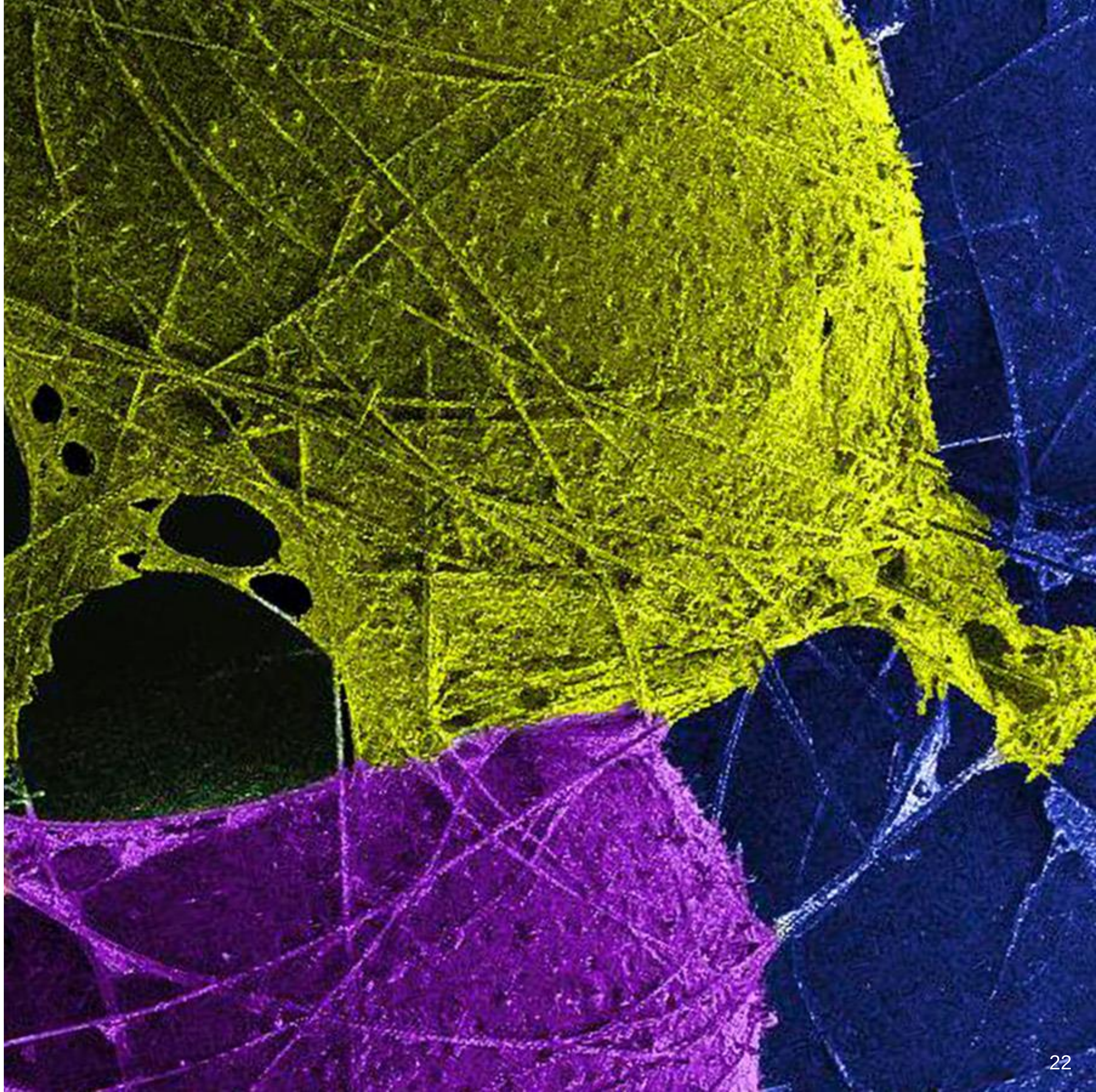
- Engineering solutions for chemical security—ideas
  - Try to keep chemical facilities and shipping routes away from vulnerable infrastructure (government buildings, tunnels, bridges, urban areas)
  - Advanced route planning to reduce number and distance of HazMat shipments (DOW case)
  - Alternate routings and shipping times, if possible
  - 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 (control information about shipping schedules and routes)
  - Integration of cyber security into the overall supply chain security strategy

Security Engineering—details

- Engineering solutions for chemical security—wrap-up
  - Other ideas?
  - What are we missing?
  - Can we use a “red team” approach to find vulnerabilities?
  - What are some emerging technological solutions that could be used to improve chemical security?

Pacific Northwest
NATIONAL LABORATORY

Thank you



Exercise C (& D): Identifying Potential Vulnerabilities in the Supply Chain

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

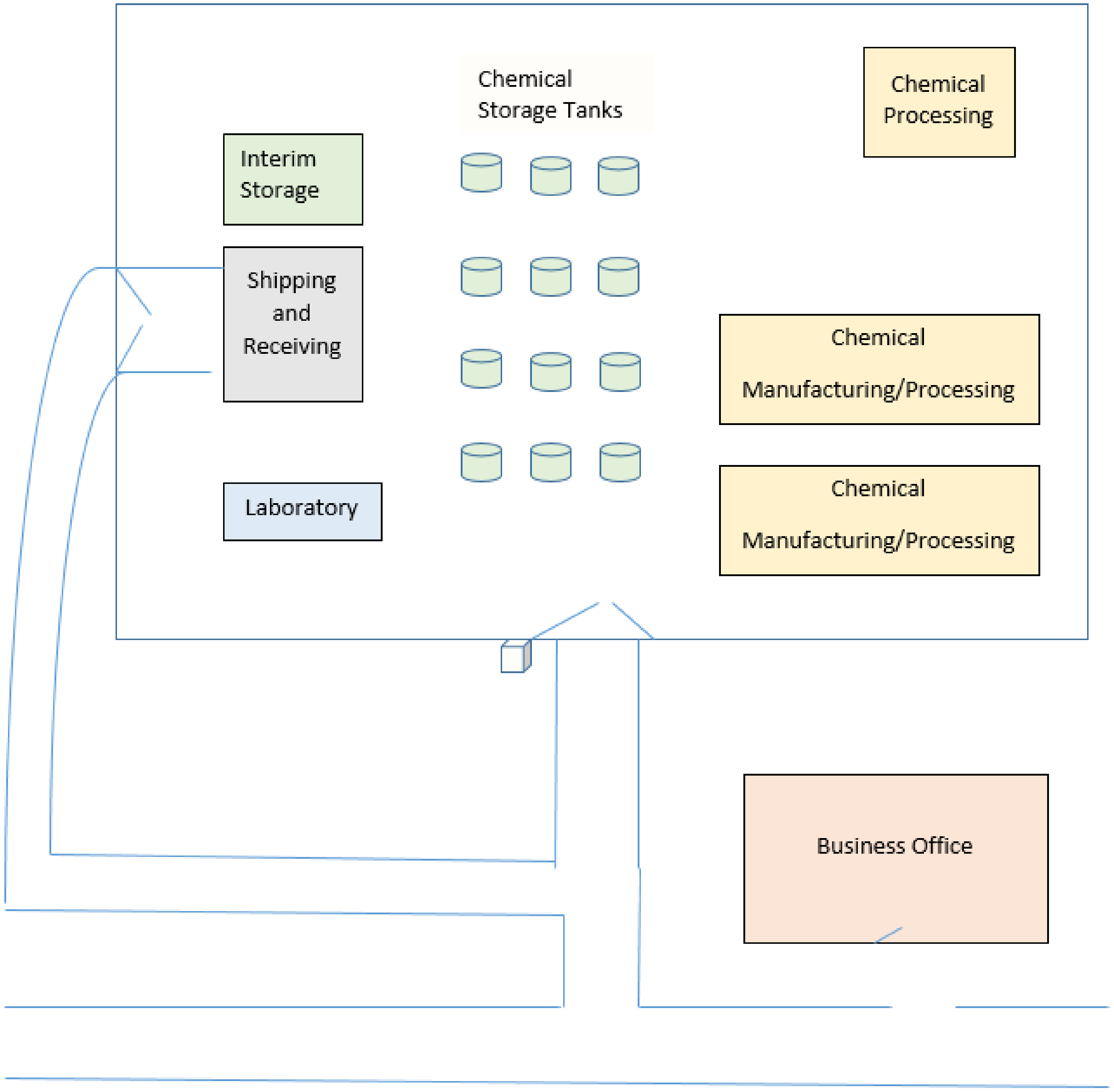
PNNL is operated by Battelle for the U.S. Department of Energy

Instructions

In the previous exercise you have:

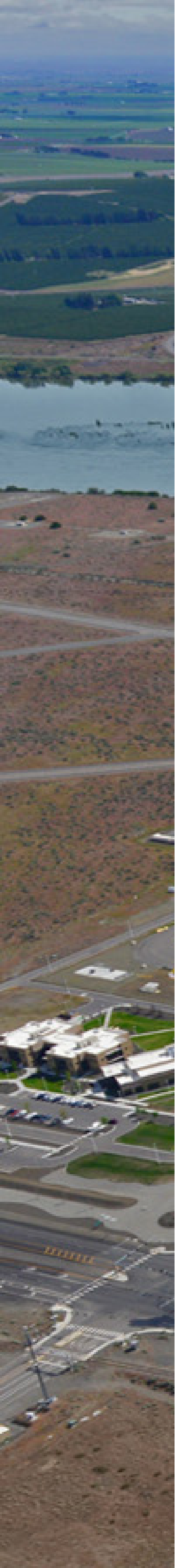
- identified an array of attack scenarios involving threat agents mounting attacks on Alpha Chemicals & Pharmaceuticals.
- Identified preliminary physical, cyber, and personnel security enhancements that Plant Alpha Chemicals & Pharmaceuticals might implement to reduce or eliminate those attack pathways.

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



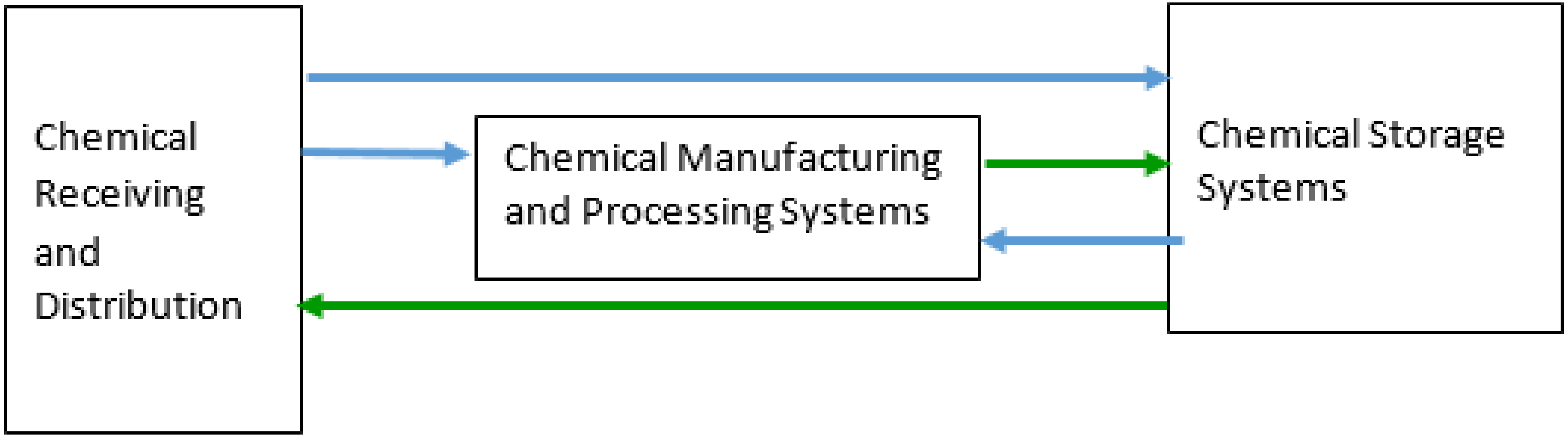
Plant MAP:

Alpha Chemicals & Pharmaceuticals



Alpha Chemicals & Pharmaceuticals

Flow of Materials

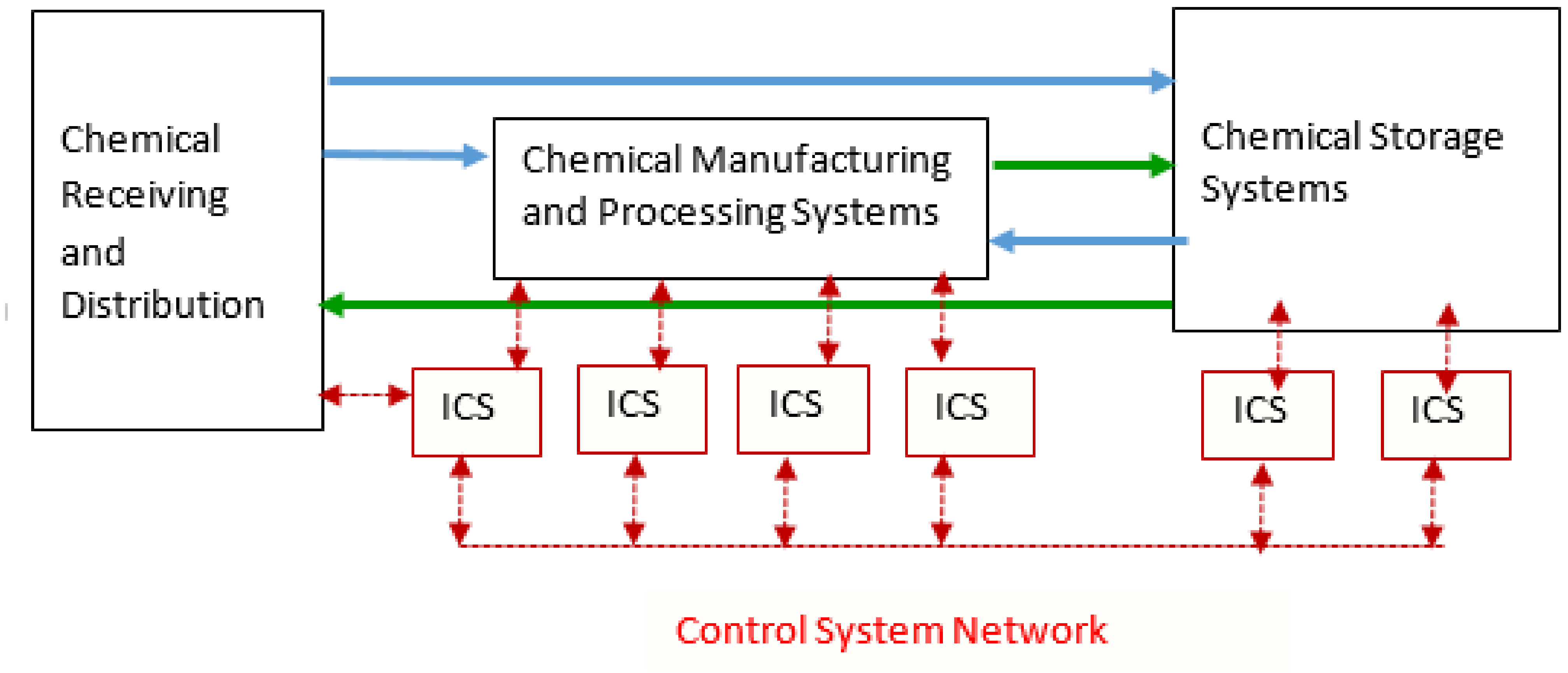


Chemical Receiving and Distribution

Chemical Manufacturing and Processing Systems

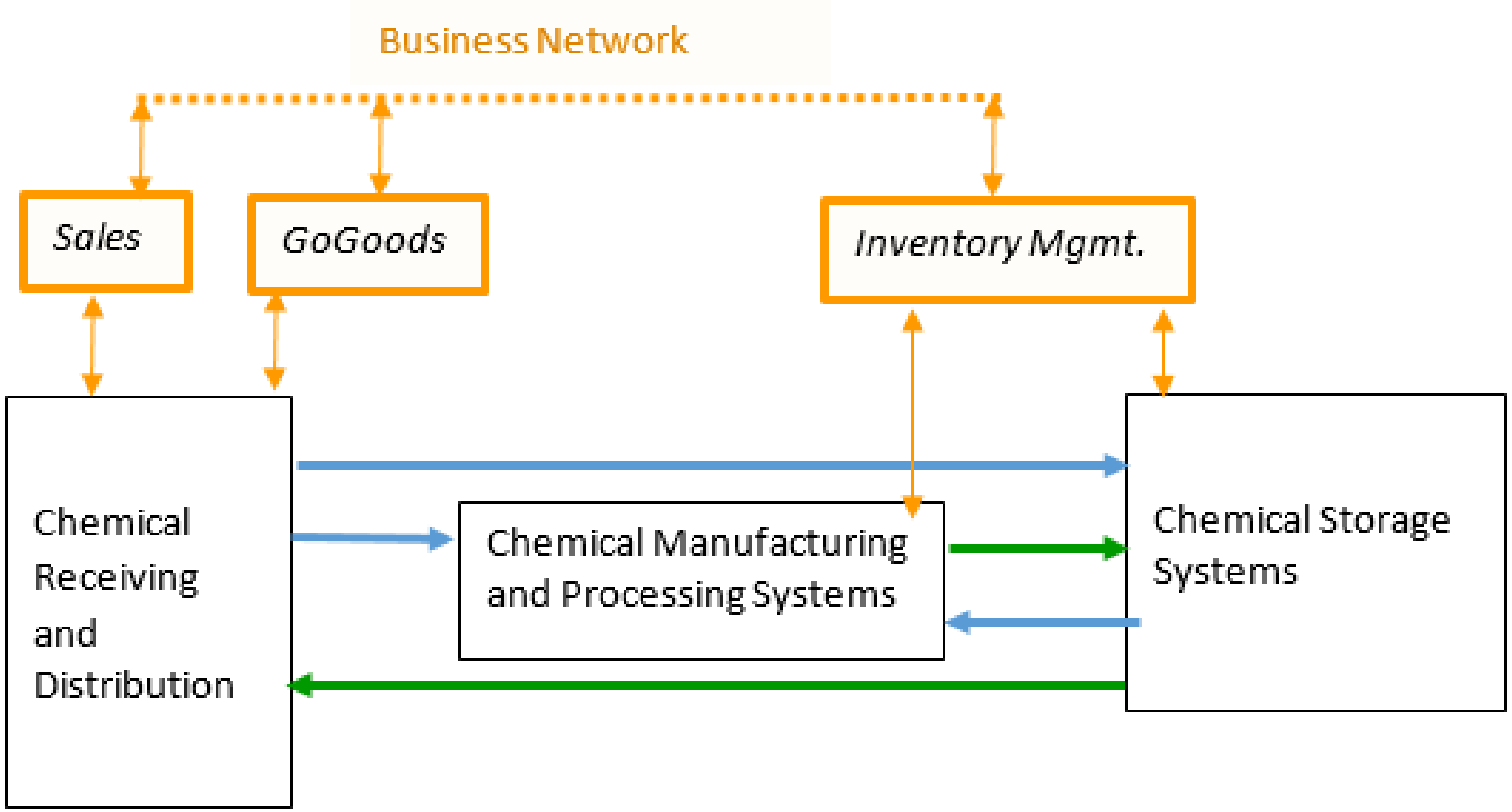
Chemical Storage Systems

Alpha Chemicals & Pharmaceuticals Control System Network

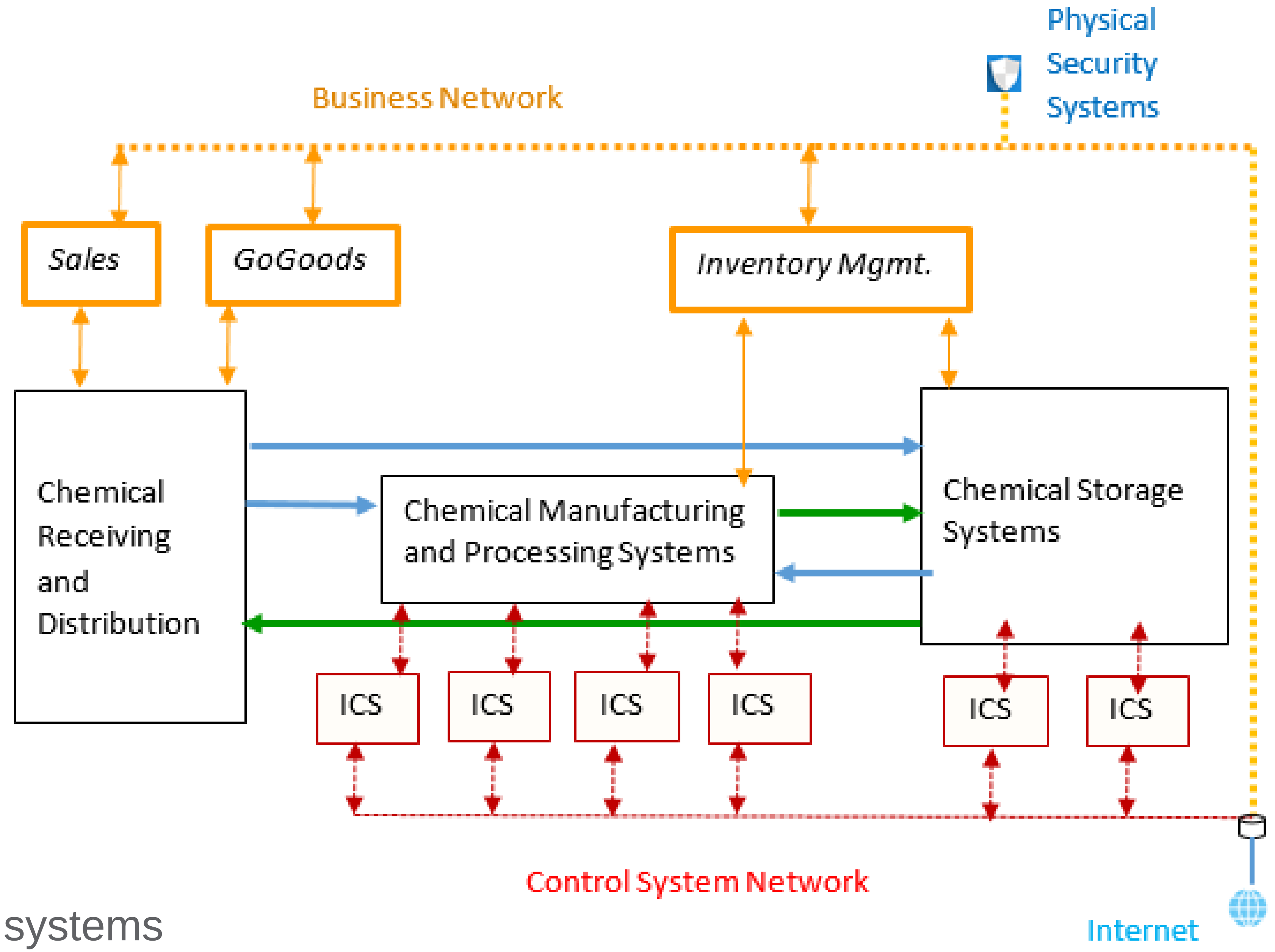

Chemical Receiving and Distribution
Chemical Manufacturing and Processing Systems
Chemical Storage Systems
ICS
ICS
ICS
ICS
ICS
ICS
Control System Network

ICS: industrial control systems

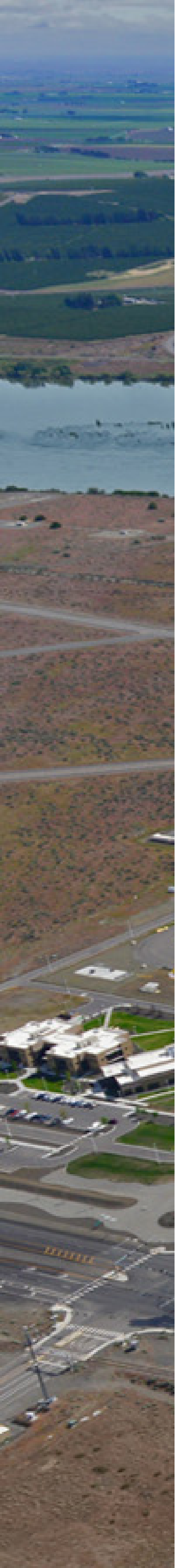
Alpha Chemicals & Pharmaceuticals Business IT Network


Business Network
Sales
GoGoods
Inventory Mgmt.
Chemical Receiving and Distribution
Chemical Manufacturing and Processing Systems
Chemical Storage Systems

Alpha Chemicals & Pharmaceuticals
Integrated View of Facility Networks and Flows



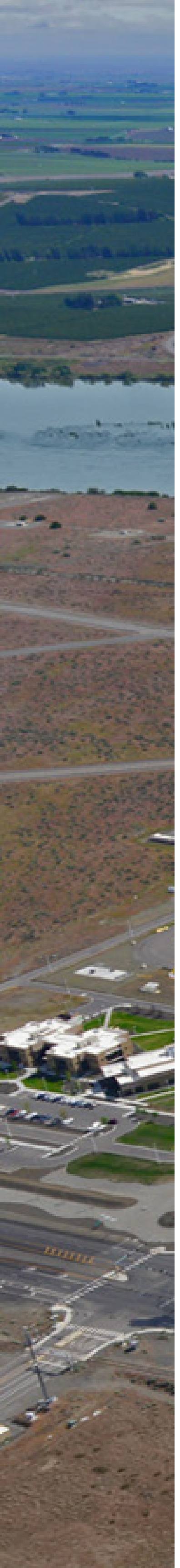
ICS: industrial control systems



A Supplier Request

A supplier you have worked with for many years wants to directly connect to your chemical inventory system so that they can see when your inventory is running low and promptly ship additional products in order to maintain your inventory. Should you:

1. Immediately agree to this time saving connection
2. Explore their security arrangements so you can be assured that your information will only be used for the intended purpose
3. Agree to the deal, but only after you have installed appropriate security controls to limit the information the supplier can access
4. Turn them down.   We do not allow any external suppliers monitor our inventory information



Pacific Northwest
NATIONAL LABORATORY

Thank you

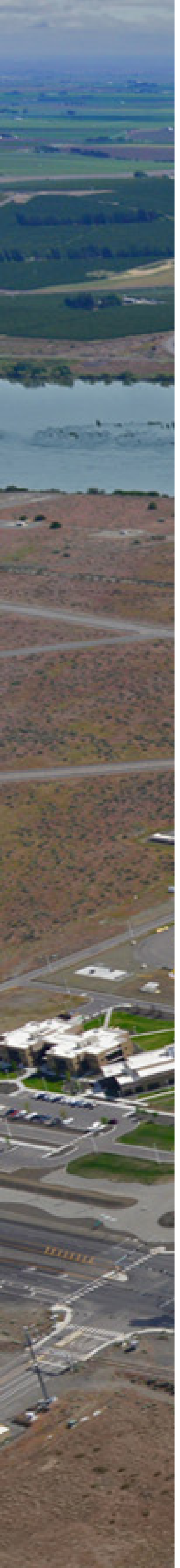
If you have any further questions:

Radhakishan.Motkuri@pnnl.gov

Social Engineering for Chemical Security

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

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

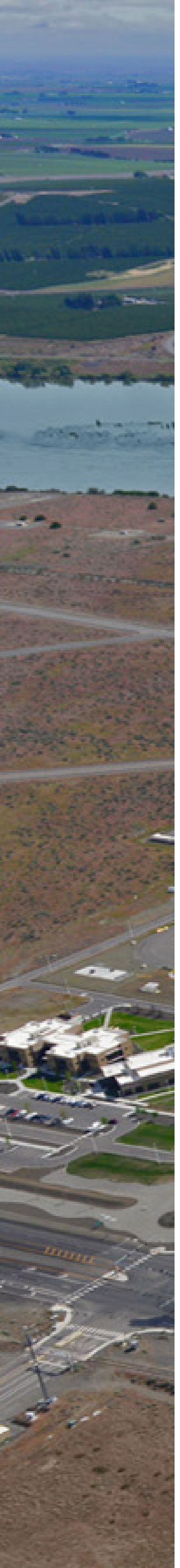


Social Engineering for Chemical Security

Purpose & Learning Objectives

Increasing awareness on how to work effectively, safely and securely with people by developing results-oriented communication skills. (Social engineering and physical/chemical security)

- In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems.
- An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity.



Social Engineering for Chemical Security

Purpose & Learning Objectives

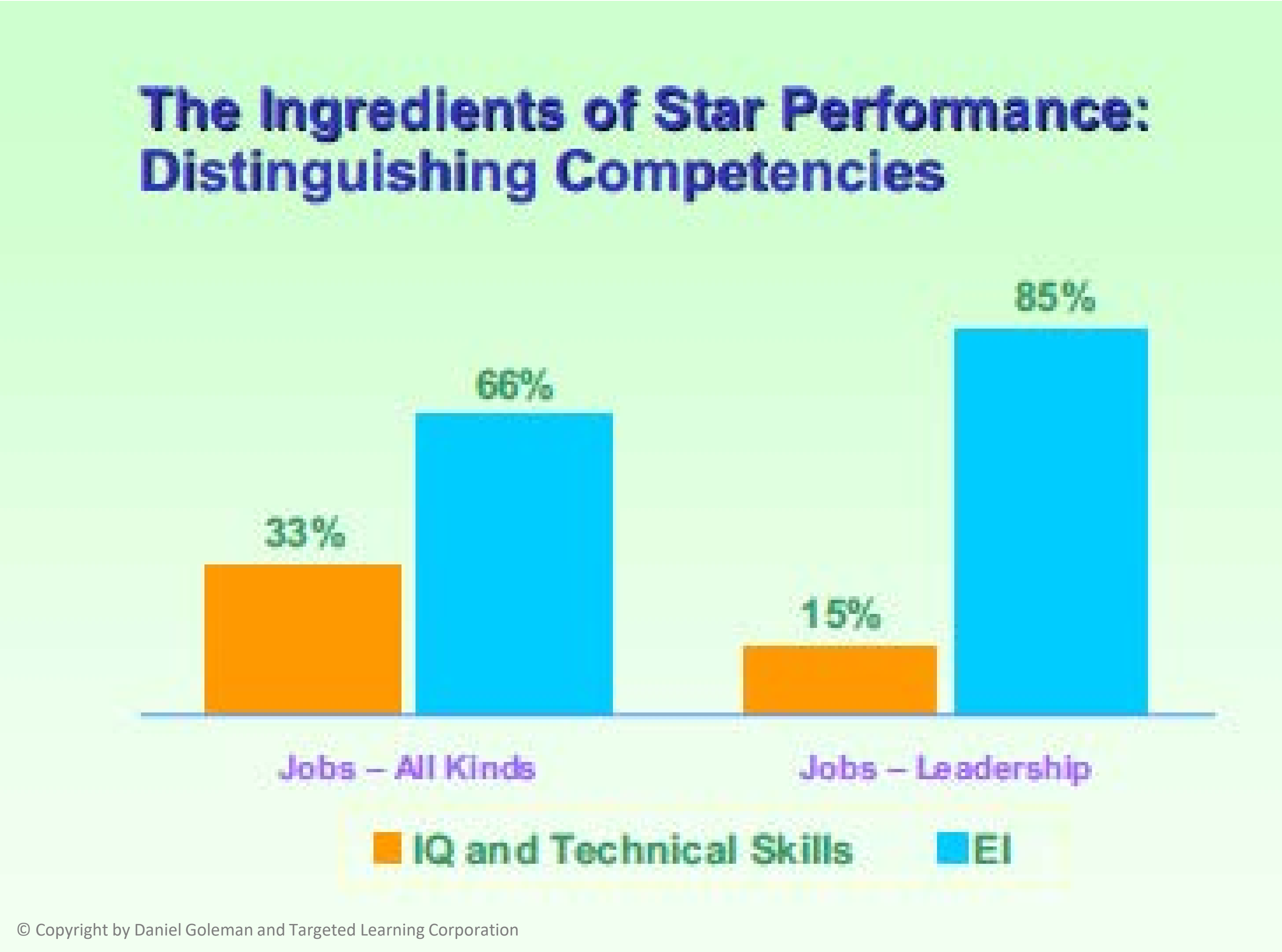
Premises of Social Styles

- We are creatures of habit
- People are different
- We make judgments about other people’s habits
- Focusing only on behavior allows us to avoid the pitfalls of judgment and understand what others need to work effectively with us

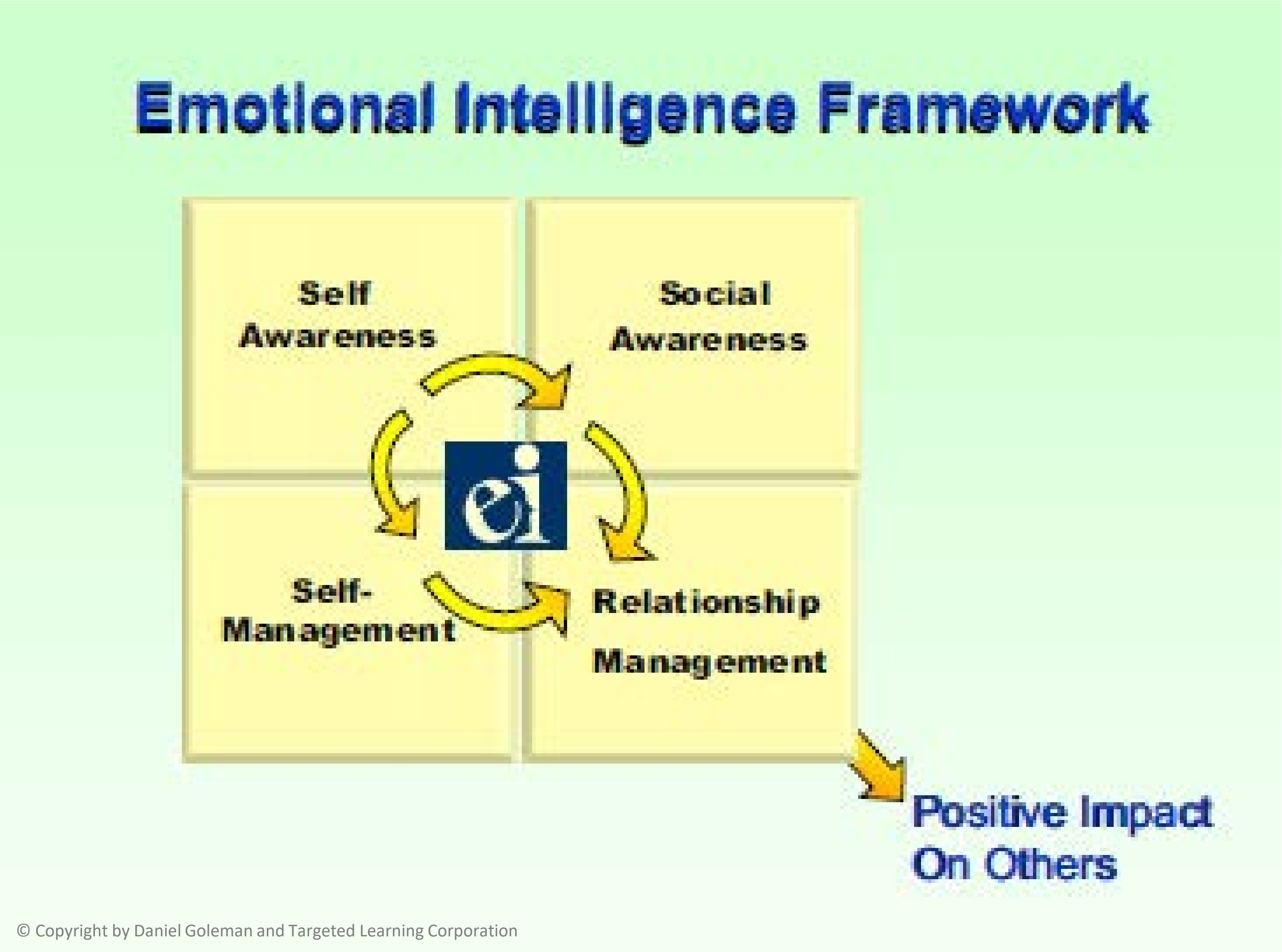
- Recognize and understand differences in people’s styles
- Understand the needs, strengths, and expectations of each style
- Adapt the way you work with others to increase effectiveness, productivity, and security

Social Engineering for Chemical Security

Connecting Emotional Intelligence and Leadership



Emotional Intelligence Framework

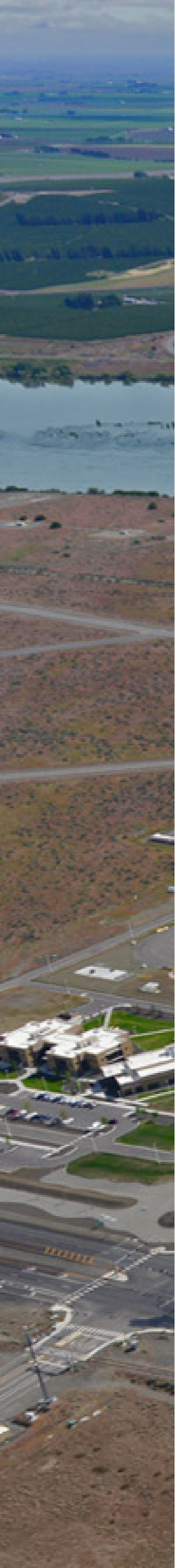


© Copyright by Daniel Goleman and Targeted Learning Corporation

Emotional intelligence (EI) set of skills that are thought to contribute to the appraisal of emotions in oneself and others

This helps to

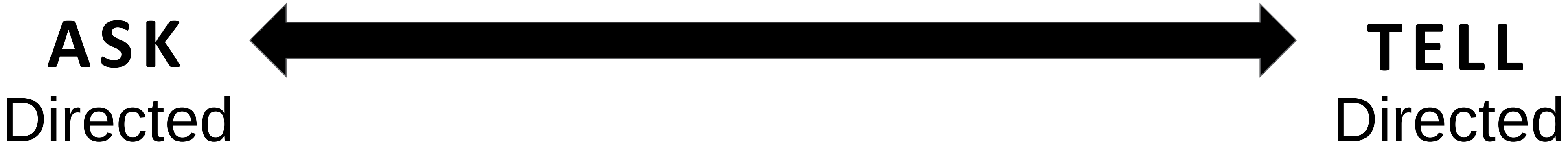
- better understand what motivates others
- helps work more cooperatively with others
- helps improving the overall security culture

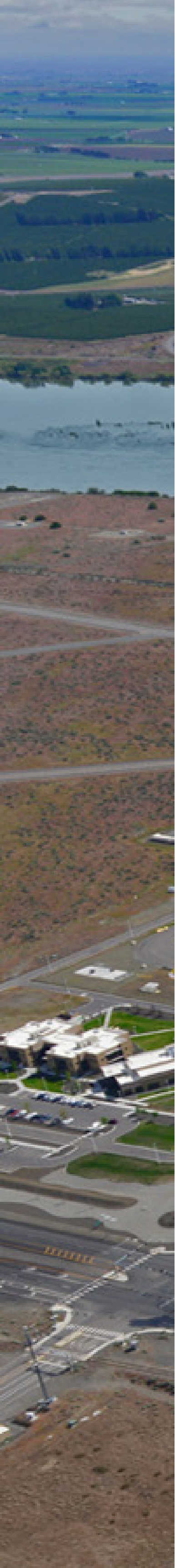


Assertiveness

Assertiveness is the antidote to fear, shyness, passivity, and even anger

The way in which a person is perceived as attempting to influence the thoughts and actions of others

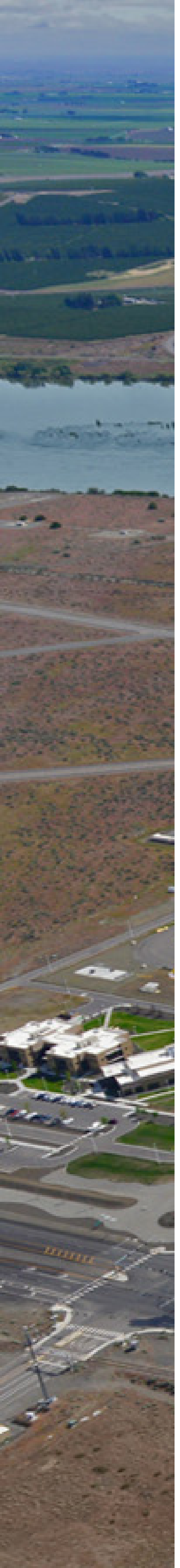




Pacific Northwest NATIONAL LABORATORY

Assertiveness

ASK Directed		**TELL** Directed	
Approach:	Indirect	**Approach:**	Direct
Statements:	Conditional	**Statements:**	Declarative
Questions:	More	**Questions:**	Fewer
Pace:	Slower	**Pace:**	Faster
Interruption:	Fewer	**Interruption:**	Many
Body Position:	Leans Back	**Body Position:**	Leans Forward
Volume:	Quieter	**Volume:**	Louder
Eye Contact:	Less Direct	**Eye Contact:**	More Direct
Decisions:	Takes Time	**Decisions:**	Responds Quickly



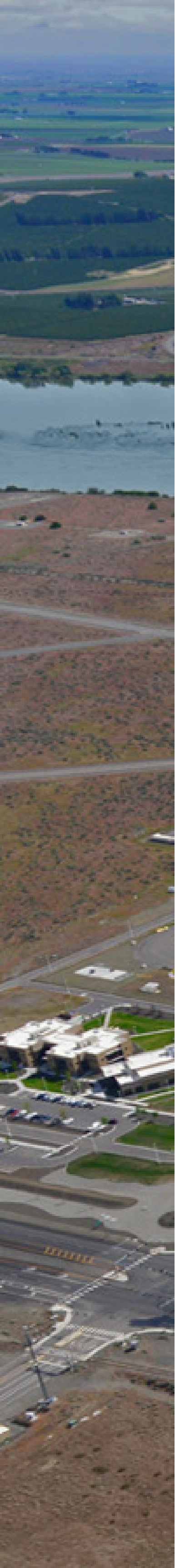
Pacific Northwest
NATIONAL LABORATORY

ASK or TELL ?

ASK
Directed

TELL
Directed

Ask	Speaks deliberately, often pausing
Tell	Make declarative statements
Tell	Speaks quickly and often firmly
Ask	Seldom interrupts others
Ask	Seldom uses voice to emphasize



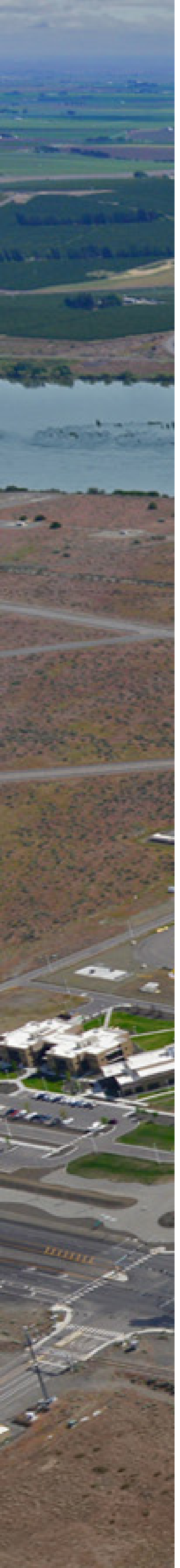
Pacific Northwest
NATIONAL LABORATORY

ASK or TELL ?

ASK ⟷ **TELL**

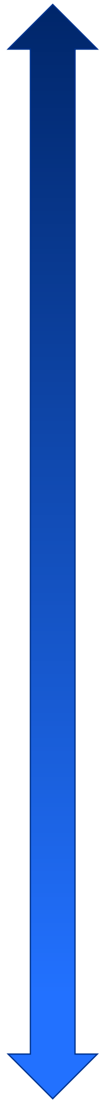
Directed ⟷ Directed

Ask	Makes many conditional statements
Tell	Often interrupts others
Tell	Uses voice to emphasize
Ask	Tends to lean back
Tell	Tends to lean forward



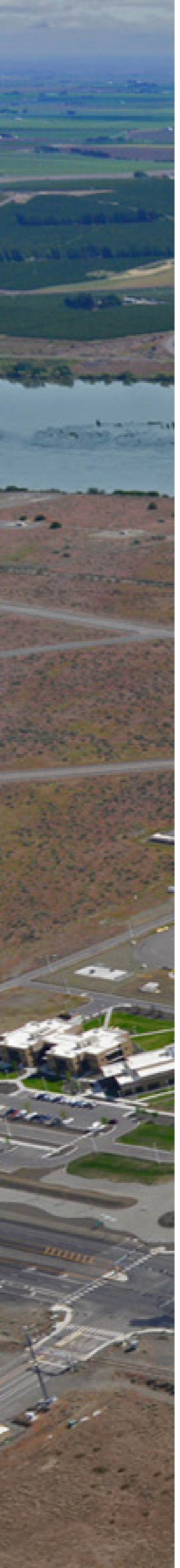
Responsiveness

The way in which a person is perceived as expressing feelings when relating to others

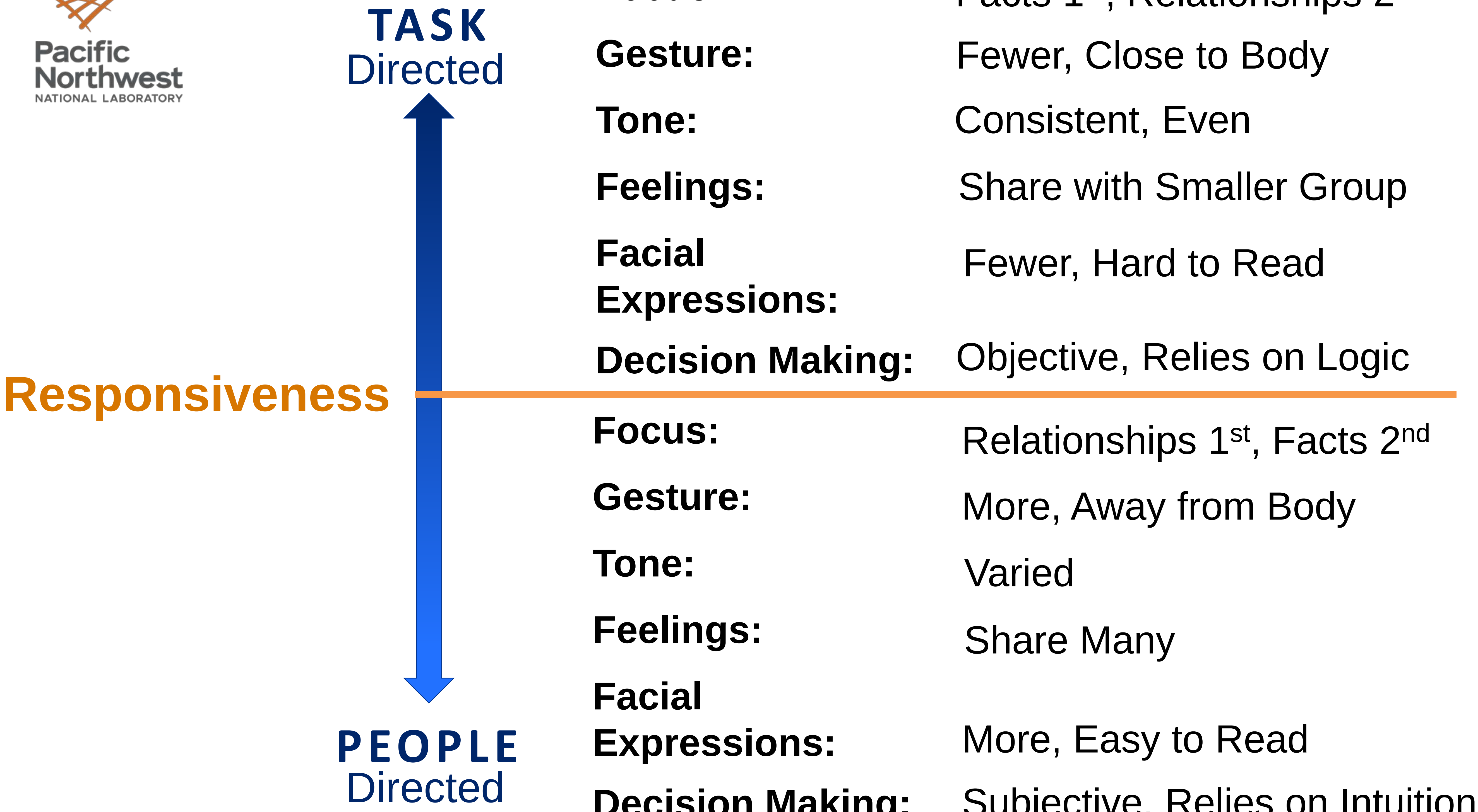


TASK
Directed

PEOPLE
Directed



Pacific Northwest NATIONAL LABORATORY



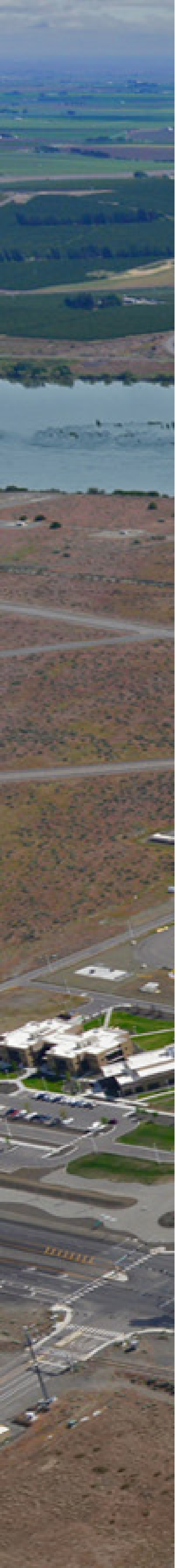
TASK Directed

Focus:	Facts 1st, Relationships 2nd
Gesture:	Fewer, Close to Body
Tone:	Consistent, Even
Feelings:	Share with Smaller Group
Facial Expressions:	Fewer, Hard to Read
Decision Making:	Objective, Relies on Logic

Responsiveness

Focus:	Relationships 1st, Facts 2nd
Gesture:	More, Away from Body
Tone:	Varied
Feelings:	Share Many
Facial Expressions:	More, Easy to Read
Decision Making:	Subjective, Relies on Intuition

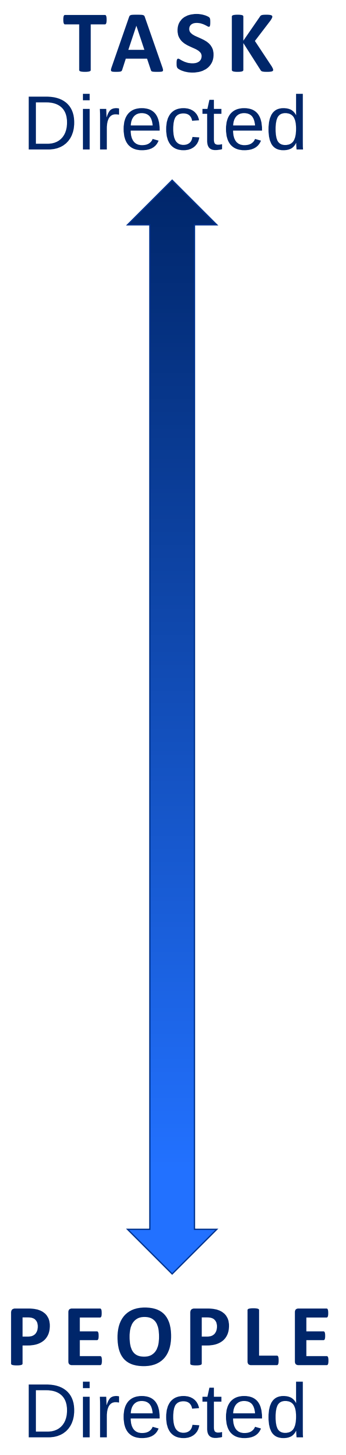
PEOPLE Directed



Pacific Northwest NATIONAL LABORATORY

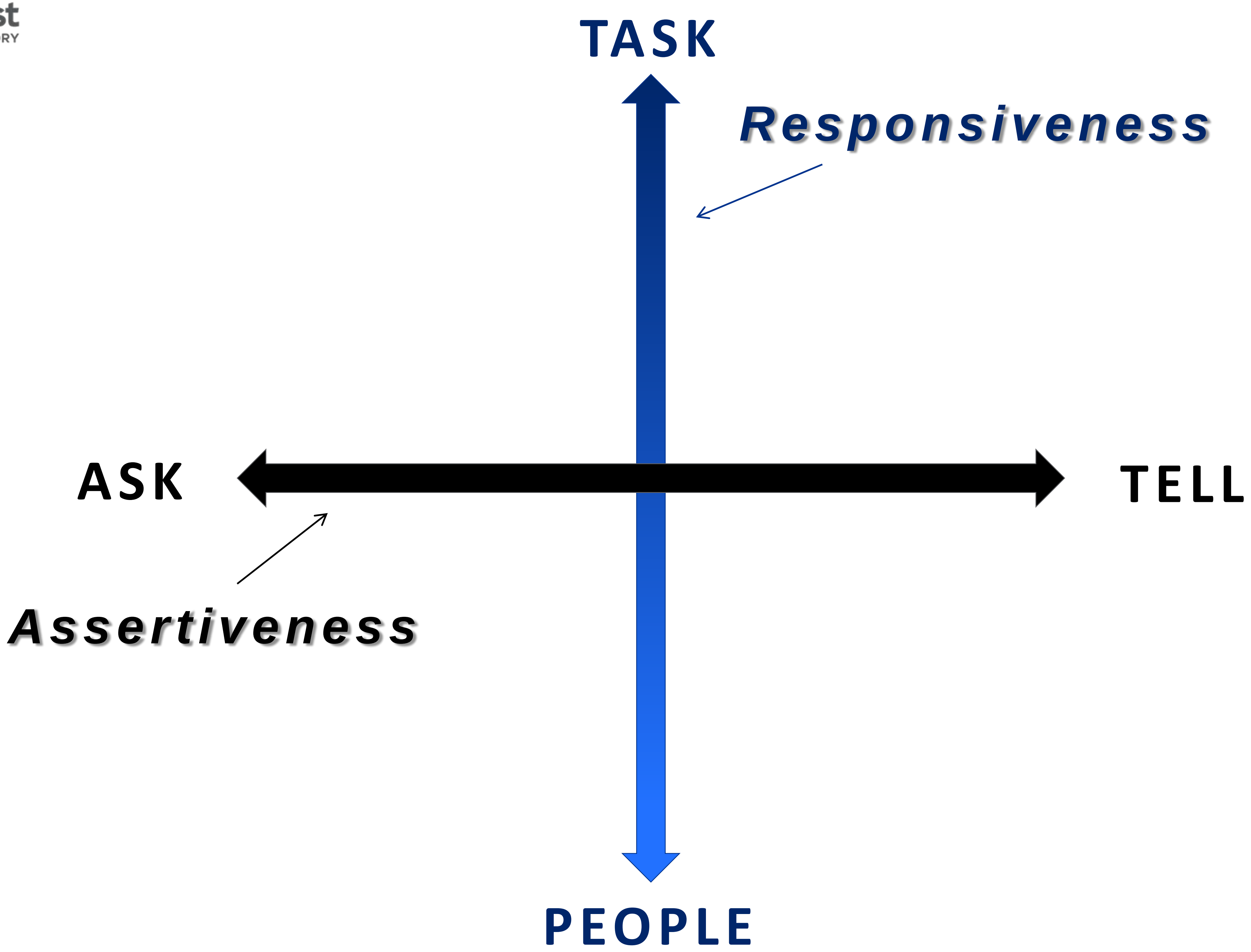
Task or People?

People	Uses broad, expansive body gestures
Task	Talks about tasks and facts
People	Talks more about people and relationships
Task	Uses minimal body gestures
Task	Exposes a narrow range of personal feelings to others


TASK Directed

PEOPLE Directed

The Social Style Model



TASK

Responsiveness

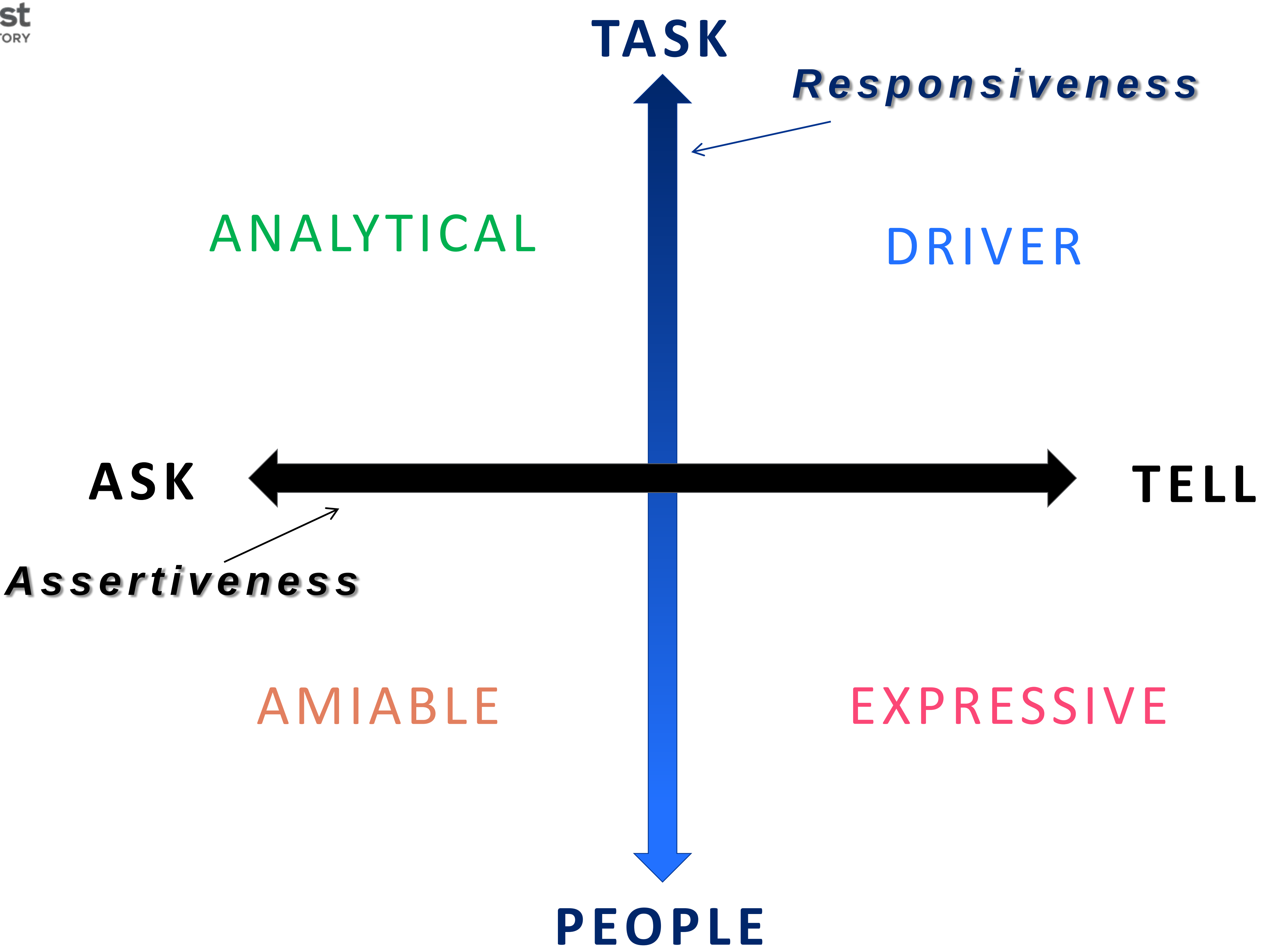
ASK

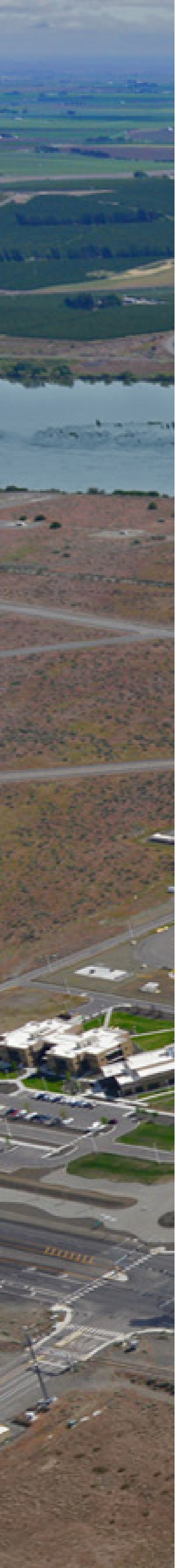
TELL

Assertiveness

PEOPLE

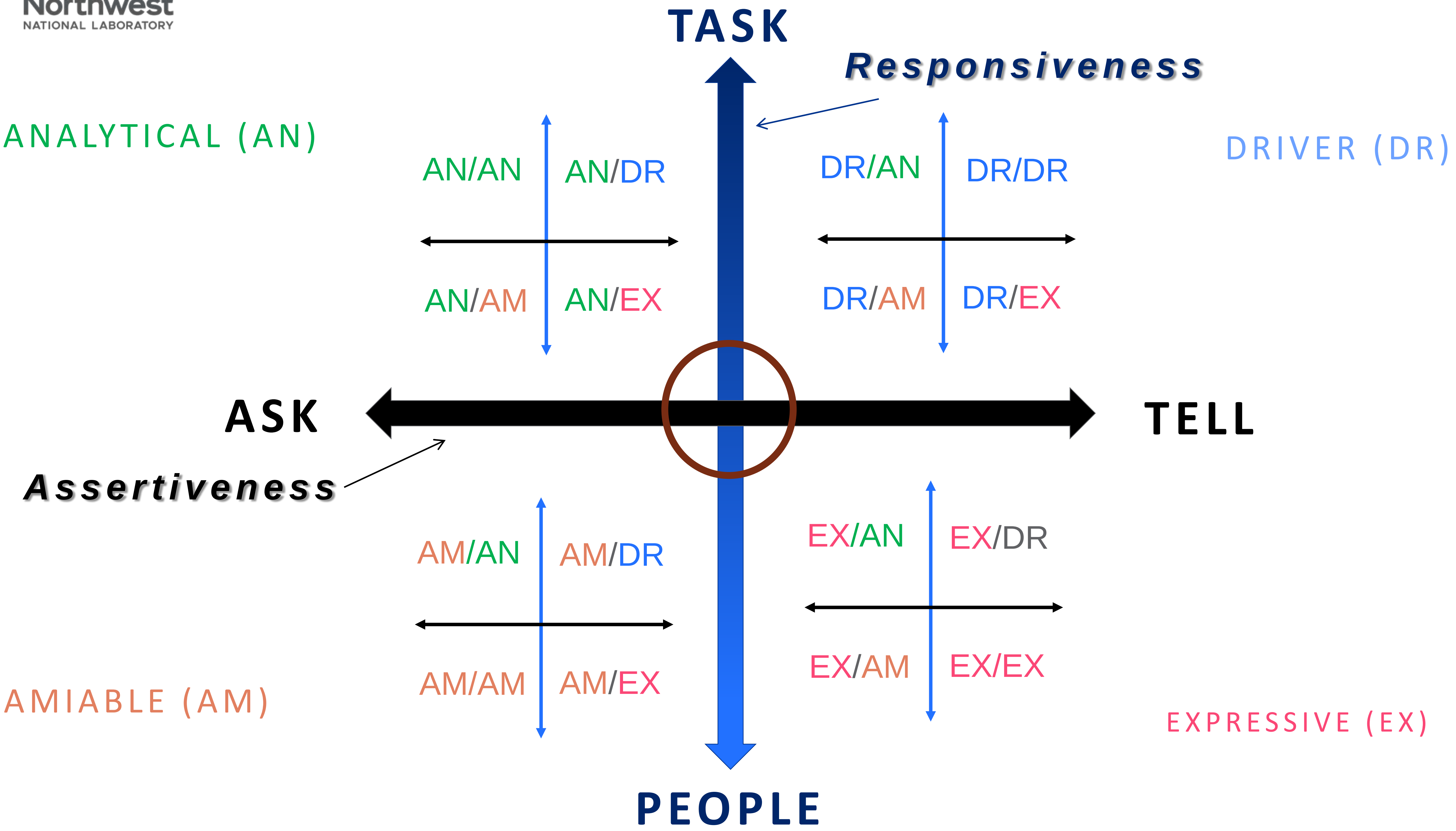
The Social Style Model





Pacific Northwest
NATIONAL LABORATORY

The Social Style Model



TASK

Responsiveness

ANALYTICAL (AN)

DRIVER (DR)

AN/AN

AN/DR

AN/AM

AN/EX

DR/AN

DR/DR

DR/AM

DR/EX

ASK

TELL

Assertiveness

AM/AN

AM/DR

AM/AM

AM/EX

EX/AN

EX/DR

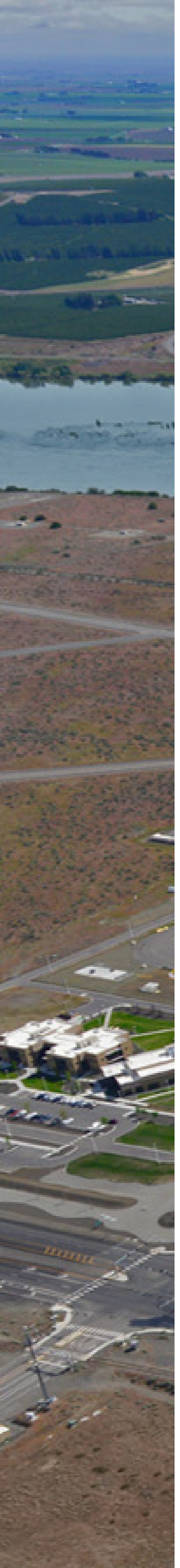
EX/AM

EX/EX

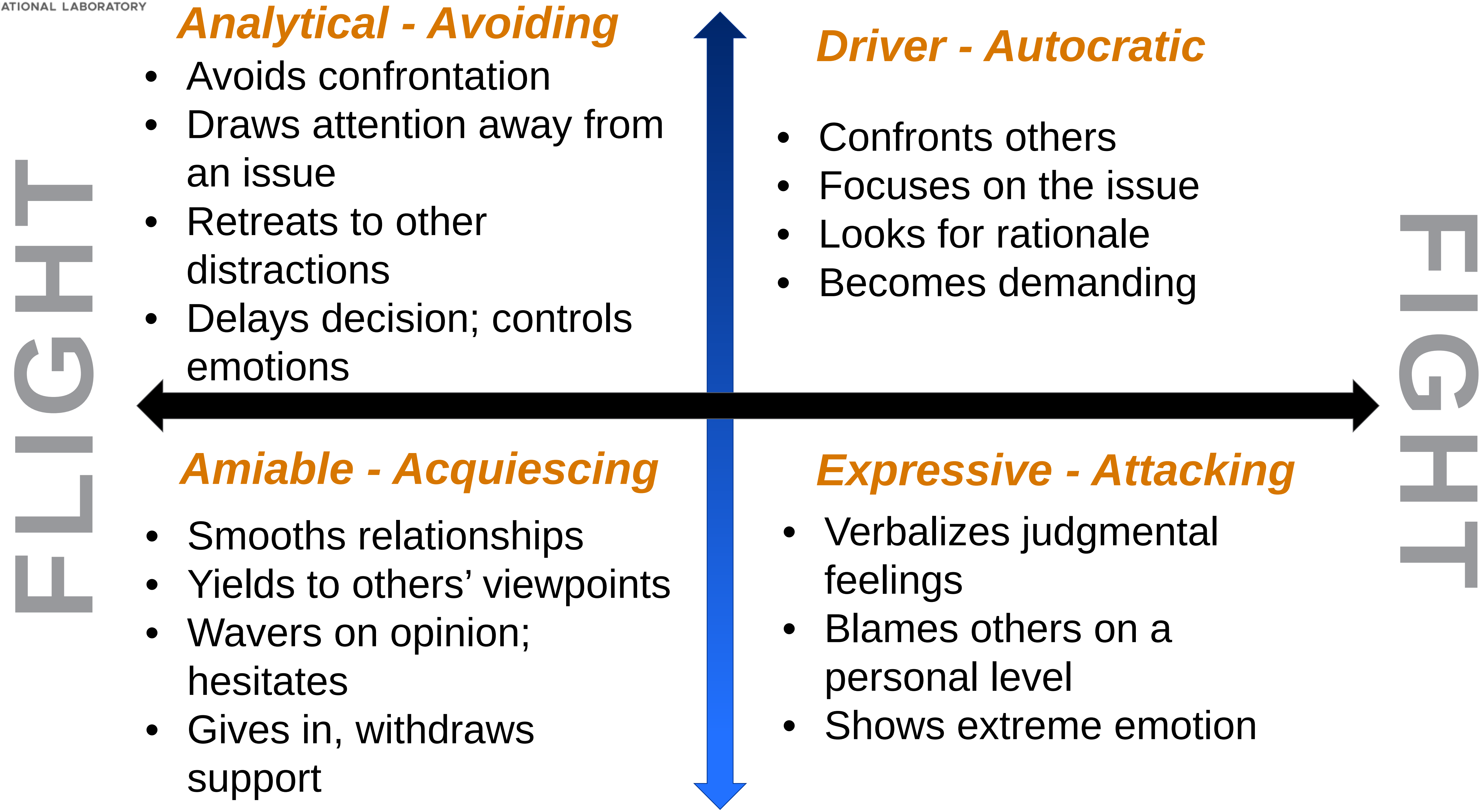
AMIABLE (AM)

EXPRESSIVE (EX)

PEOPLE



Back-up Behaviors



Analytical - Avoiding

- Avoids confrontation
- Draws attention away from an issue
- Retreats to other distractions
- Delays decision; controls emotions

Driver - Autocratic

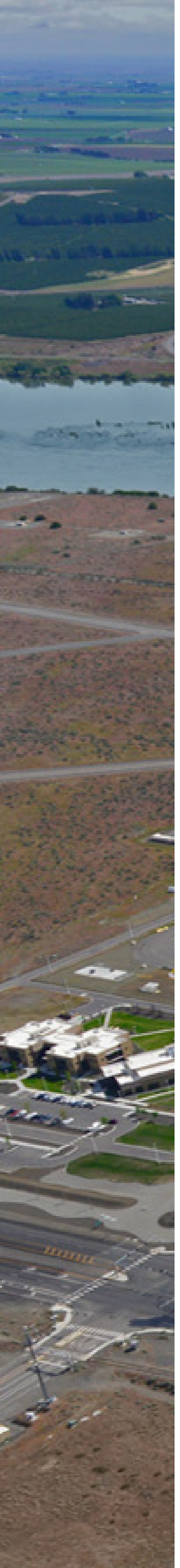
- Confronts others
- Focuses on the issue
- Looks for rationale
- Becomes demanding

Amiable - Acquiescing

- Smooths relationships
- Yields to others’ viewpoints
- Wavers on opinion; hesitates
- Gives in, withdraws support

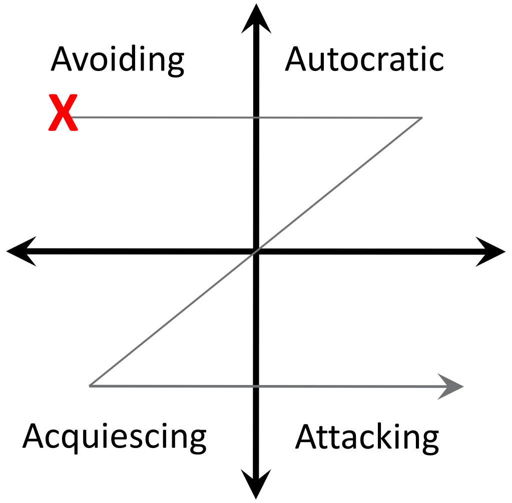
Expressive - Attacking

- Verbalizes judgmental feelings
- Blames others on a personal level
- Shows extreme emotion

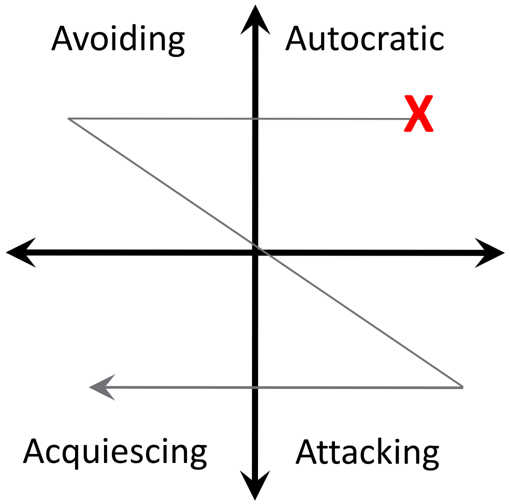


Z-Patterns

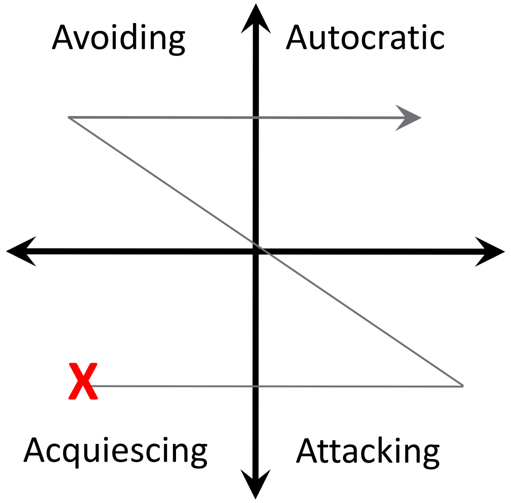
Analytical Z Pattern



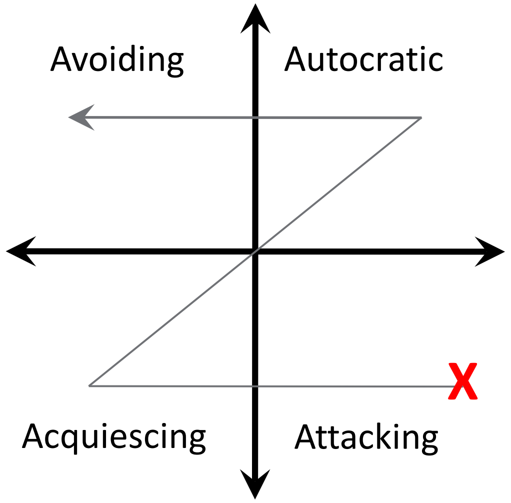
Driver Z Pattern

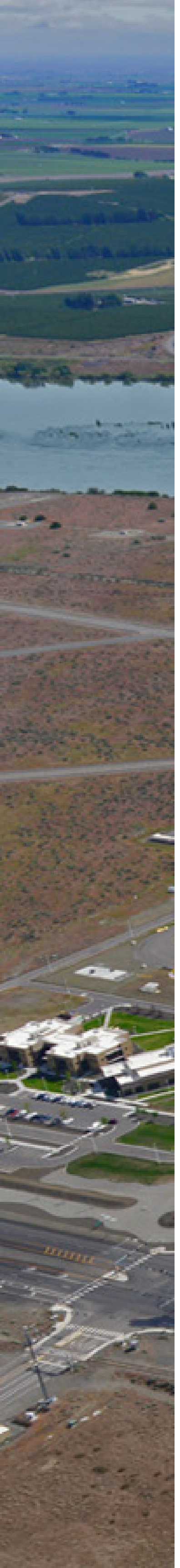


Amiable Z Pattern

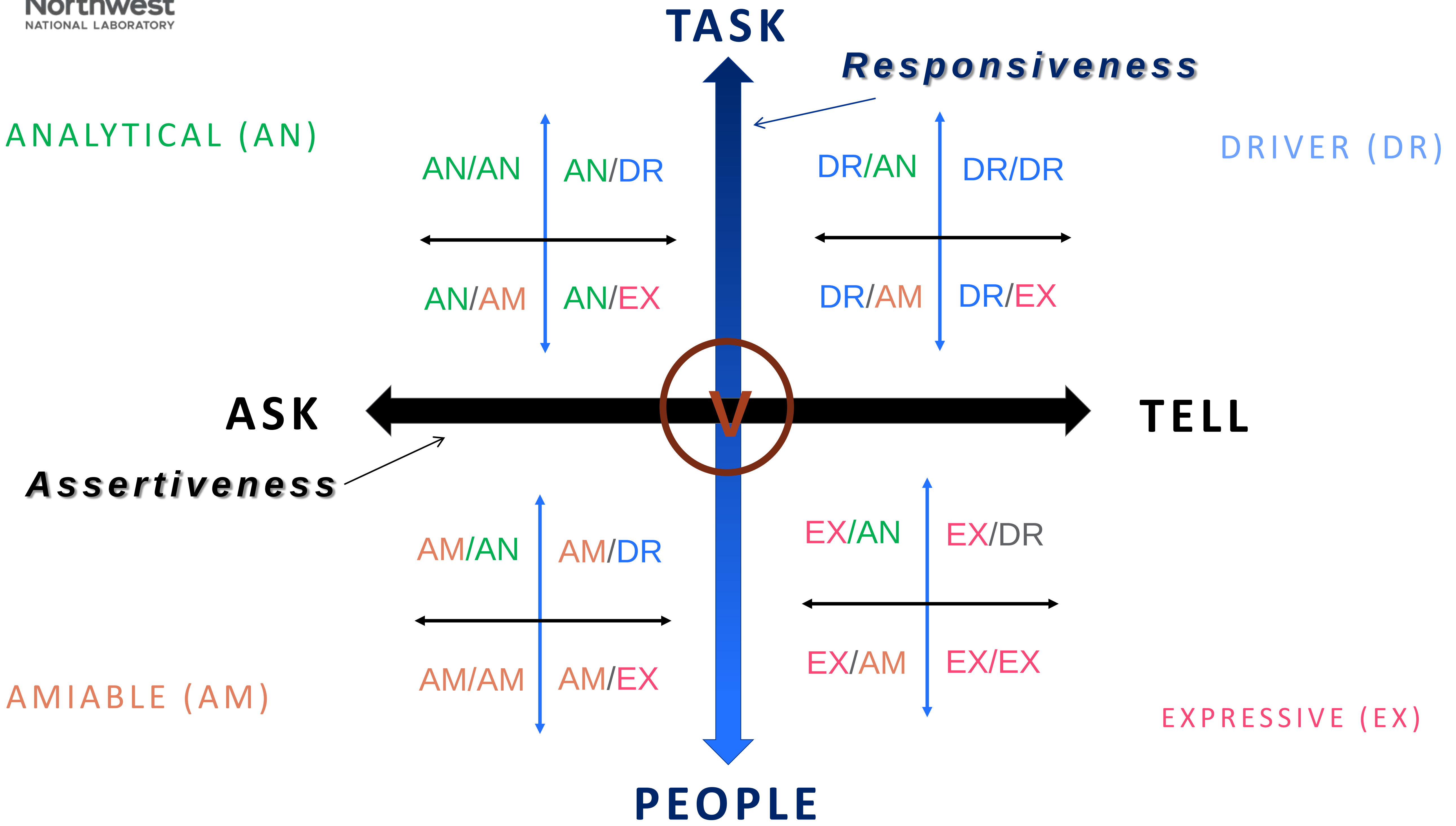


Expressive Z Pattern





The Social Style Model



TASK

Responsiveness

ANALYTICAL (AN)

AN/AN AN/DR

AN/AM AN/EX

DR/AN DR/DR

DR/AM DR/EX

DRIVER (DR)

ASK

V

TELL

Assertiveness

AM/AN AM/DR

AM/AM AM/EX

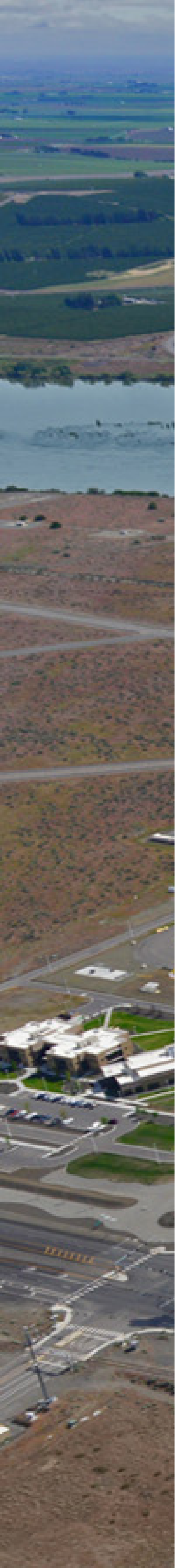
EX/AN EX/DR

EX/AM EX/EX

AMIABLE (AM)

EXPRESSIVE (EX)

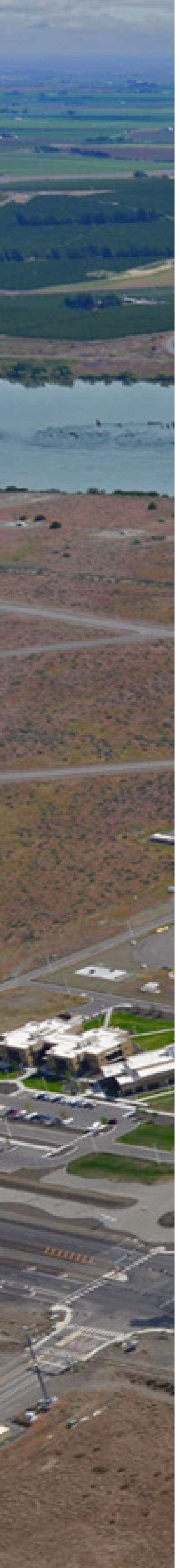
PEOPLE



What is Versatility?

VERSATILITY:

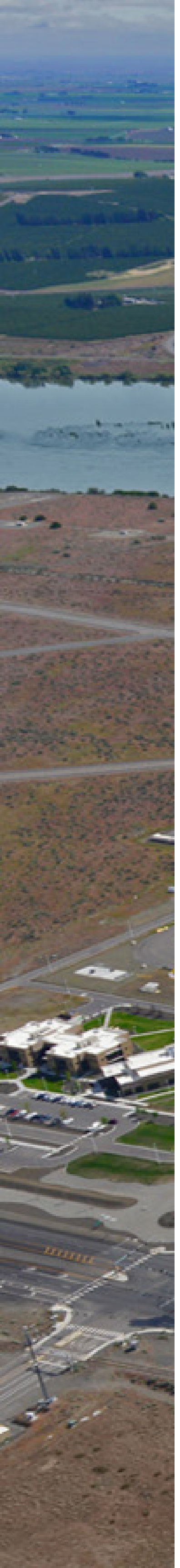
The ability to adapt one’s own behaviors to meet the concerns and expectations of others in order to create productive relationships



Versatility is a Stretch!

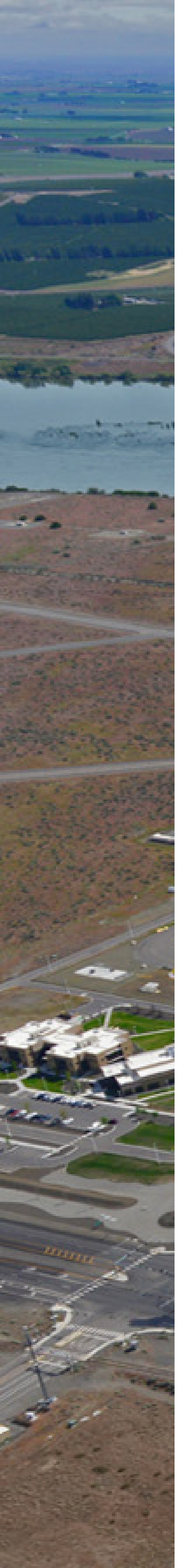
When you modify your behavior, you make a *temporary* adaptation of your own behaviors.

You do not become the other person’s style.



Versatility is a Choice

- Do I need this relationship to work? (relation to safe and secure work)
- What are the benefits?
- What are the risks?
- Is this the best time?



Pacific Northwest
NATIONAL LABORATORY

Ways to Modify

Pace

The speed of your speech and physical movements

Voice

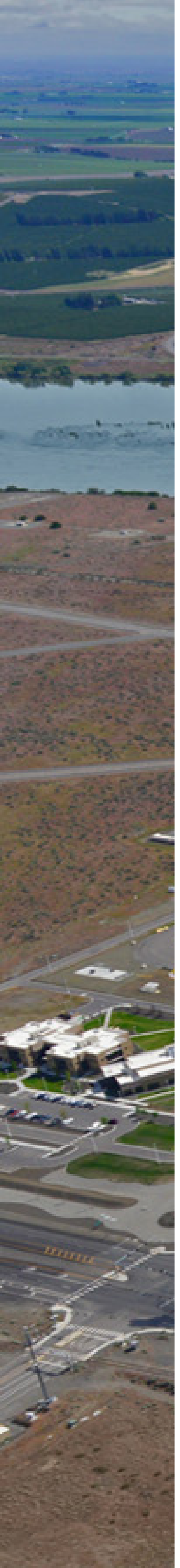
The use of emphasis, tone, and volume

Body Language

The use of gestures, facial expressions, and interpersonal distance

Focus/Content

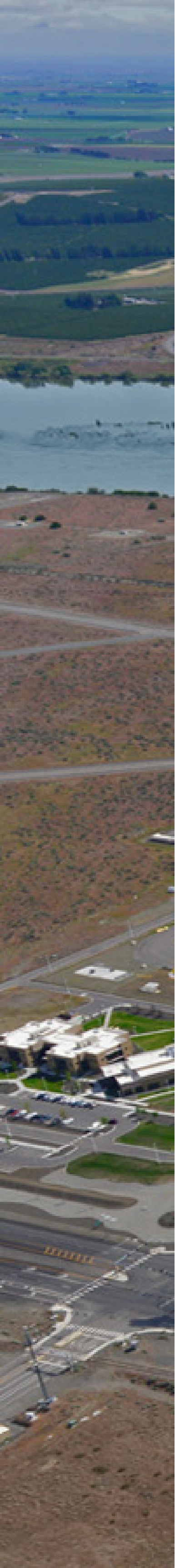
The discussion topics and priorities



When working with others, why is it important to be good at communication and building relationships?

What challenges do you face in communicating with others and building productive relationships?

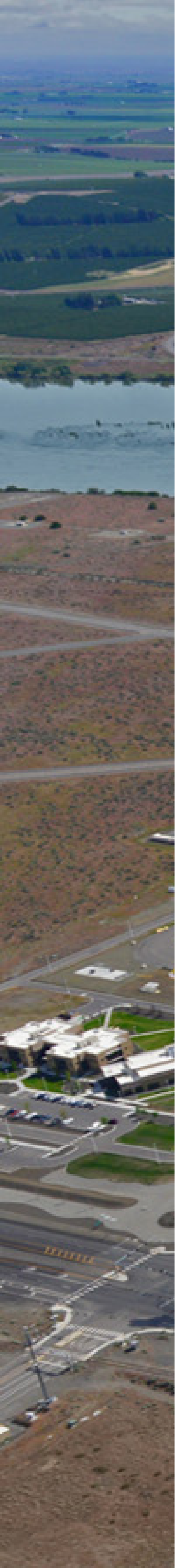
How this can improve both safety and security culture



Summary

- Social engineering is becoming an integral part (or important aspect) in enhancing the safety and security culture!
- Effective leaders leverage their emotional intelligence.
- Focusing on behavior allows us to understand the other person’s needs (will help in security needs/enhancements)
- Versatility is a choice we make about modifying our behavior to increase effectiveness, productivity, and results when communicating with others, while staying true to who we are as individuals.

Pacific Northwest
NATIONAL LABORATORY



Thank you

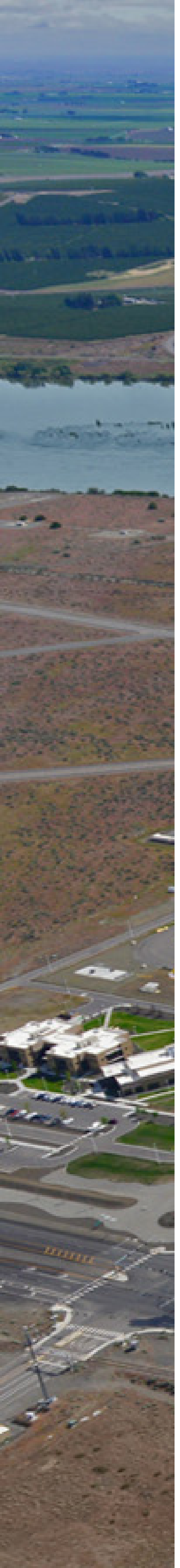
If you have any further questions:

Radhakishan.Motkuri@pnnl.gov

Lesson 7:
Assessing Chemical Security

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

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

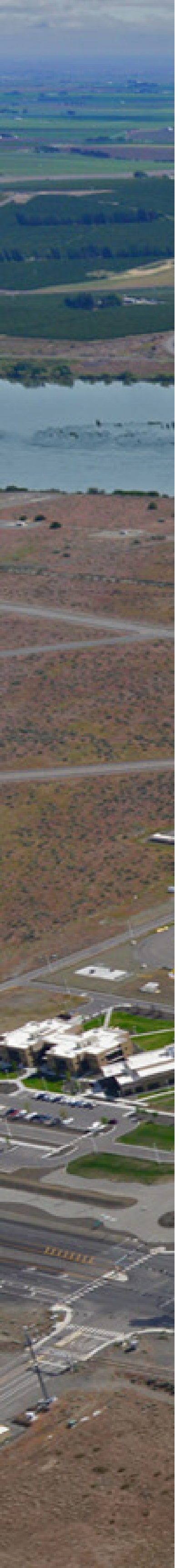


Presentation Topics

- Introduction
- What is a maturity model?
- The Chemical Security Assessment Model (CSAM)

Sri Nikhil Gupta Gourisetti

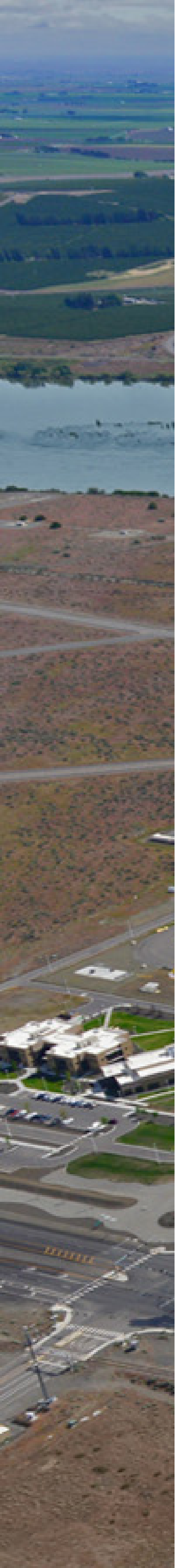
- I am a PNNL senior research scientist
- Specialized knowledge and interests in:
  - Maturity modeling for risk assessment and management
  - Industrial Control Systems (ICS) cyber security
  - Critical Infrastructure Security
  - Software engineering
  - Power systems modeling & simulation
  - Physics-driven machine learning systems
  - Blockchain technologies.
- PhD, Masters, and Bachelor of Science from the University of Arkansas



Maturity Models

Maturity Model Definition:

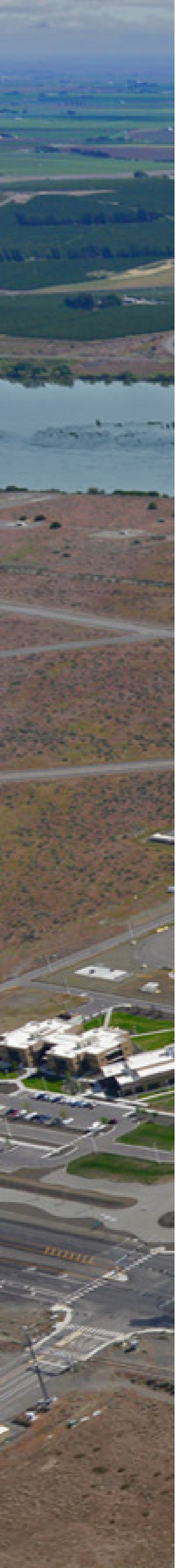
- An organized way to convey a path of experience, wisdom, perfection, or acculturation.
- The Lego example…



Progression Model: Two Simple Examples

Progression for Counting
Computer
Calculator
Adding machine
Slide rule
Abacus
Pencil & paper
Fingers

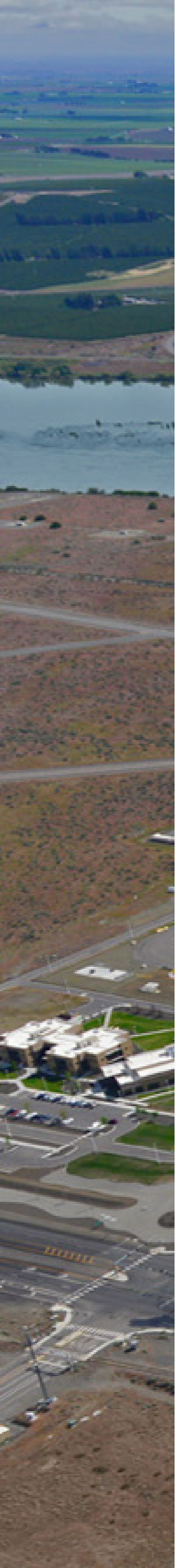
Progression for Human Mobility
Fly
Sprint
Run
Jog
Walk
Crawl



Capability Maturity Model: Example of Increasing Maturity

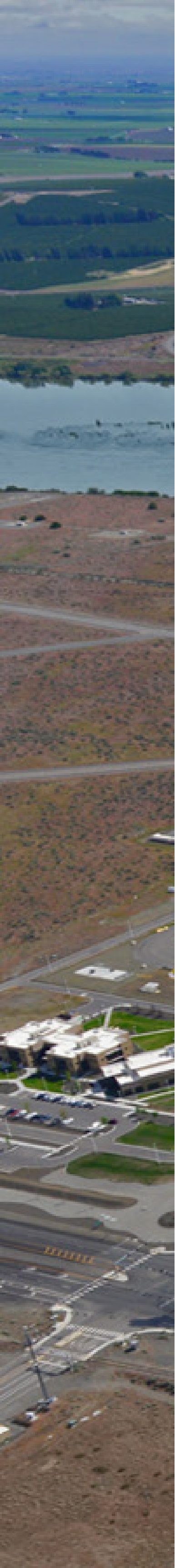
Example 1
Practices are optimized
Practices are quantitatively managed
Practices are defined
Practices are managed
Practices are ad hoc

Example 2
Practices are shared
Practices are defined
Practices are measured
Practices are managed
Practices are planned
Practices are performed but ad hoc
Practices are incomplete



Overview of Maturity Models

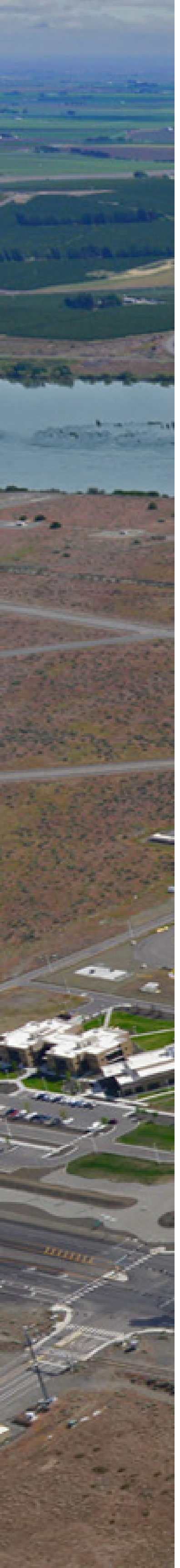
- **Challenge:** Develop capabilities to understand and **assess the security posture** of an organization.
- **Objectives:**
  - **Strengthen** security capabilities
  - Enable consistent **evaluation** and benchmarking of security capabilities
  - Share knowledge and best practices
  - Enable prioritized actions and **security investments**
- **Results:** Help decision makers determine the **adequacy** of their security program and identify areas for **improvement.**



PNNL Maturity Models Based on the Cybersecurity Capability Maturity Model (C2M2) Framework

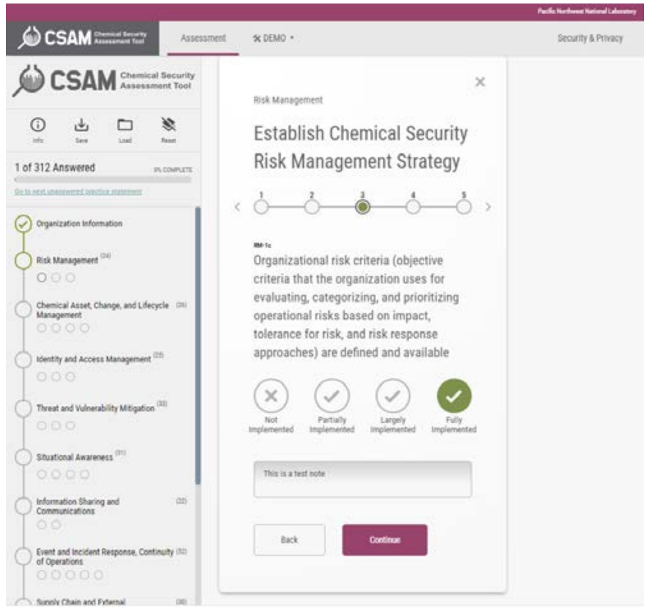
- The **Electricity Subsector C2M2** assesses an energy sector organization's cybersecurity programmatic maturity.
- The **Building Systems C2M2** assists building managers in evaluating the maturity cybersecurity program for their building's digital control systems.
- The **Secure Design and Development C2M2** is designed to assess the cybersecurity maturity of their design and development processes of assist product vendors, hardware designers, software and firmware developers, and software/hardware integrators.
- The **Facility Cybersecurity Framework** (FCF) suite of maturity models provides tools to assess the cybersecurity maturity of facilities based on different standards and guidance:
- The **Transmission Resiliency Maturity Model** (TRMM) objectively evaluates and benchmarks transmission resiliency policies, programs, and investments.

https://www.pnnl.gov/pnnl-maturity-models



Today We Introduce Two New Maturity Models

- The **Chemical Security Assessment Model (CSAM)** is designed to assist chemical facilities and laboratories in identifying the maturity of the chemical security program, and to identify programmatic areas to strengthen and maintain a desired level of security throughout the chemical life cycle.



Pacific Northwest National Laboratory
CSAM Chemical Security Assessment Tool
Assessment
DEMO
Security & Privacy
Info
Save
Load
Reset
Organization Information
Risk Management (24)
Chemical Asset, Change, and Lifecycle Management (26)
Identity and Access Management (25)
Threat and Vulnerability Mitigation (33)
Situational Awareness (31)
Information Sharing and Communications (22)
Event and Incident Response, Continuity of Operations (32)
Supply Chain and External (38)
1
2
3
4
5
Not Implemented
Partially Implemented
Largely Implemented
Fully Implemented
Back
Continue

1 of 312 Answered 0% COMPLETE

Go to next unanswered practice statement

Risk Management

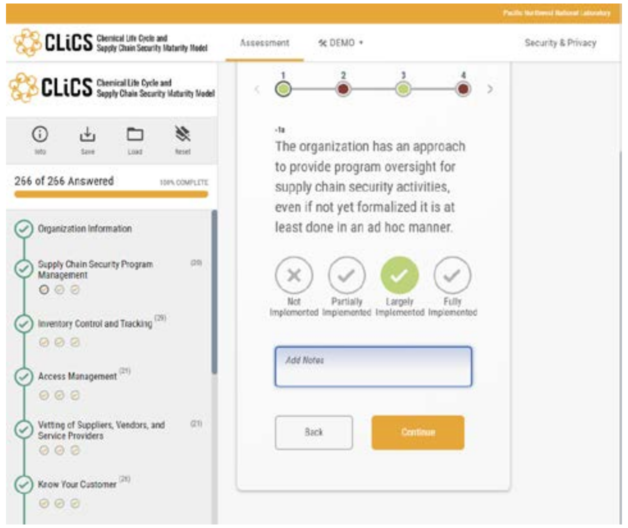
Establish Chemical Security Risk Management Strategy

RM-1c

Organizational risk criteria (objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact, tolerance for risk, and risk response approaches) are defined and available

This is a test note

- The **Chemical Life Cycle and Supply Chain Security** (CLiCS) Maturity Model focuses on chemical security throughout the product life cycle, with an emphasis on supply chain and “know your customer” security objectives.



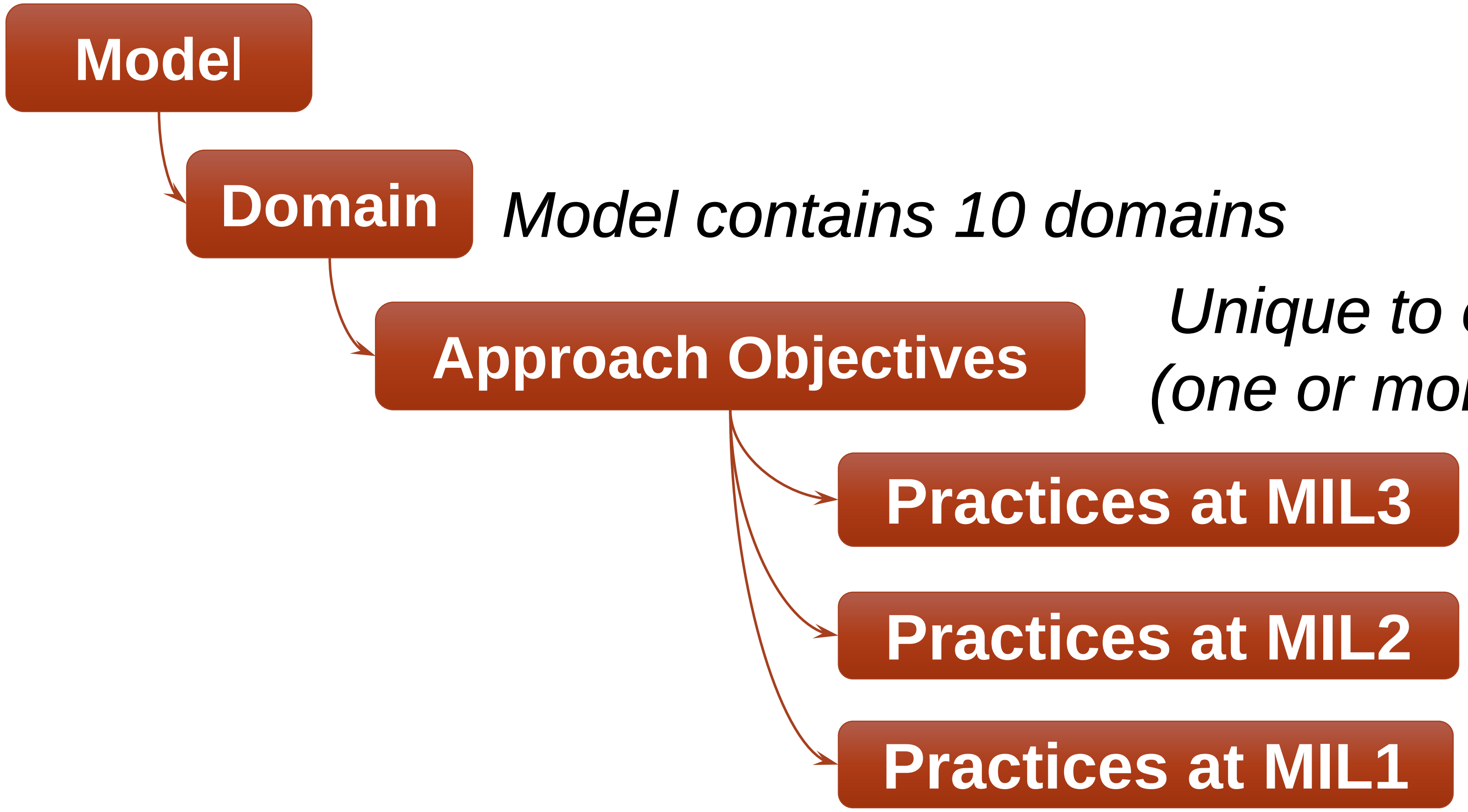
Pacific Northwest National Laboratory
CLiCS Chemical Life Cycle and Supply Chain Security Maturity Model
Assessment
DEMO
Security & Privacy
Info
Save
Load
Reset
Organization Information
Supply Chain Security Program Management (20)
Inventory Control and Tracking (29)
Access Management (21)
Vetting of Suppliers, Vendors, and Service Providers (21)
Know Your Customer (26)
1
2
3
4
Not Implemented
Partially Implemented
Largely Implemented
Fully Implemented
Add Notes
Back
Continue

266 of 256 Answered 100% COMPLETE

-1a

The organization has an approach to provide program oversight for supply chain security activities, even if not yet formalized it is at least done in an ad hoc manner.

Organization of the Maturity Models



Model

Domain

Model contains 10 domains

Approach Objectives

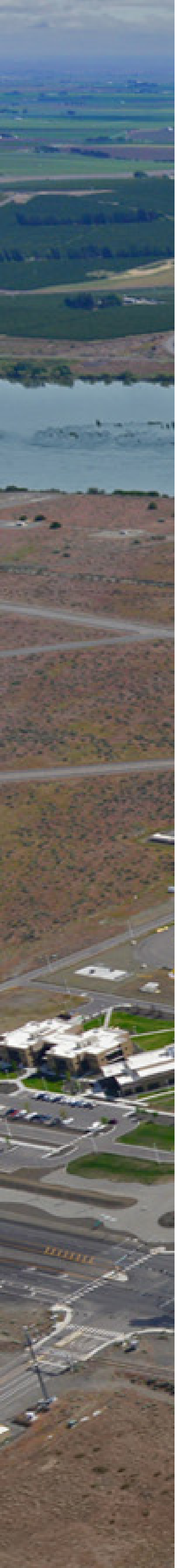
Unique to each domain (one or more per domain)

Practices at MIL3

Practices at MIL2

Practices at MIL1

Approach objectives are supported by a progression of practices that are unique to the domain

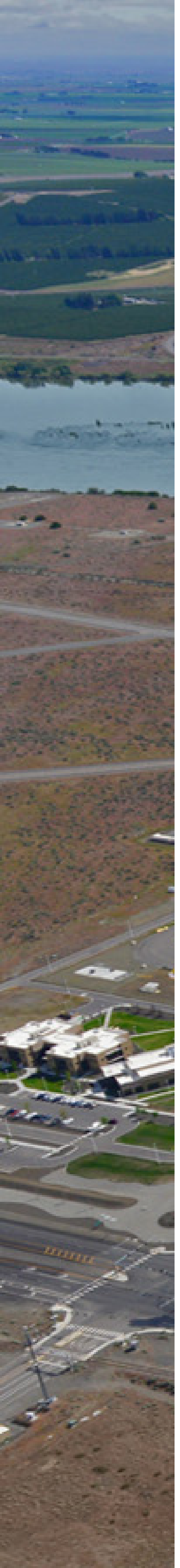


Pacific Northwest
NATIONAL LABORATORY

The CSAM Includes 10 Domains

RM	Risk Management
ACM	Asset, Change, and Lifecycle Management
IAM	Identity and Access Management
TVM	Threat and Vulnerability Management
SA	Situational Awareness
ISC	Information Sharing & Communications
IR	Event & Incident Response / Continuity of Operations
EDM	Supply Chain and External Dependencies Management
WM	Workforce Management
CPM	Chemical Security Program Management

Domains are logical groupings of cybersecurity practices



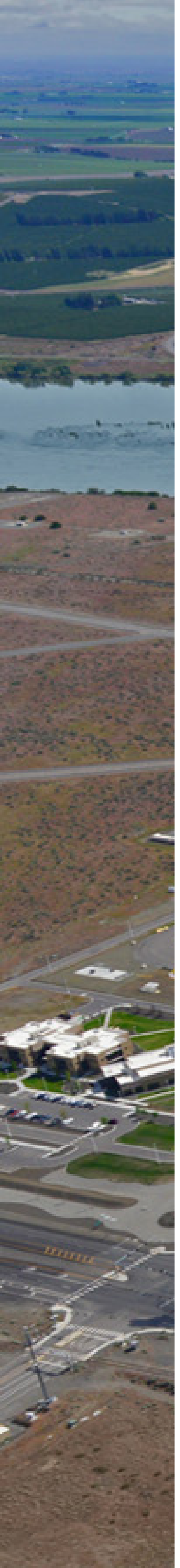
Maturity Indicator Level (MIL) Indicates the Maturity Level in Each Domain

MIL 3 - Guided & reviewed in conformance with policy. Responsibility and authority assigned to appropriately skilled personnel.

MIL 2 - Practices documented, stakeholders involved, and adequate resources provided and used

MIL 1 - Initial practices performed maybe in ad hoc manner (i.e., makeshift, improvised, undocumented)

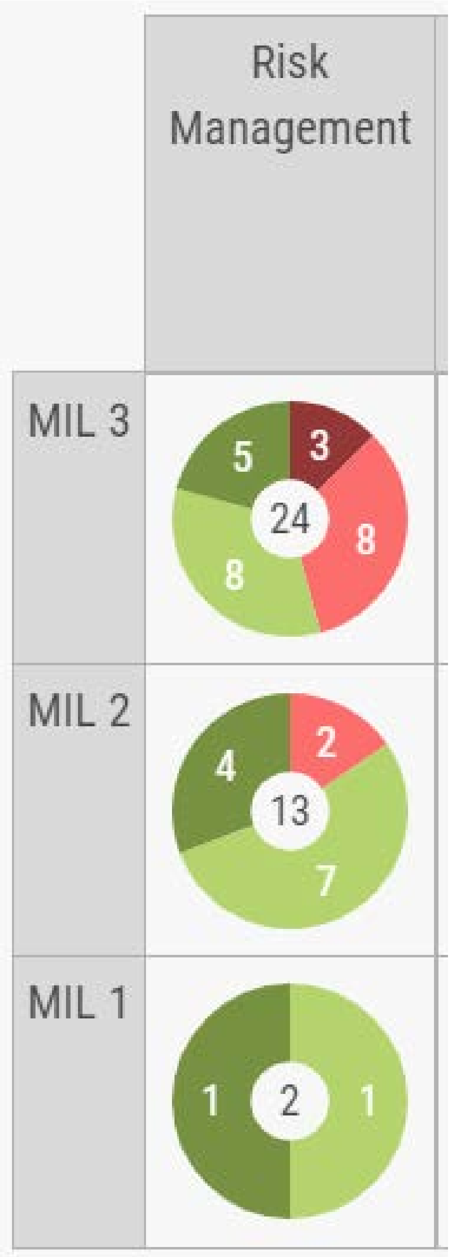
MIL 0 – Not Achieved



Each Domain Characterized by a Series of Practices.

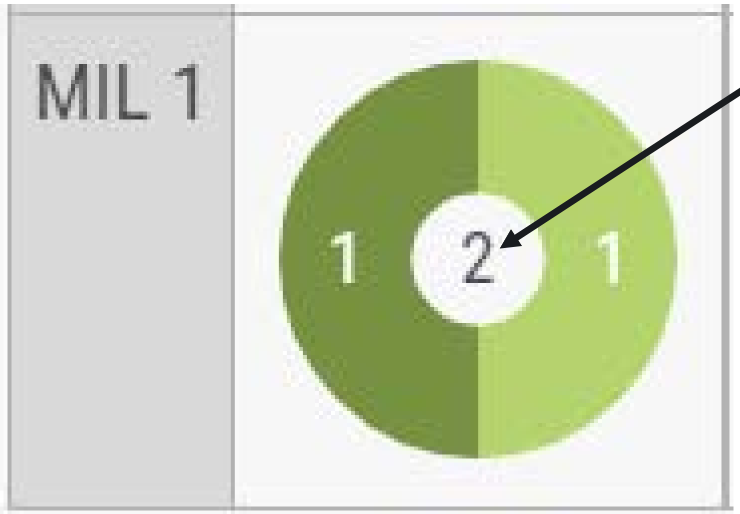
4-point answer scale	The organization’s performance of the practice described in the model is …
Fully Implemented (FI)	Complete
Largely Implemented (LI)	Complete, but with a recognized opportunity for improvement
Partially Implemented (PI)	Incomplete; there are multiple opportunities for improvement
Not Implemented (NI)	Absent; the practice is not performed in the organization

Sample Domain Scoring

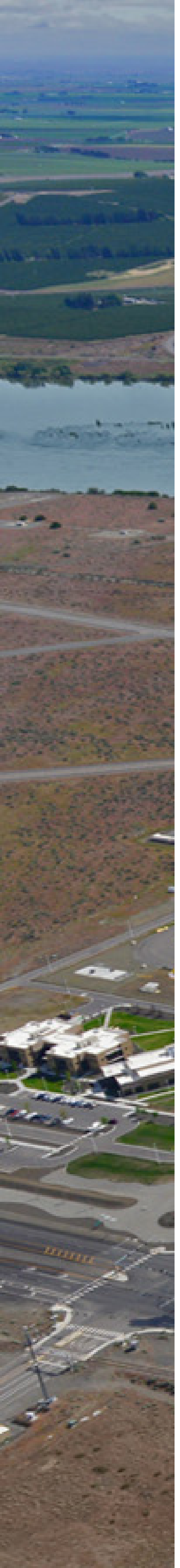


- We have assigned scores to each practice in the Risk Management domain based on our assessment of a sample facility. These are the distribution of scores for this domain.
- For a MIL level to be achieved, all the practices must have a dark or light green score. Any red or pink scores keep that MIL from being achieved.
- This domain has achieved MIL1 but is short of achieving MIL2

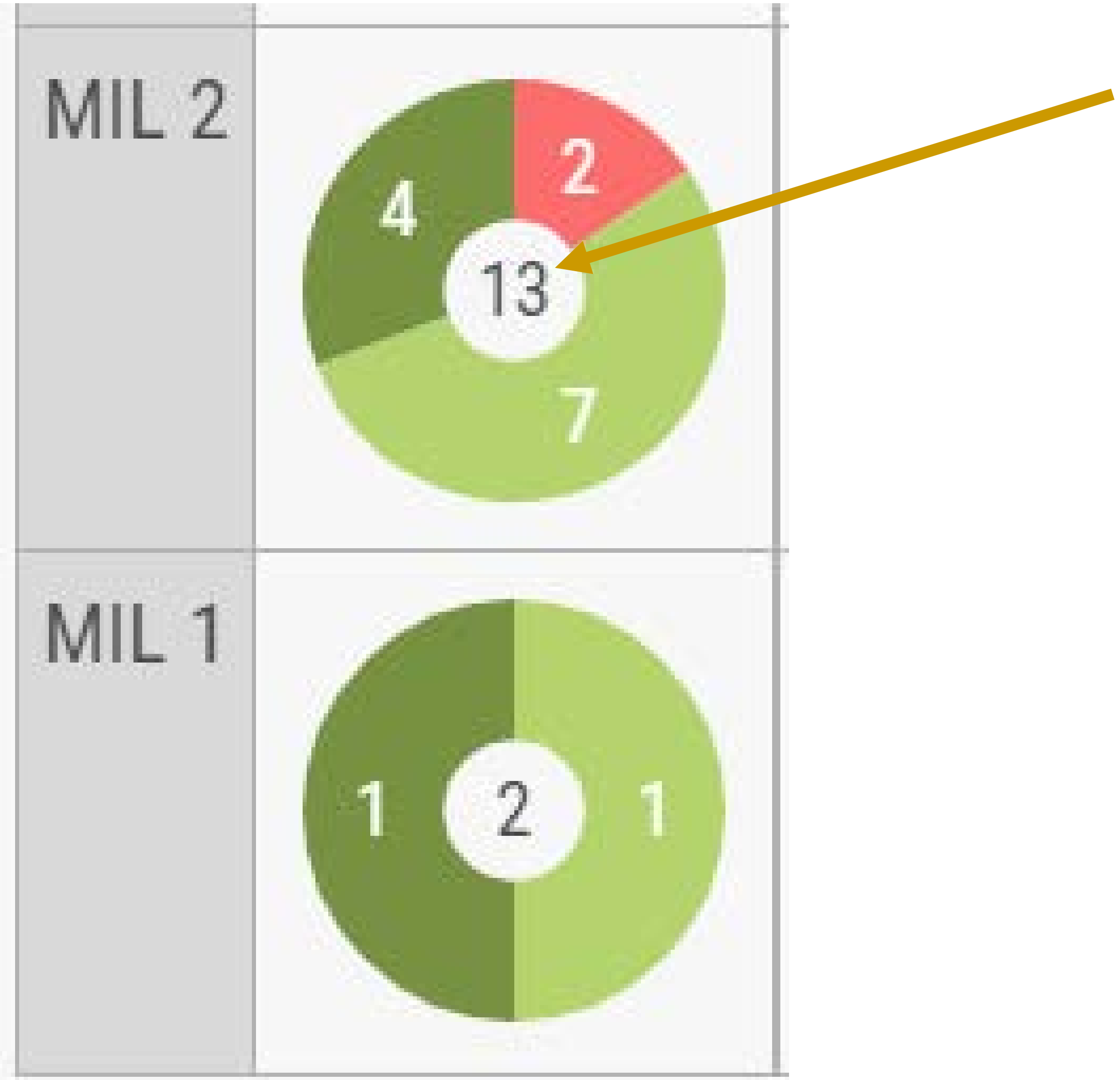
Sample Domain Scoring (cont.)



- For the Risk Management domain there are 2 practices at MIL1.
- 1 is “fully implemented” and 1 is “largely implemented”.
- There are no “partially” or “not implemented” practices.
- All the practices are “green”; therefore, MIL has been achieved

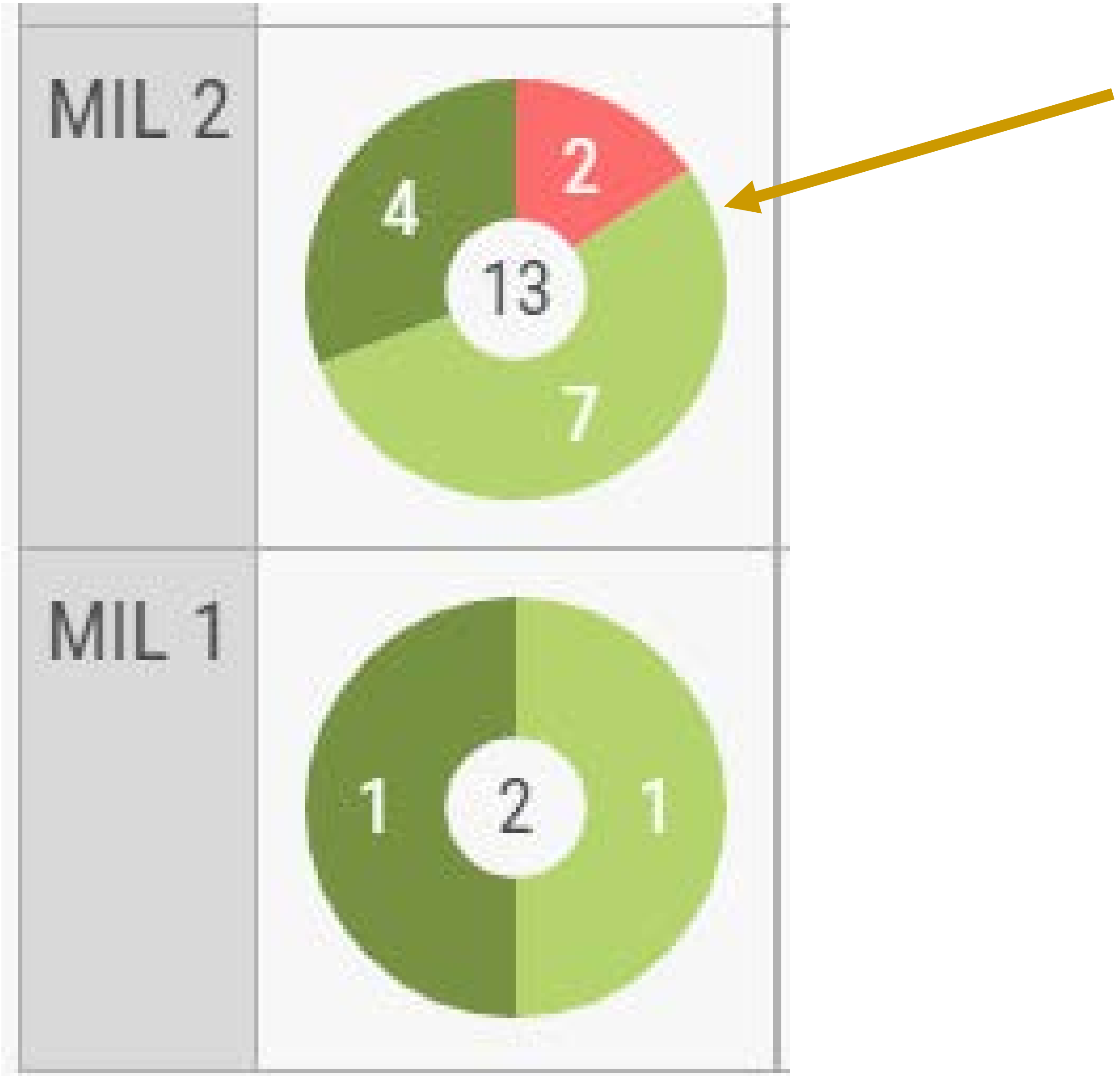


Sample Domain Scoring (cont.)



- There are a **total of 13** practices that need to be “fully” or “largely implemented” to achieve MIL2.
- 11 are MIL2 practices and 2 practices are carried upwards from MIL1
- You have to achieve all your MIL 1 practices before you can fully achieve MIL2)

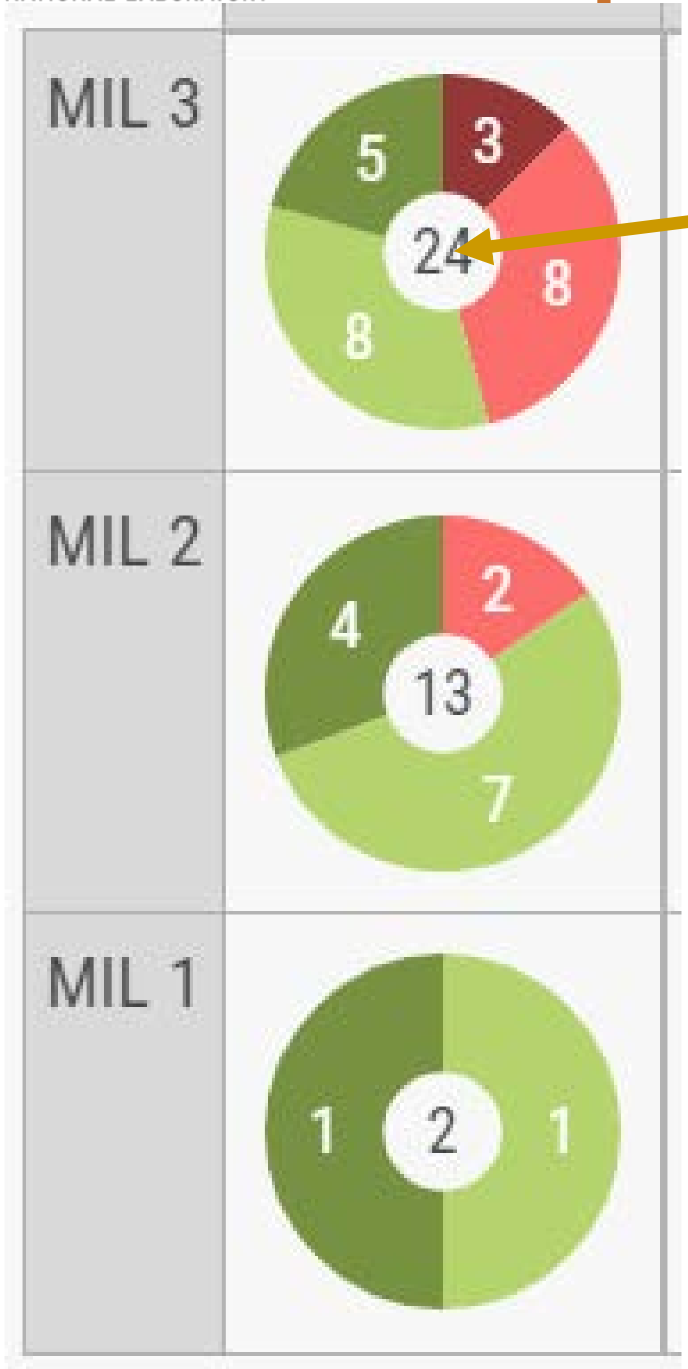
Sample Domain Scoring (cont.)



The status at MIL2:

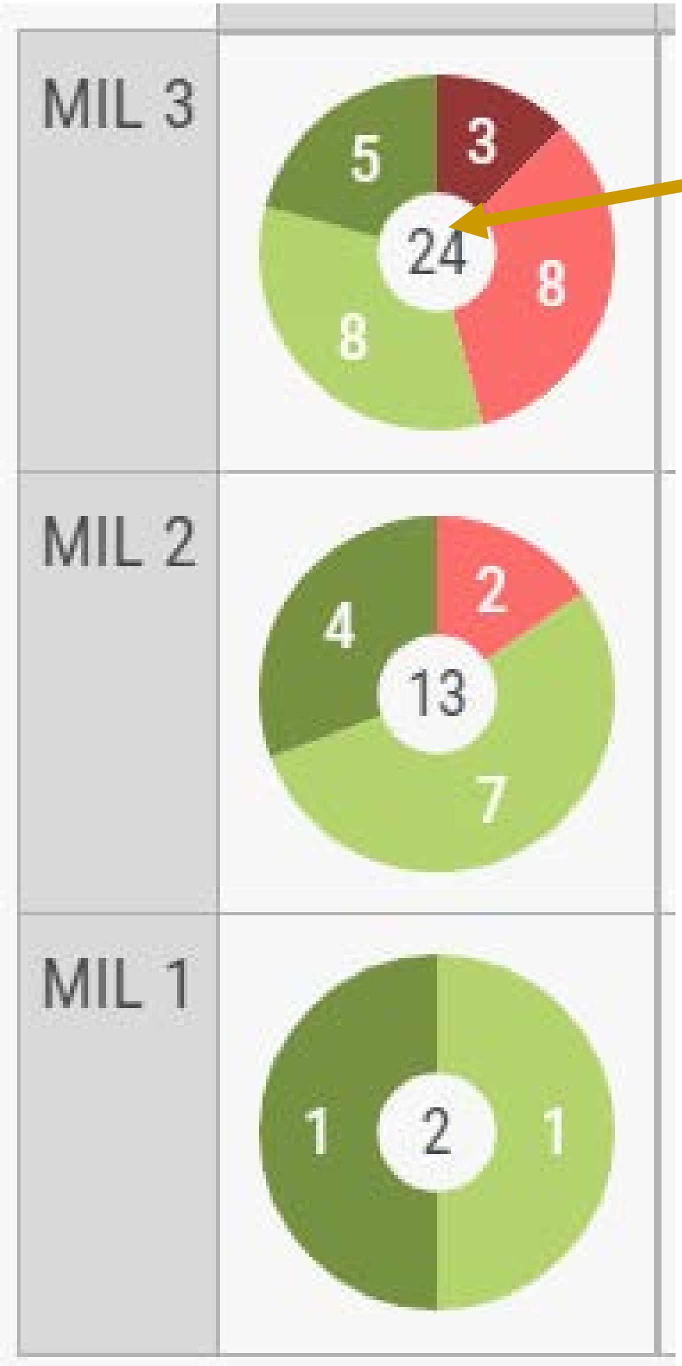
- 4 practices are “fully implemented”, including 1 inherited from MIL1.
- 7 practices are “largely implemented”, including 1 inherited from MIL1
- There are 2 “partially implemented” practices, all from MIL2.

Sample Domain Scoring (cont.)



- There are a **total of 24** practices that need to be “fully” or “largely implemented” to achieve MIL3
- 11 of these are new MIL3 practices
- 11 are MIL2 practices
- 02 are MIL1 practices

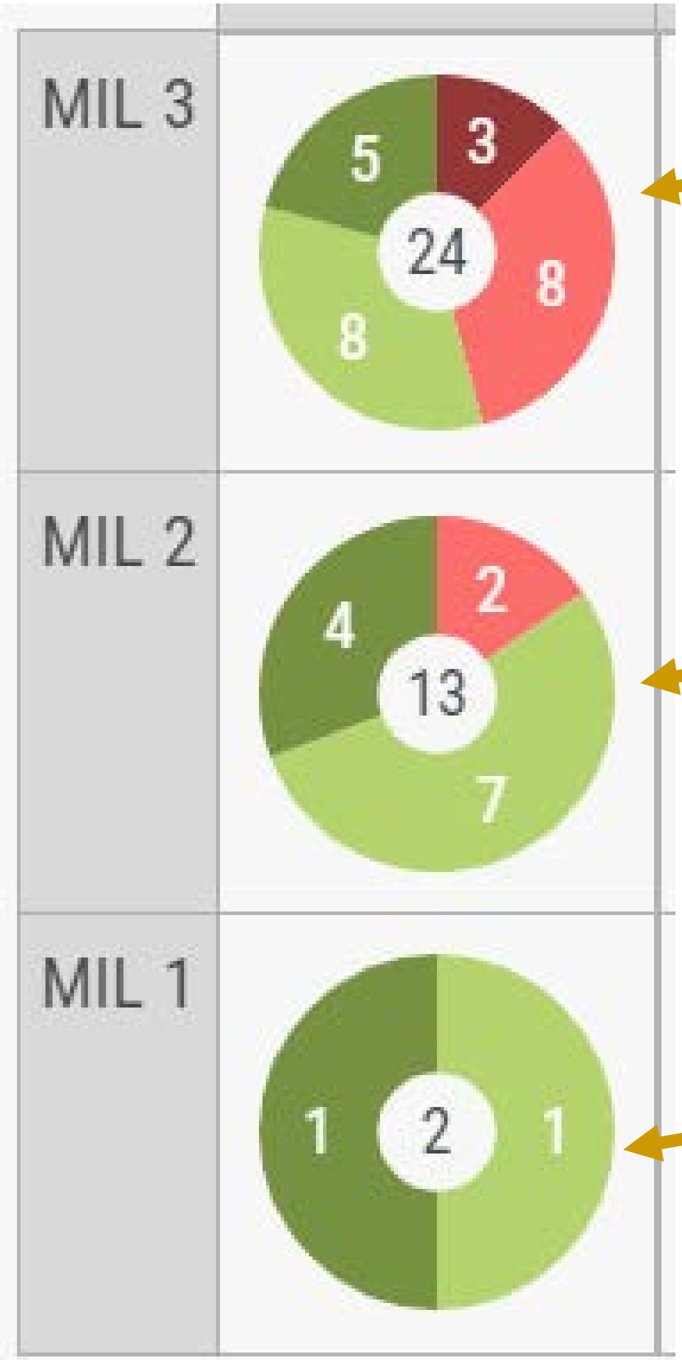
Sample Domain Scoring (cont.)



The status at MIL3:

- 5 practices are “fully implemented”, but only one is a MIL3 practice.
- 8 practices are “largely implemented”, but one is a MIL3 practice.
- There are 8 “partially implemented” practices, including 2 inherited from MIL2.
- There are 3 “not implemented” practices – all MIL3 practices

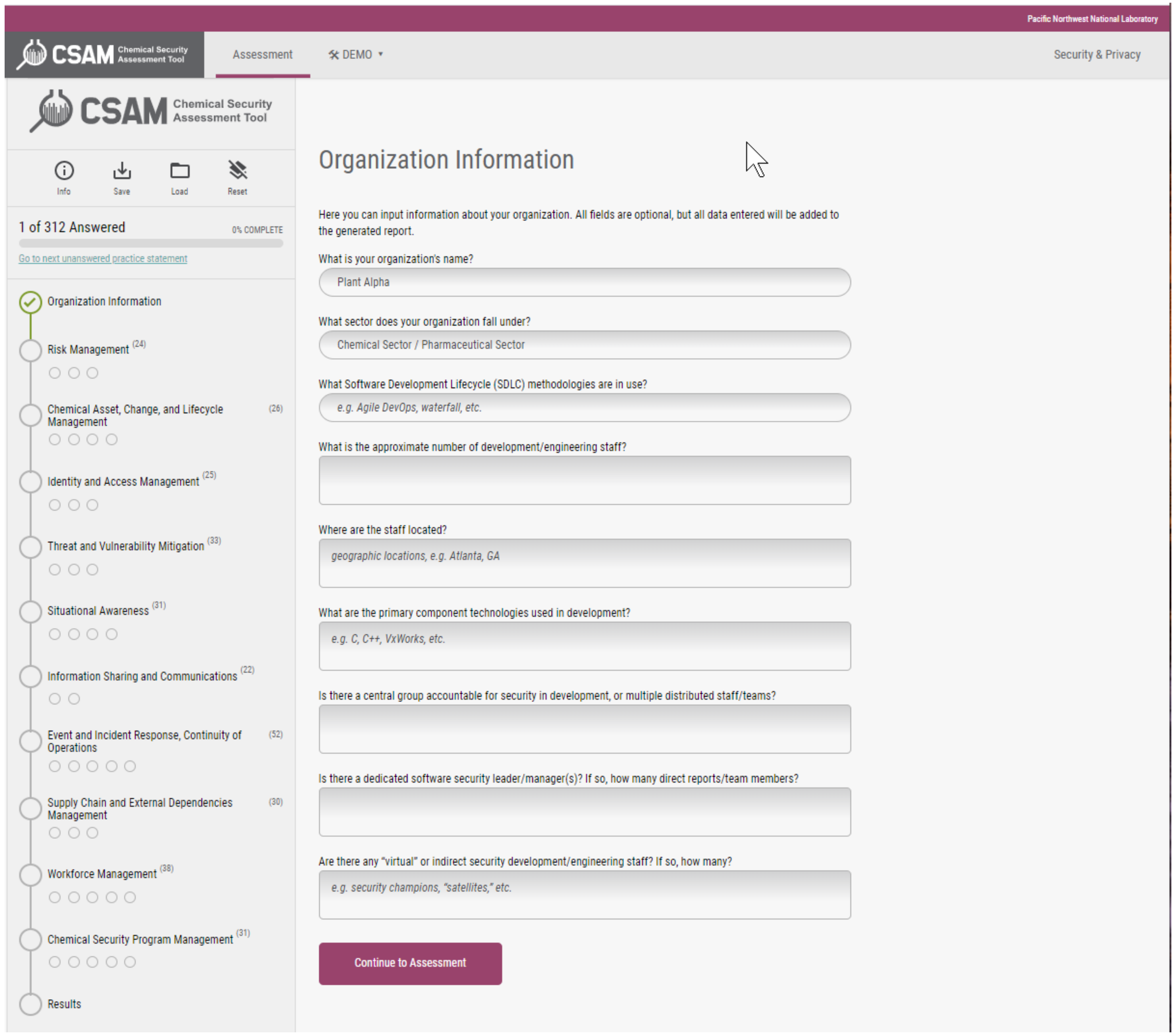
Sample Domain Scoring (cont.)



- There is considerable work to do to reach MIL3 for this domain; 11 practices would have to improve to reach “largely implemented”.
- MIL2 might be a more realistic and affordable goal. Only 2 practices need to improve from “partly” to “largely implemented” to achieve MIL2.
- MIL1 is currently achieved

Chemical Security Assessment Model

- We are implementing user-friendly, on-line versions of an array of maturity model tools.



Pacific Northwest National Laboratory
CSAM Chemical Security Assessment Tool
Assessment
DEMO ▾
Security & Privacy
CSAM Chemical Security Assessment Tool
Info
Save
Load
Reset

1 of 312 Answered 0% COMPLETE

Go to next unanswered practice statement

- Organization Information
- Risk Management (24) ○ ○ ○
- Chemical Asset, Change, and Lifecycle Management (26) ○ ○ ○ ○
- Identity and Access Management (25) ○ ○ ○
- Threat and Vulnerability Mitigation (33) ○ ○ ○
- Situational Awareness (31) ○ ○ ○ ○
- Information Sharing and Communications (22) ○ ○
- Event and Incident Response, Continuity of Operations (52) ○ ○ ○ ○ ○
- Supply Chain and External Dependencies Management (30) ○ ○ ○
- Workforce Management (38) ○ ○ ○ ○ ○
- Chemical Security Program Management (31) ○ ○ ○ ○ ○
- Results

Organization Information

Here you can input information about your organization. All fields are optional, but all data entered will be added to the generated report.

What is your organization's name?

Plant Alpha

What sector does your organization fall under?

Chemical Sector / Pharmaceutical Sector

What Software Development Lifecycle (SDLC) methodologies are in use?

e.g. Agile DevOps, waterfall, etc.

What is the approximate number of development/engineering staff?

Where are the staff located?

geographic locations, e.g. Atlanta, GA

What are the primary component technologies used in development?

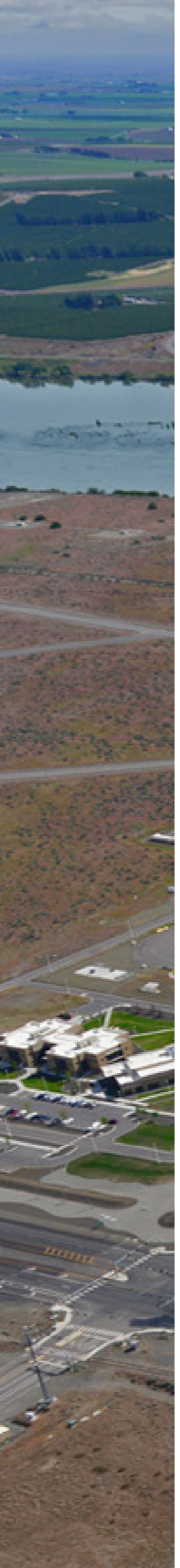
e.g. C, C++, VxWorks, etc.

Is there a central group accountable for security in development, or multiple distributed staff/teams?

Is there a dedicated software security leader/manager(s)? If so, how many direct reports/team members?

Are there any "virtual" or indirect security development/engineering staff? If so, how many?

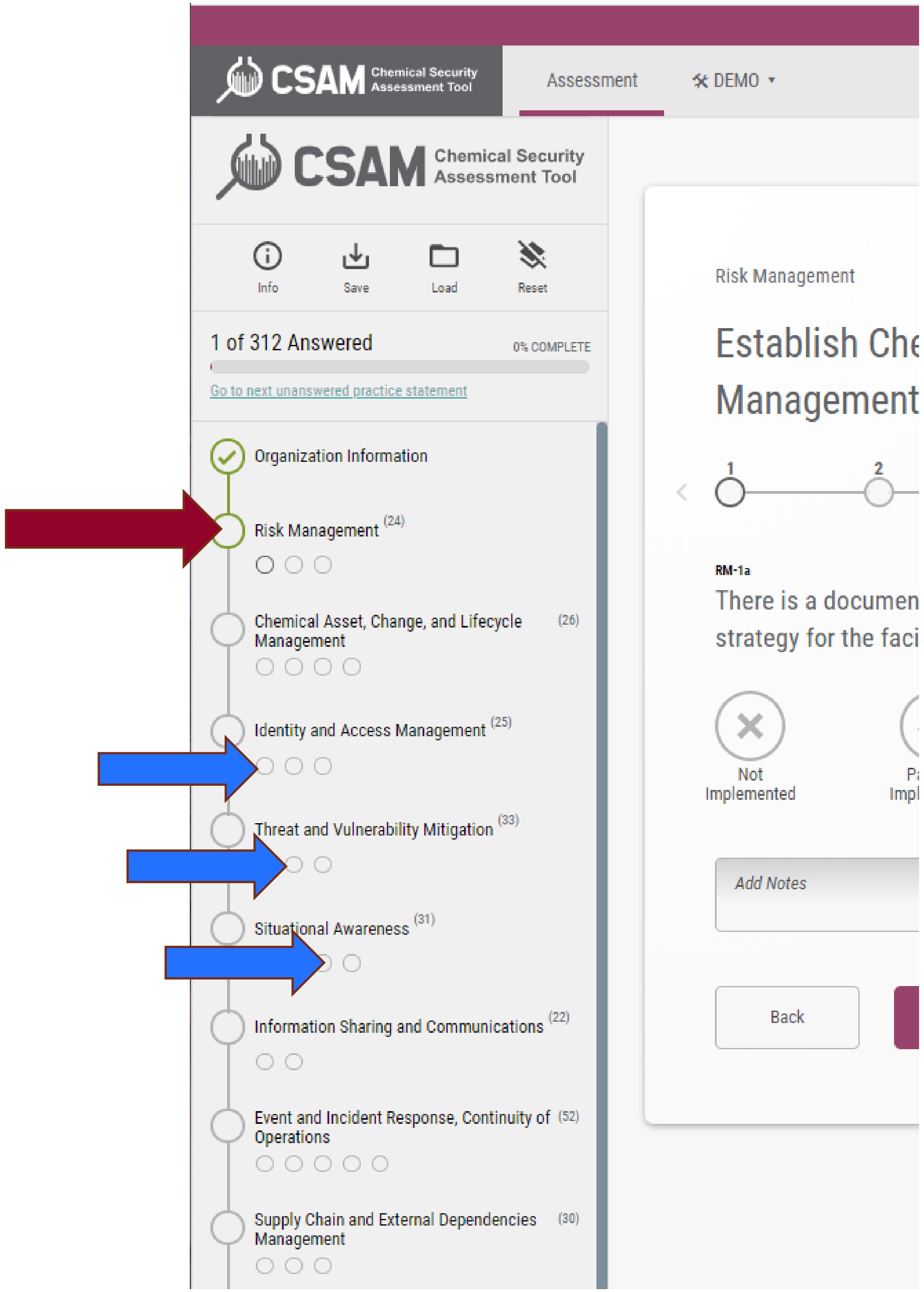
e.g. security champions, "satellites," etc.



Pacific Northwest
NATIONAL LABORATORY

Navigation Menu

Navigate to each domain or objective by clicking the appropriate circle



CSAM Chemical Security Assessment Tool

1 of 312 Answered — 0% COMPLETE

Go to next unanswered practice statement

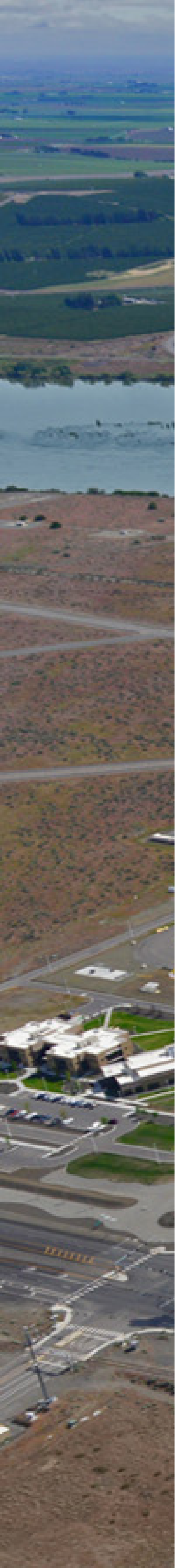
- Organization Information
- Risk Management (24) ○ ○ ○
- Chemical Asset, Change, and Lifecycle Management (26) ○ ○ ○ ○
- Identity and Access Management (25) ○ ○ ○
- Threat and Vulnerability Mitigation (33) ○ ○ ○
- Situational Awareness (31) ○ ○ ○
- Information Sharing and Communications (22) ○ ○
- Event and Incident Response, Continuity of Operations (52) ○ ○ ○ ○ ○
- Supply Chain and External Dependencies Management (30) ○ ○ ○

Risk Management

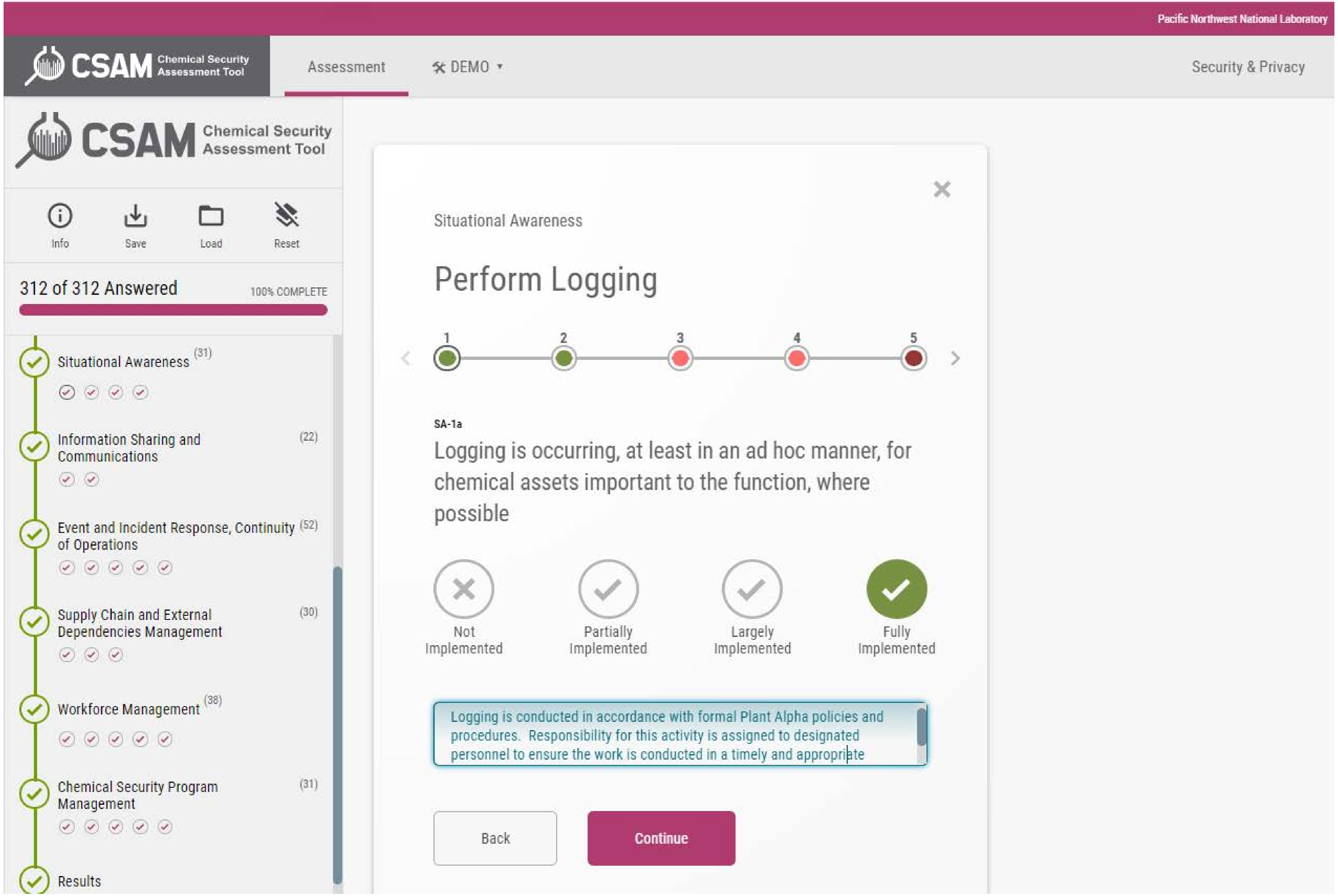
Establish Che
Management

RM-1a

There is a documen
strategy for the faci



Pacific Northwest
NATIONAL LABORATORY


Pacific Northwest National Laboratory
CSAM Chemical Security Assessment Tool
Assessment
DEMO
Security & Privacy
Info
Save
Load
Reset
Situational Awareness (31)
Information Sharing and Communications (22)
Event and Incident Response, Continuity of Operations (52)
Supply Chain and External Dependencies Management (30)
Workforce Management (38)
Chemical Security Program Management (31)
Results
1
2
3
4
5
Not Implemented
Partially Implemented
Largely Implemented
Fully Implemented
Back
Continue

312 of 312 Answered 100% COMPLETE

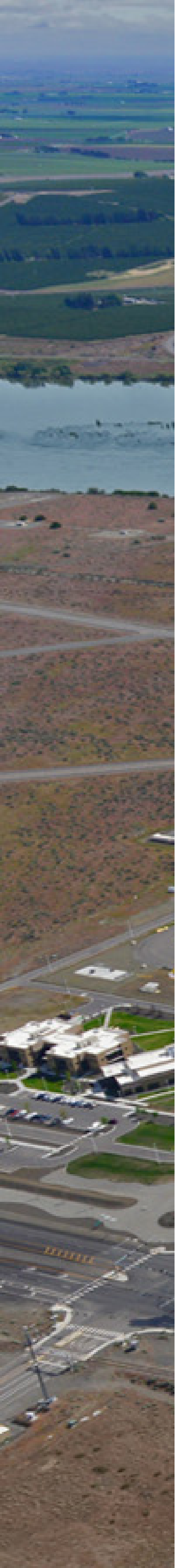
Situational Awareness

Perform Logging

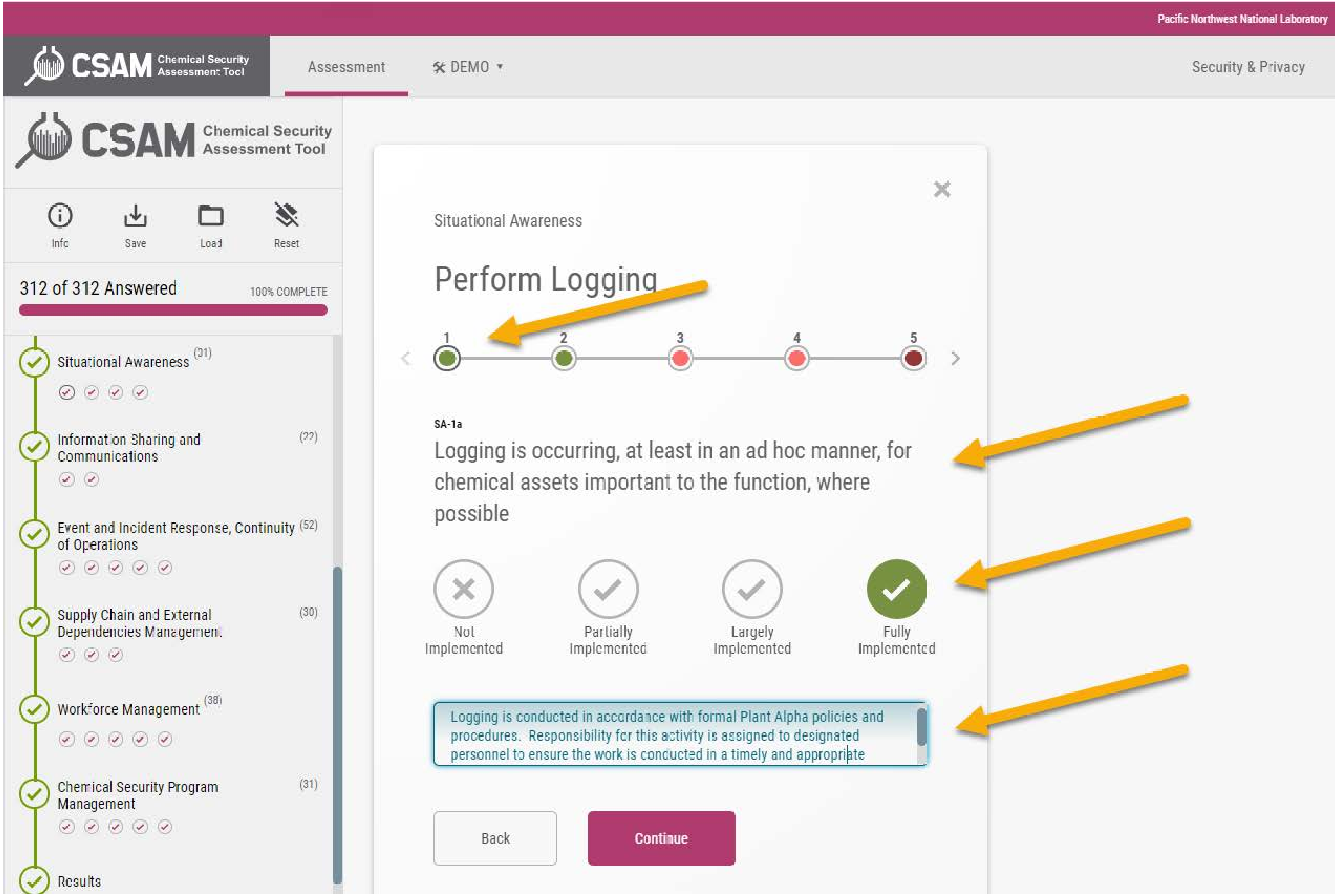
SA-1a

Logging is occurring, at least in an ad hoc manner, for chemical assets important to the function, where possible

Logging is conducted in accordance with formal Plant Alpha policies and procedures. Responsibility for this activity is assigned to designated personnel to ensure the work is conducted in a timely and appropriate



Pacific Northwest
NATIONAL LABORATORY



Pacific Northwest National Laboratory
CSAM Chemical Security Assessment Tool
Assessment
DEMO ▾
Security & Privacy
CSAM Chemical Security Assessment Tool
Info
Save
Load
Reset

312 of 312 Answered 100% COMPLETE

- Situational Awareness (31)
- Information Sharing and Communications (22)
- Event and Incident Response, Continuity of Operations (52)
- Supply Chain and External Dependencies Management (30)
- Workforce Management (38)
- Chemical Security Program Management (31)
- Results

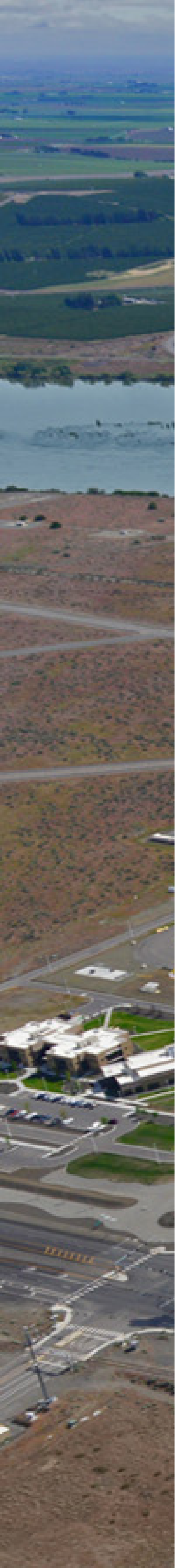
Situational Awareness

Perform Logging

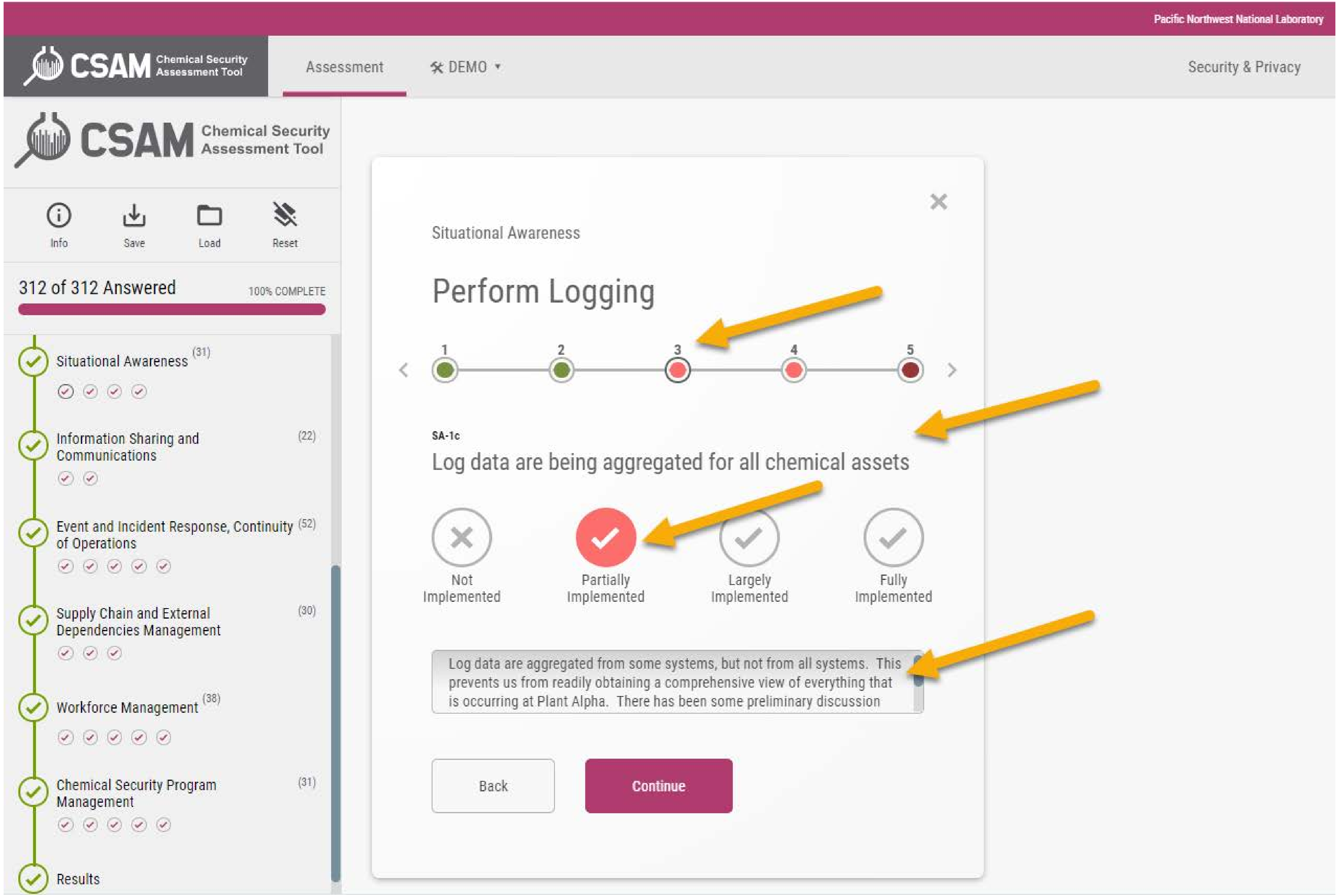
SA-1a

Logging is occurring, at least in an ad hoc manner, for chemical assets important to the function, where possible

Logging is conducted in accordance with formal Plant Alpha policies and procedures. Responsibility for this activity is assigned to designated personnel to ensure the work is conducted in a timely and appropriate



Pacific Northwest
NATIONAL LABORATORY



Pacific Northwest National Laboratory
CSAM Chemical Security Assessment Tool
Assessment
DEMO ▾
Security & Privacy
CSAM Chemical Security Assessment Tool
Info
Save
Load
Reset

312 of 312 Answered 100% COMPLETE

- ✓ Situational Awareness (31)
- ✓ Information Sharing and Communications (22)
- ✓ Event and Incident Response, Continuity of Operations (52)
- ✓ Supply Chain and External Dependencies Management (30)
- ✓ Workforce Management (38)
- ✓ Chemical Security Program Management (31)
- ✓ Results

Situational Awareness

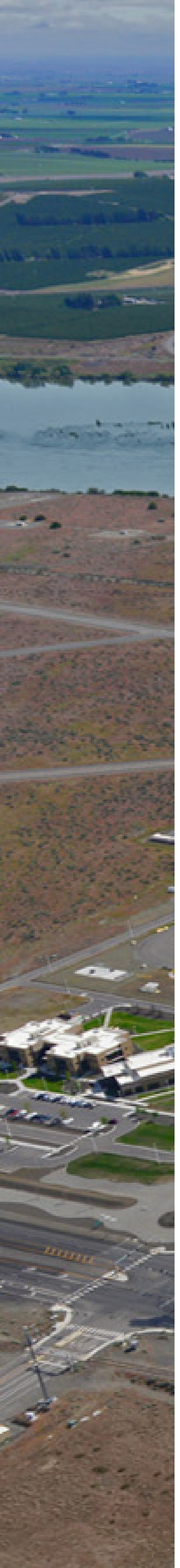
Perform Logging

SA-1c

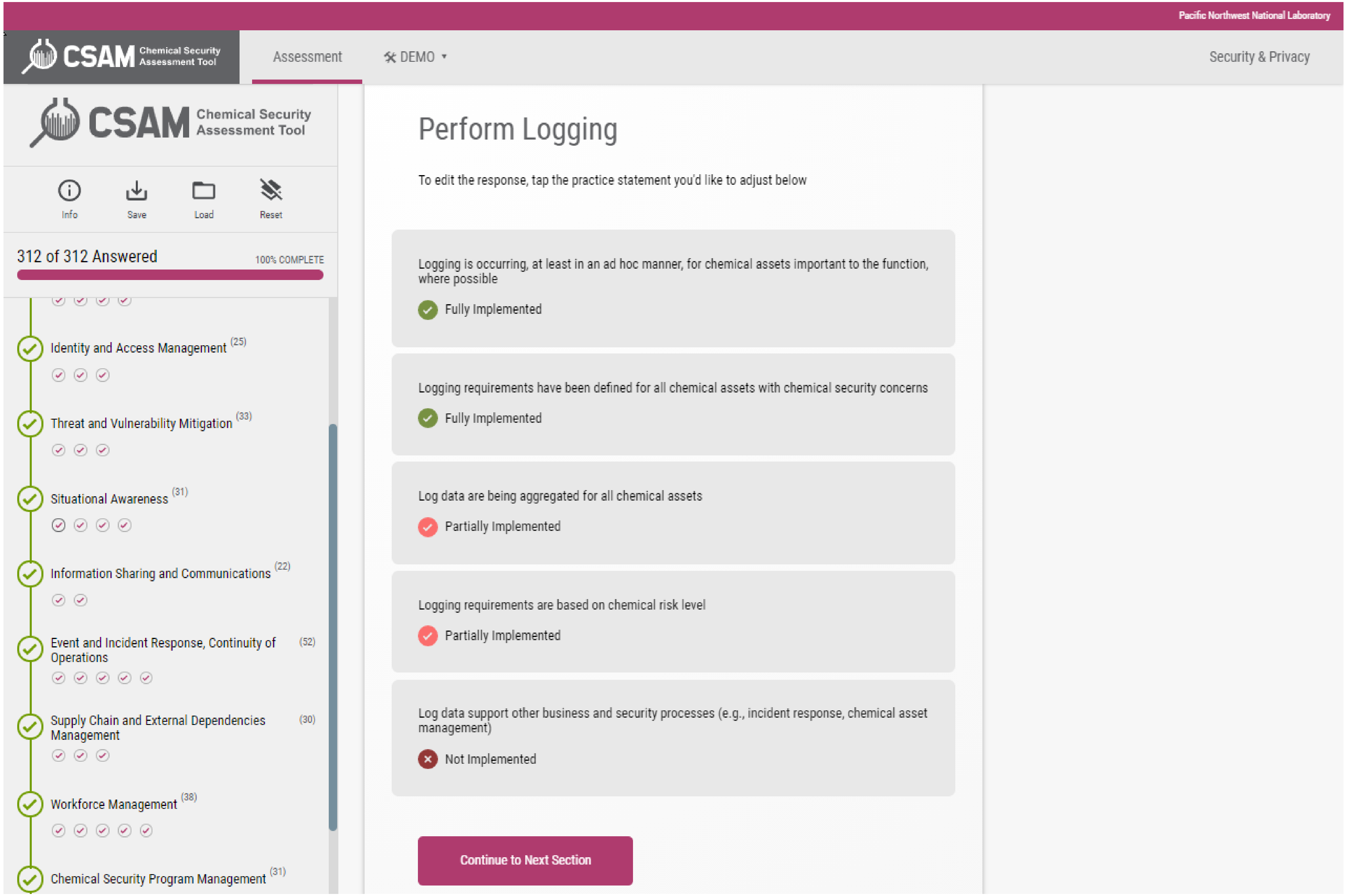
Log data are being aggregated for all chemical assets

☒ Not Implemented
[✓ Partially Implemented]
○ Largely Implemented
○ Fully Implemented

Log data are aggregated from some systems, but not from all systems. This prevents us from readily obtaining a comprehensive view of everything that is occurring at Plant Alpha. There has been some preliminary discussion



Pacific Northwest
NATIONAL LABORATORY



Pacific Northwest National Laboratory
CSAM Chemical Security Assessment Tool
Assessment
DEMO ▾
Security & Privacy
CSAM Chemical Security Assessment Tool
Info
Save
Load
Reset

312 of 312 Answered 100% COMPLETE

- Identity and Access Management (25)
- Threat and Vulnerability Mitigation (33)
- Situational Awareness (31)
- Information Sharing and Communications (22)
- Event and Incident Response, Continuity of Operations (52)
- Supply Chain and External Dependencies Management (30)
- Workforce Management (38)
- Chemical Security Program Management (31)

Perform Logging

To edit the response, tap the practice statement you'd like to adjust below

Logging is occurring, at least in an ad hoc manner, for chemical assets important to the function, where possible

✓ Fully Implemented

Logging requirements have been defined for all chemical assets with chemical security concerns

✓ Fully Implemented

Log data are being aggregated for all chemical assets

✓ Partially Implemented

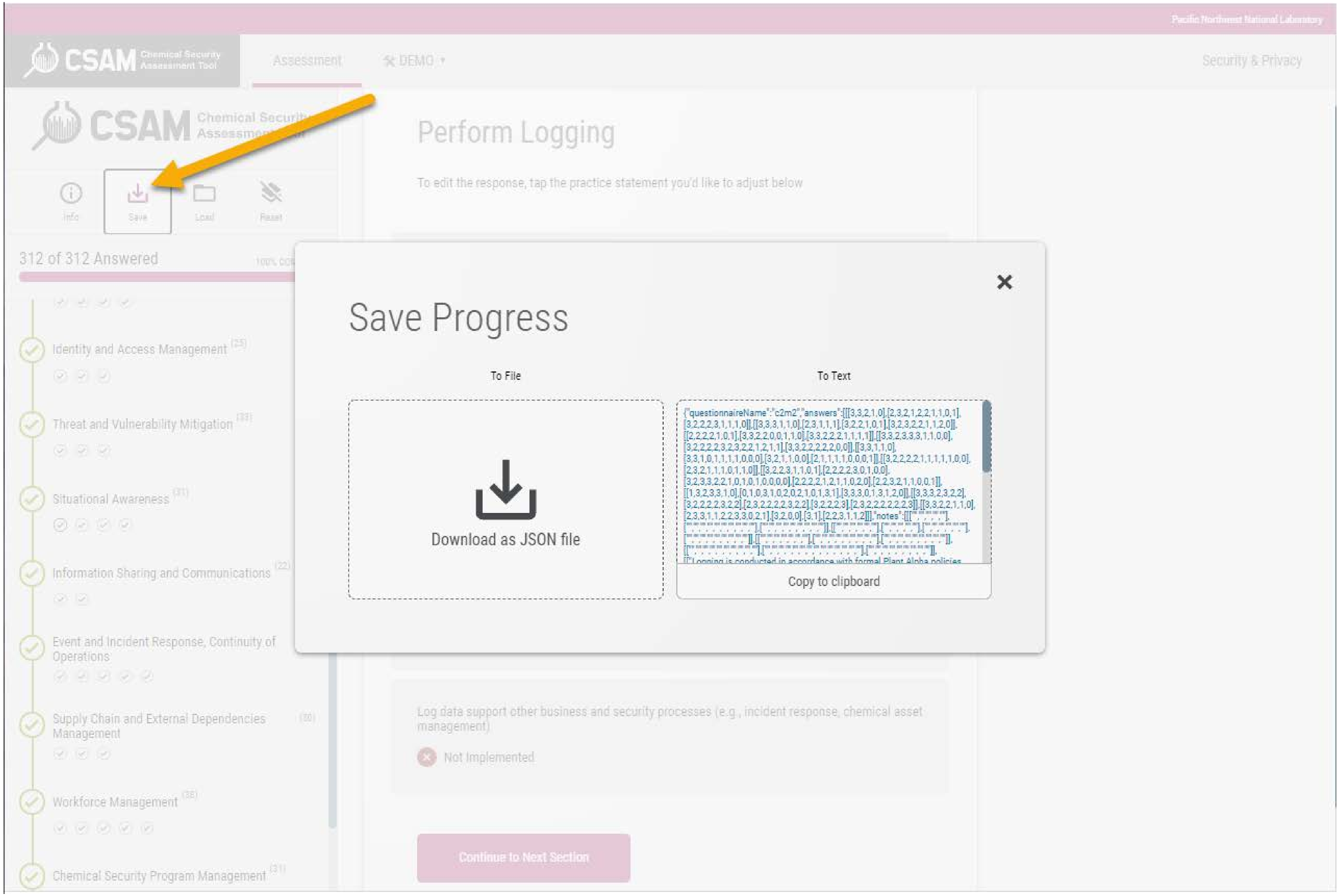
Logging requirements are based on chemical risk level

✓ Partially Implemented

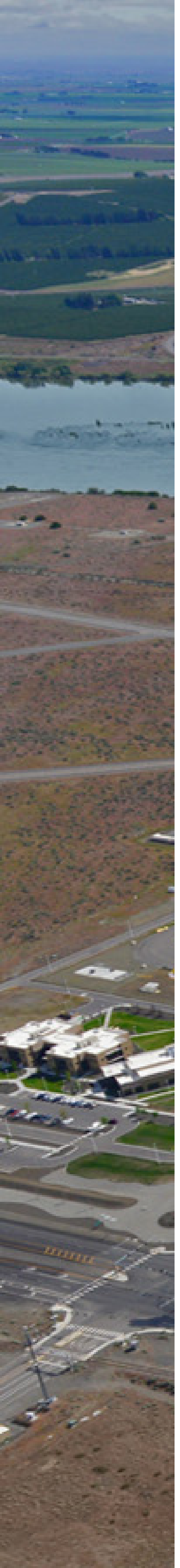
Log data support other business and security processes (e.g., incident response, chemical asset management)

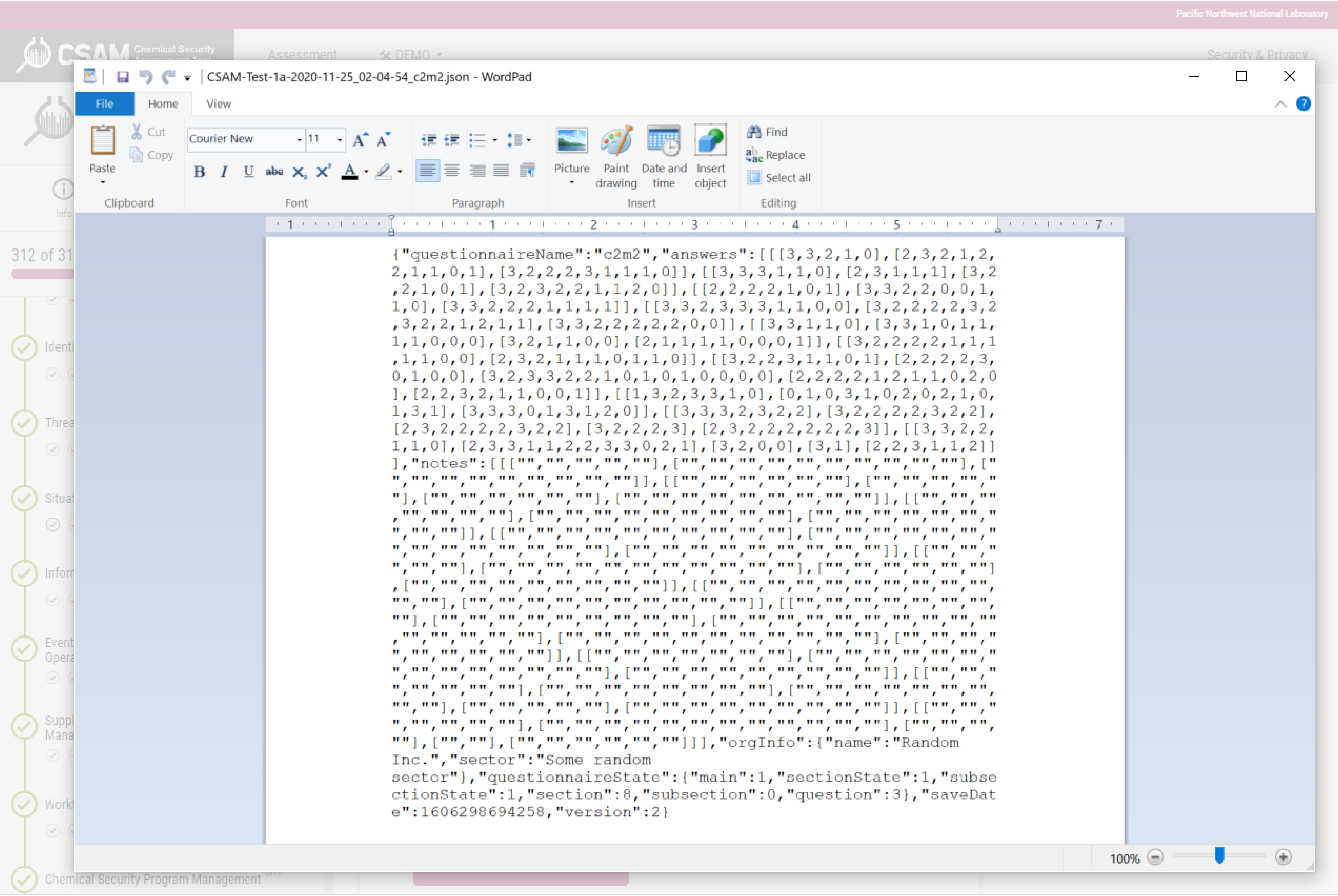
✕ Not Implemented

Continue to Next Section

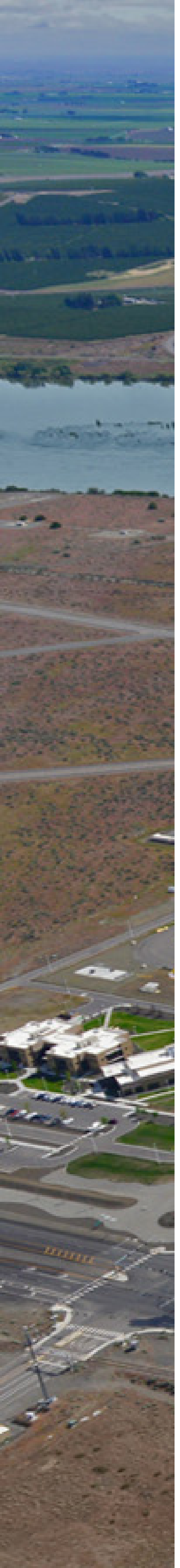

Pacific Northwest National Laboratory
CSAM Chemical Security Assessment Tool
Assessment
DEMO
Security & Privacy
CSAM Chemical Security Assessment Tool
Info
Save
Load
Reset
312 of 312 Answered
100% complete
Identity and Access Management (25)
Threat and Vulnerability Mitigation (33)
Situational Awareness (31)
Information Sharing and Communications (22)
Event and Incident Response, Continuity of Operations
Supply Chain and External Dependencies Management (30)
Workforce Management (38)
Chemical Security Program Management (31)
Perform Logging
To edit the response, tap the practice statement you'd like to adjust below
Log data support other business and security processes (e.g., incident response, chemical asset management)
Not Implemented
Continue to Next Section
×
Save Progress
To File
To Text
Download as JSON file
Copy to clipboard

```
{"questionnaireName":"c2m2","answers":[[[3,3,2,1,0],[2,3,2,1,2,2,1,1,0,1],
[3,2,2,2,3,1,1,1,0]],[[3,3,3,1,1,0],[2,3,1,1,1],[3,2,2,1,0,1],[3,2,3,2,2,1,1,2,0]],
[[2,2,2,2,1,0,1],[3,3,2,2,0,0,1,1,0]],[3,3,2,2,2,1,1,1,1]],[[3,3,2,3,3,3,1,1,0,0],
[3,2,2,2,2,3,2,3,2,2,1,2,1,1],[3,3,2,2,2,2,2,0,0]],[[3,3,1,1,0],
[3,3,1,0,1,1,1,1,0,0,0],[3,2,1,1,0,0],[2,1,1,1,1,0,0,0,1]],[[3,2,2,2,2,1,1,1,1,1,0,0],
[2,3,2,1,1,1,0,1,1,0]],[[3,2,2,3,1,1,0,1],[2,2,2,2,3,0,1,0,0],
[3,2,3,3,2,2,1,0,1,0,1,0,0,0,0],[2,2,2,2,1,2,1,1,0,2,0],[2,2,3,2,1,1,0,0,1]],
[[1,3,2,3,3,1,0],[0,1,0,3,1,0,2,0,2,1,0,1,3,1],[3,3,3,0,1,3,1,2,0]],[[3,3,3,2,3,2,2],
[3,2,2,2,2,3,2,2],[2,3,2,2,2,2,3,2,2],[3,2,2,2,3],[2,3,2,2,2,2,2,2,3]],[[3,3,2,2,1,1,0],
[2,3,3,1,1,2,2,3,3,0,2,1],[3,2,0,0],[3,1],[2,2,3,1,1,2]]],"notes":[[["","","","",""],
[illegible]
["Logging is conducted in accordance with formal Plant Alpha policies
```

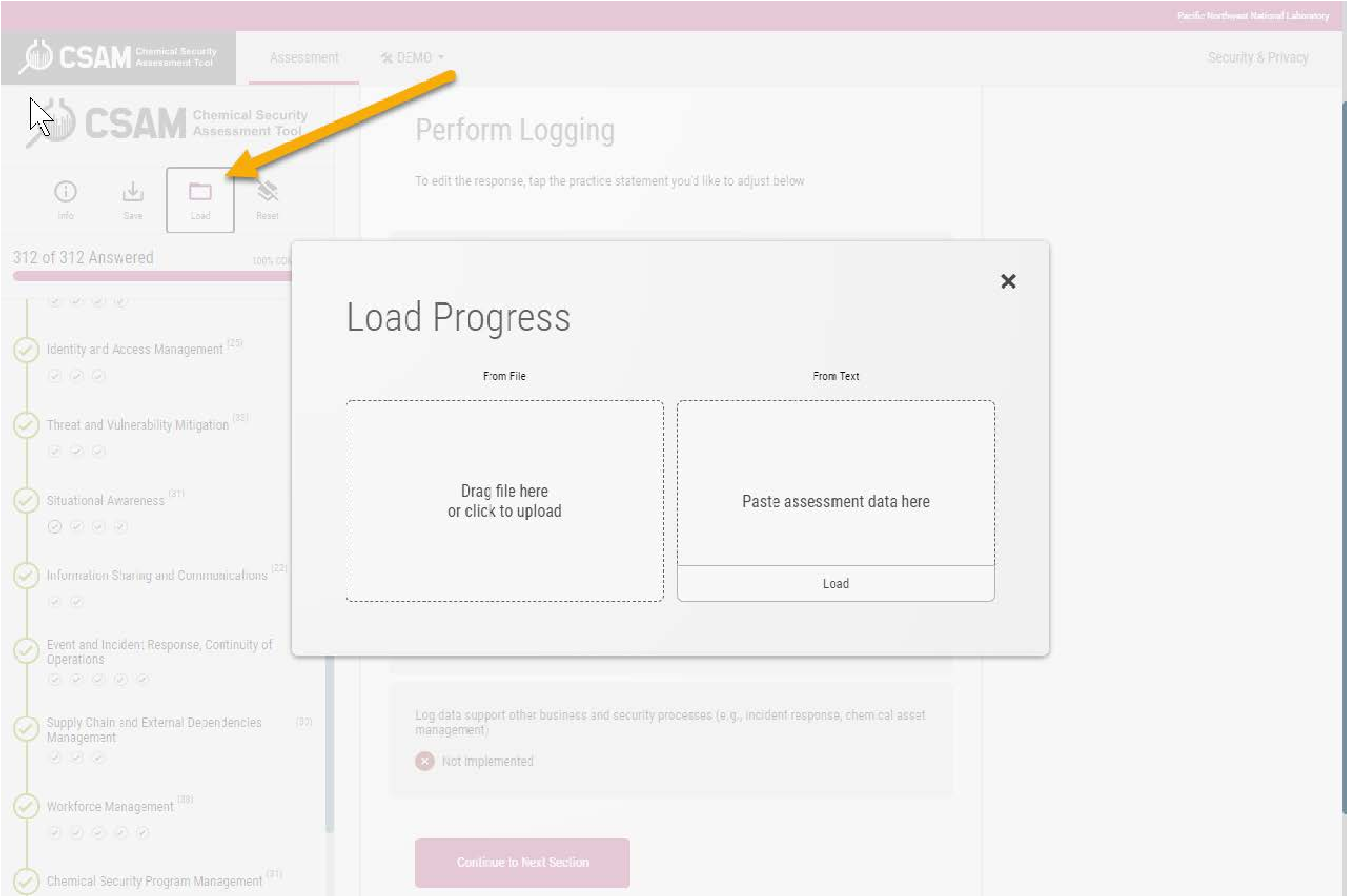




```
{"questionnaireName":"c2m2","answers":[[[3,3,2,1,0],[2,3,2,1,2,
2,1,1,0,1],[3,2,2,2,3,1,1,1,0]],[[3,3,3,1,1,0],[2,3,1,1,1],[3,2
,2,1,0,1],[3,2,3,2,2,1,1,2,0]],[[2,2,2,2,1,0,1],[3,3,2,2,0,0,1,
1,0],[3,3,2,2,2,1,1,1,1]],[[3,3,2,3,3,3,1,1,0,0],[3,2,2,2,2,3,2
,3,2,2,1,2,1,1],[3,3,2,2,2,2,2,0,0]],[[3,3,1,1,0],[3,3,1,0,1,1,
1,1,0,0,0],[3,2,1,1,0,0],[2,1,1,1,1,0,0,0,1]],[[3,2,2,2,2,1,1,1
,1,1,0,0],[2,3,2,1,1,1,0,1,1,0]],[[3,2,2,3,1,1,0,1],[2,2,2,2,3,
0,1,0,0],[3,2,3,3,2,2,1,0,1,0,1,0,0,0,0],[2,2,2,2,1,2,1,1,0,2,0
],[2,2,3,2,1,1,0,0,1]],[[1,3,2,3,3,1,0],[0,1,0,3,1,0,2,0,2,1,0,
1,3,1],[3,3,3,0,1,3,1,2,0]],[[3,3,3,2,3,2,2],[3,2,2,2,2,3,2,2],
[2,3,2,2,2,2,3,2,2],[3,2,2,2,3],[2,3,2,2,2,2,2,2,3]],[[3,3,2,2,
1,1,0],[2,3,3,1,1,2,2,3,3,0,2,1],[3,2,0,0],[3,1],[2,2,3,1,1,2]]
],"notes":[[["","","","",""],["","","","","","","","","",""],["
","","","","","","","",""]],[["","","","","",""],["","","","","
"],["","","","","",""],["","","","","","","","",""]],[["","",""
,"","","",""],["","","","","","","","",""],["","","","","","","
","",""]],[["","","","","","","","","",""],["","","","","","","
","","","","","","",""],["","","","","","","","",""]],[["","","
","",""],["","","","","","","","","","",""],["","","","","",""]
,["","","","","","","","",""]],[["","","","","","","","","","",
"",""],["","","","","","","","","",""]],[["","","","","","","",
""],["","","","","","","","",""],["","","","","","","","","",""
,"","","","",""],["","","","","","","","","","",""],["","","","
","","","","",""]],[["","","","","","",""],["","","","","","","
","","","","","","",""],["","","","","","","","",""]],[["","","
","","","",""],["","","","","","","",""],["","","","","","","",
"",""],["","","","",""],["","","","","","","","",""]],[["","","
","","","",""],["","","","","","","","","","","",""],["","","",
""],["",""],["","","","","",""]]],"orgInfo":{"name":"Random
Inc.","sector":"Some random
sector"},"questionnaireState":{"main":1,"sectionState":1,"subse
ctionState":1,"section":8,"subsection":0,"question":3},"saveDat
e":1606298694258,"version":2}
```



Pacific Northwest
NATIONAL LABORATORY



Pacific Northwest National Laboratory
CSAM Chemical Security Assessment Tool
Assessment
DEMO
Security & Privacy
CSAM Chemical Security Assessment Tool
Info
Save
Load
Reset

312 of 312 Answered

100% CO

Identity and Access Management (25)

Threat and Vulnerability Mitigation (33)

Situational Awareness (31)

Information Sharing and Communications (22)

Event and Incident Response, Continuity of Operations

Supply Chain and External Dependencies Management (30)

Workforce Management (38)

Chemical Security Program Management (31)

Perform Logging

To edit the response, tap the practice statement you'd like to adjust below

Load Progress

From File

Drag file here
or click to upload

From Text

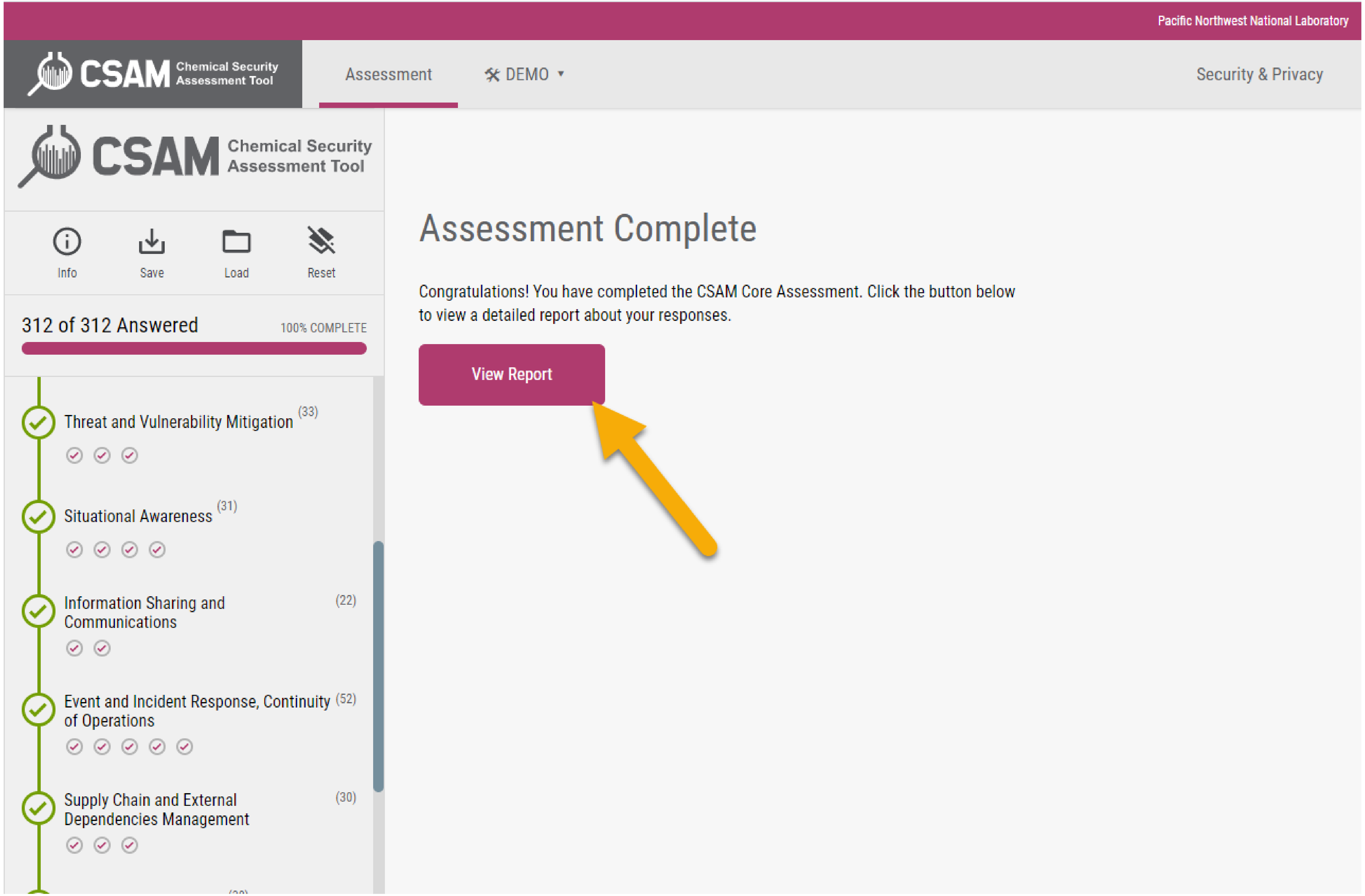
Paste assessment data here

Load

Log data support other business and security processes (e.g., incident response, chemical asset management)

Not Implemented

Continue to Next Section

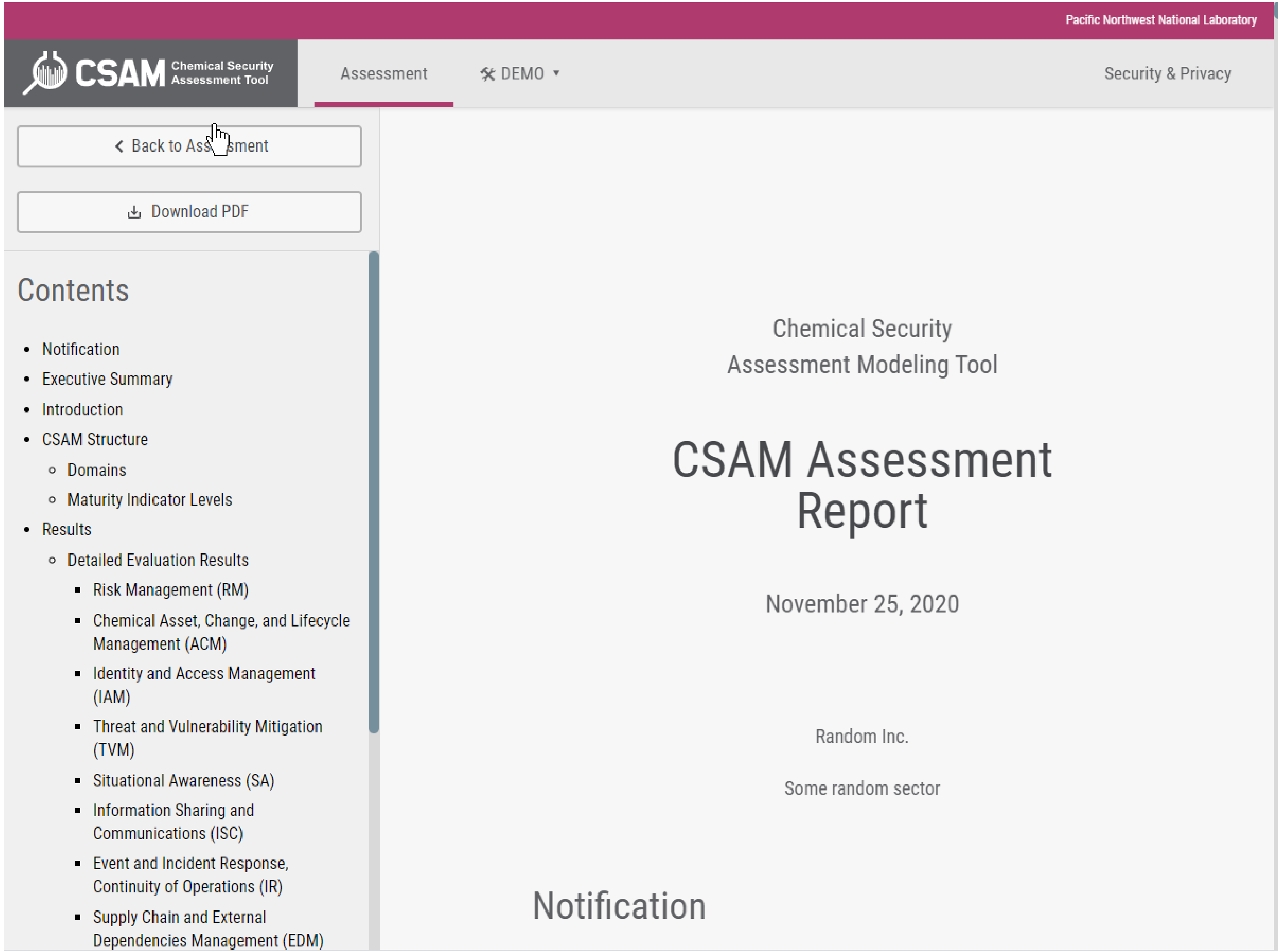

Pacific Northwest National Laboratory
CSAM Chemical Security Assessment Tool
Assessment
DEMO ▾
Security & Privacy
CSAM Chemical Security Assessment Tool
Info
Save
Load
Reset

312 of 312 Answered 100% COMPLETE

- ✓ Threat and Vulnerability Mitigation (33)
- ✓ Situational Awareness (31)
- ✓ Information Sharing and Communications (22)
- ✓ Event and Incident Response, Continuity of Operations (52)
- ✓ Supply Chain and External Dependencies Management (30)

Assessment Complete

Congratulations! You have completed the CSAM Core Assessment. Click the button below to view a detailed report about your responses.



Pacific Northwest National Laboratory
CSAM Chemical Security Assessment Tool
Assessment
DEMO ▾
Security & Privacy
‹ Back to Assessment
Download PDF

Contents

- Notification
- Executive Summary
- Introduction
- CSAM Structure
  - Domains
  - Maturity Indicator Levels
- Results
  - Detailed Evaluation Results
    - Risk Management (RM)
    - Chemical Asset, Change, and Lifecycle Management (ACM)
    - Identity and Access Management (IAM)
    - Threat and Vulnerability Mitigation (TVM)
    - Situational Awareness (SA)
    - Information Sharing and Communications (ISC)
    - Event and Incident Response, Continuity of Operations (IR)
    - Supply Chain and External Dependencies Management (EDM)

Chemical Security
Assessment Modeling Tool

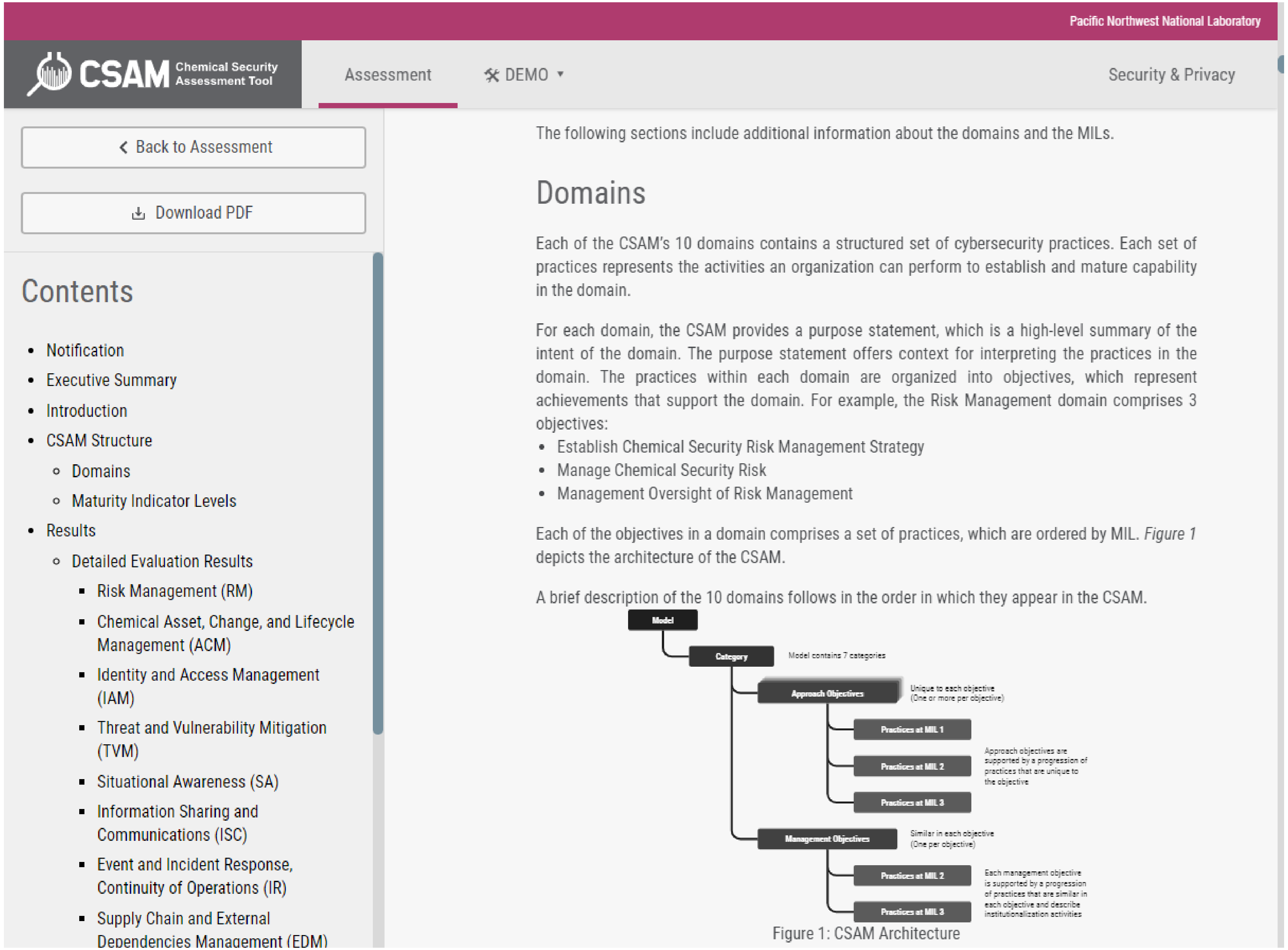
CSAM Assessment Report

November 25, 2020

Random Inc.

Some random sector

Notification


Pacific Northwest National Laboratory
CSAM Chemical Security Assessment Tool
Assessment
DEMO ▾
Security & Privacy
Back to Assessment
Download PDF

Contents

The following sections include additional information about the domains and the MILs.

Domains

Each of the CSAM's 10 domains contains a structured set of cybersecurity practices. Each set of practices represents the activities an organization can perform to establish and mature capability in the domain.

For each domain, the CSAM provides a purpose statement, which is a high-level summary of the intent of the domain. The purpose statement offers context for interpreting the practices in the domain. The practices within each domain are organized into objectives, which represent achievements that support the domain. For example, the Risk Management domain comprises 3 objectives:

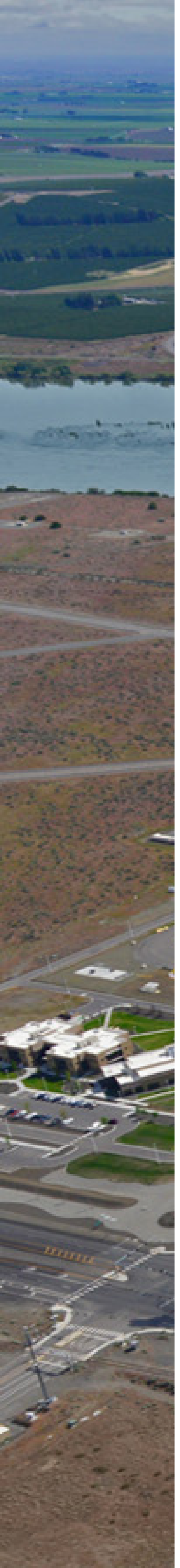
- Establish Chemical Security Risk Management Strategy
- Manage Chemical Security Risk
- Management Oversight of Risk Management

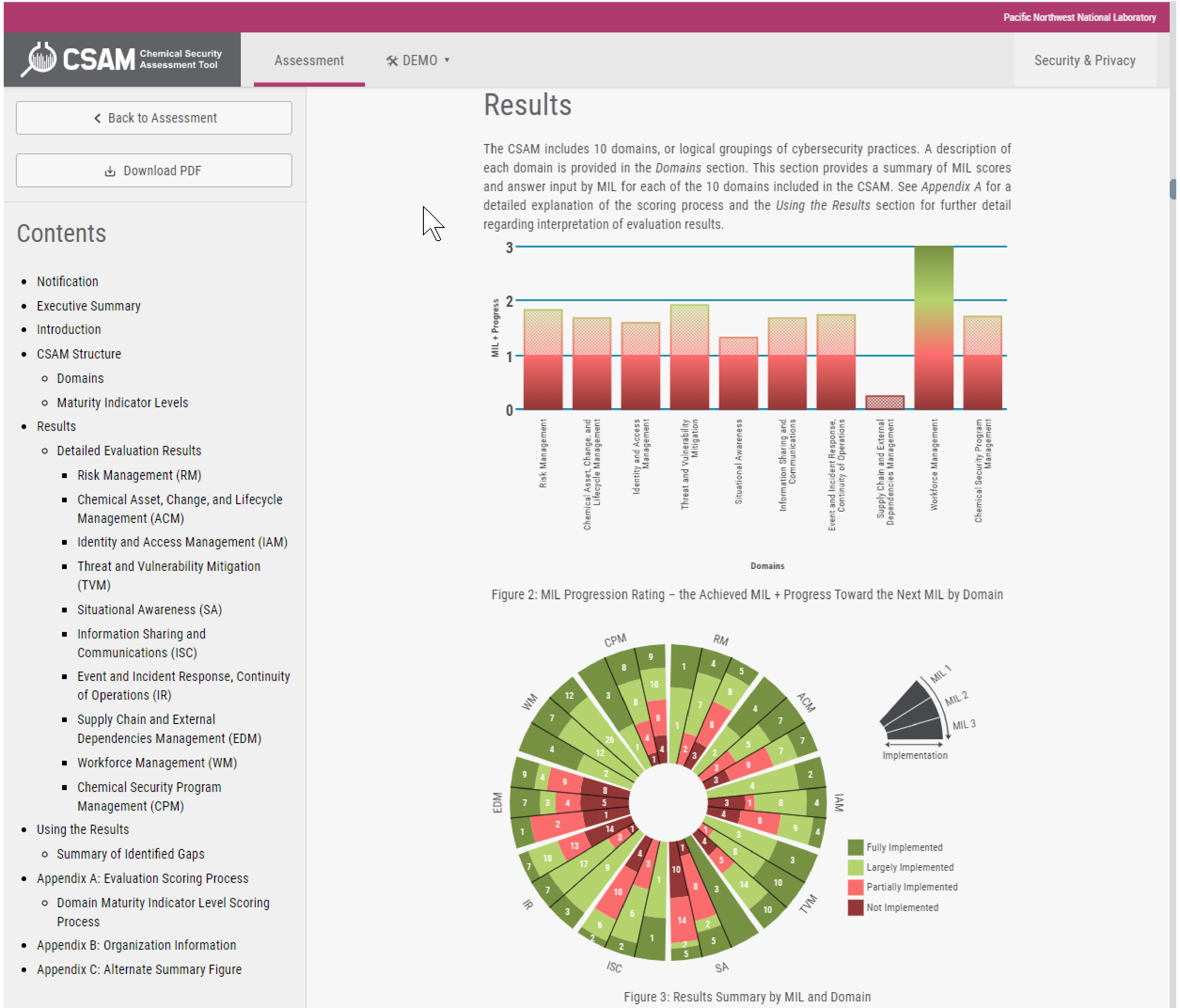
Each of the objectives in a domain comprises a set of practices, which are ordered by MIL. *Figure 1* depicts the architecture of the CSAM.

A brief description of the 10 domains follows in the order in which they appear in the CSAM.

Model
Category
Model contains 7 categories
Approach Objectives
Unique to each objective (One or more per objective)
Practices at MIL 1
Practices at MIL 2
Practices at MIL 3
Approach objectives are supported by a progression of practices that are unique to the objective
Management Objectives
Similar in each objective (One per objective)
Practices at MIL 2
Practices at MIL 3
Each management objective is supported by a progression of practices that are similar in each objective and describe institutionalization activities

Figure 1: CSAM Architecture





Pacific Northwest National Laboratory
CSAM Chemical Security Assessment Tool
Assessment
DEMO ▾
Security & Privacy
< Back to Assessment
Download PDF

Contents

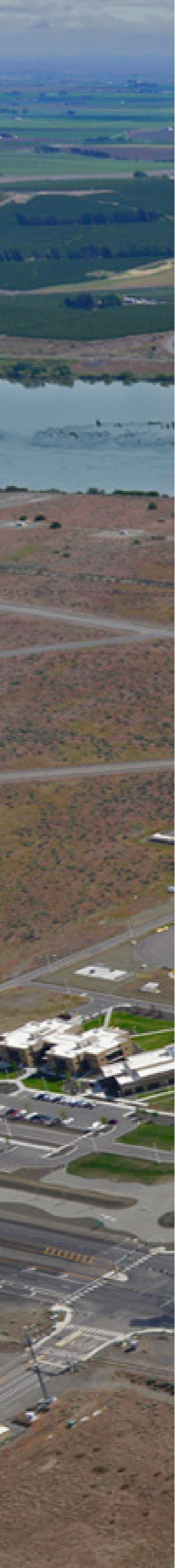
Results

The CSAM includes 10 domains, or logical groupings of cybersecurity practices. A description of each domain is provided in the *Domains* section. This section provides a summary of MIL scores and answer input by MIL for each of the 10 domains included in the CSAM. See *Appendix A* for a detailed explanation of the scoring process and the *Using the Results* section for further detail regarding interpretation of evaluation results.

MIL + Progress
3
2
1
0
Risk Management
Chemical Asset, Change, and Lifecycle Management
Identity and Access Management
Threat and Vulnerability Mitigation
Situational Awareness
Information Sharing and Communications
Event and Incident Response, Continuity of Operations
Supply Chain and External Dependencies Management
Workforce Management
Chemical Security Program Management
Domains

Figure 2: MIL Progression Rating – the Achieved MIL + Progress Toward the Next MIL by Domain

Figure 3: Results Summary by MIL and Domain



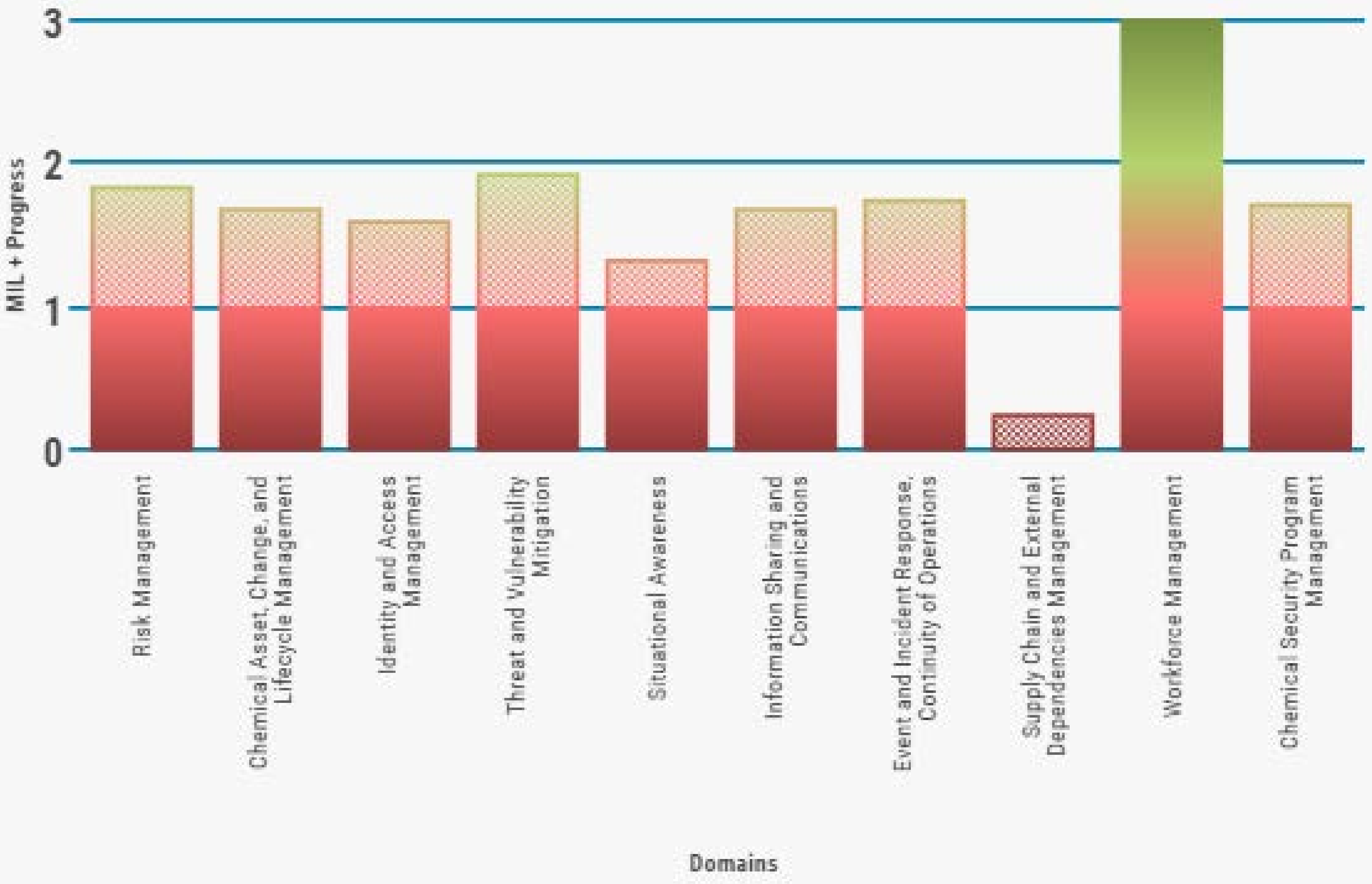
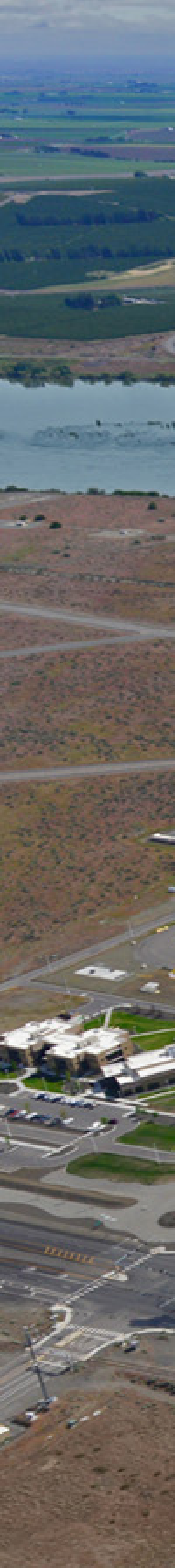

3
2
1
0
MIL + Progress
Risk Management
Chemical Asset, Change, and Lifecycle Management
Identity and Access Management
Threat and Vulnerability Mitigation
Situational Awareness
Information Sharing and Communications
Event and Incident Response, Continuity of Operations
Supply Chain and External Dependencies Management
Workforce Management
Chemical Security Program Management
Domains

Figure 2: MIL Progression Rating – the Achieved MIL + Progress Toward the Next MIL by Domain



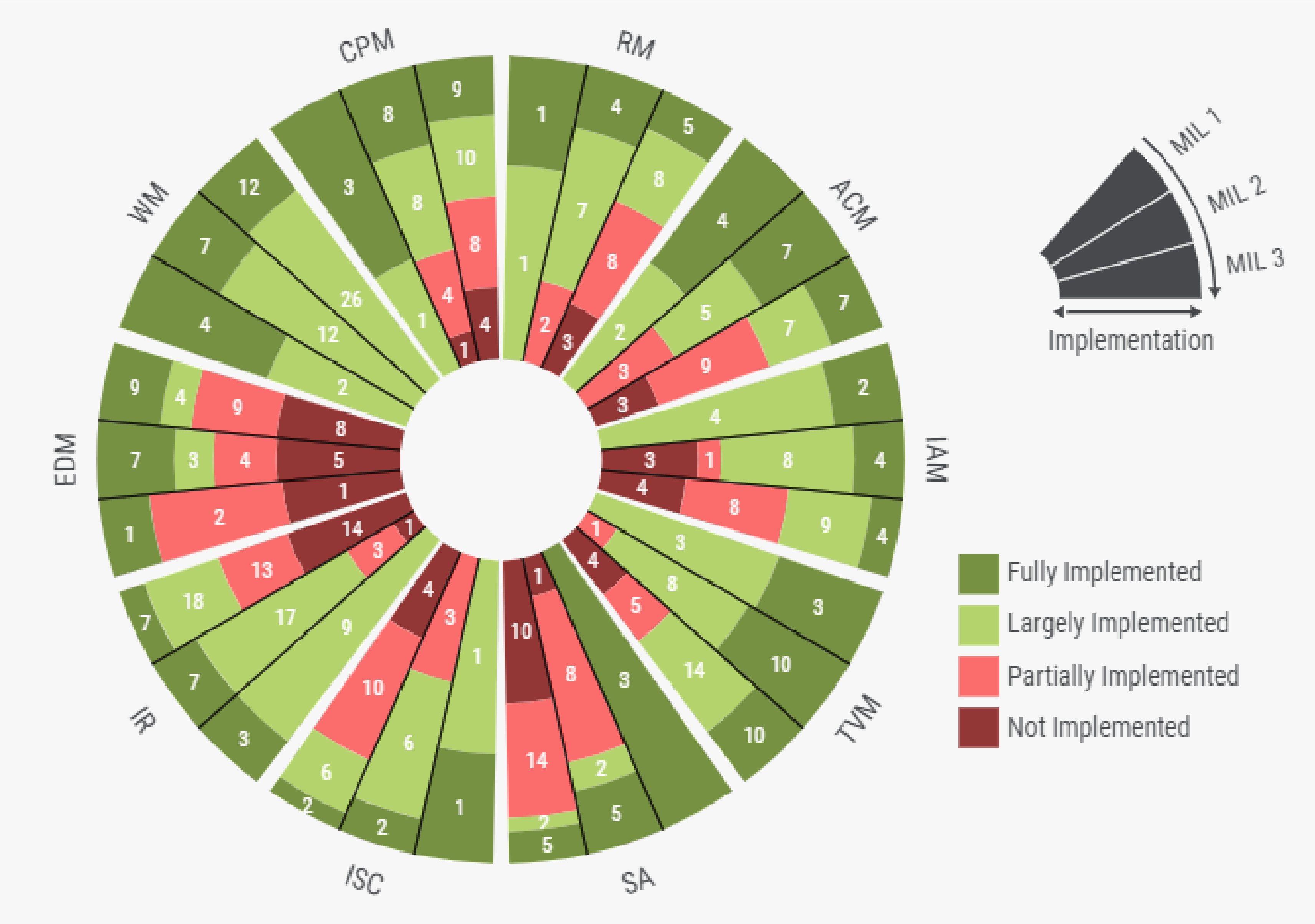
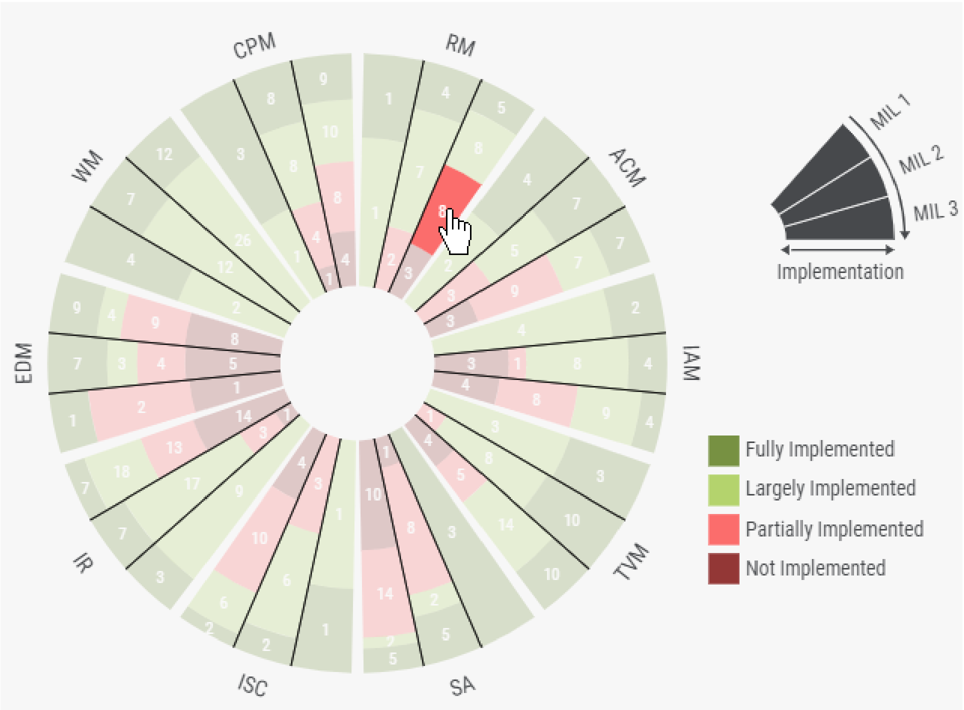
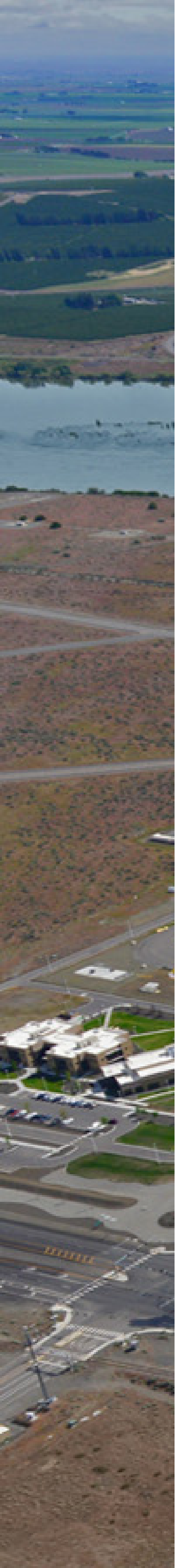
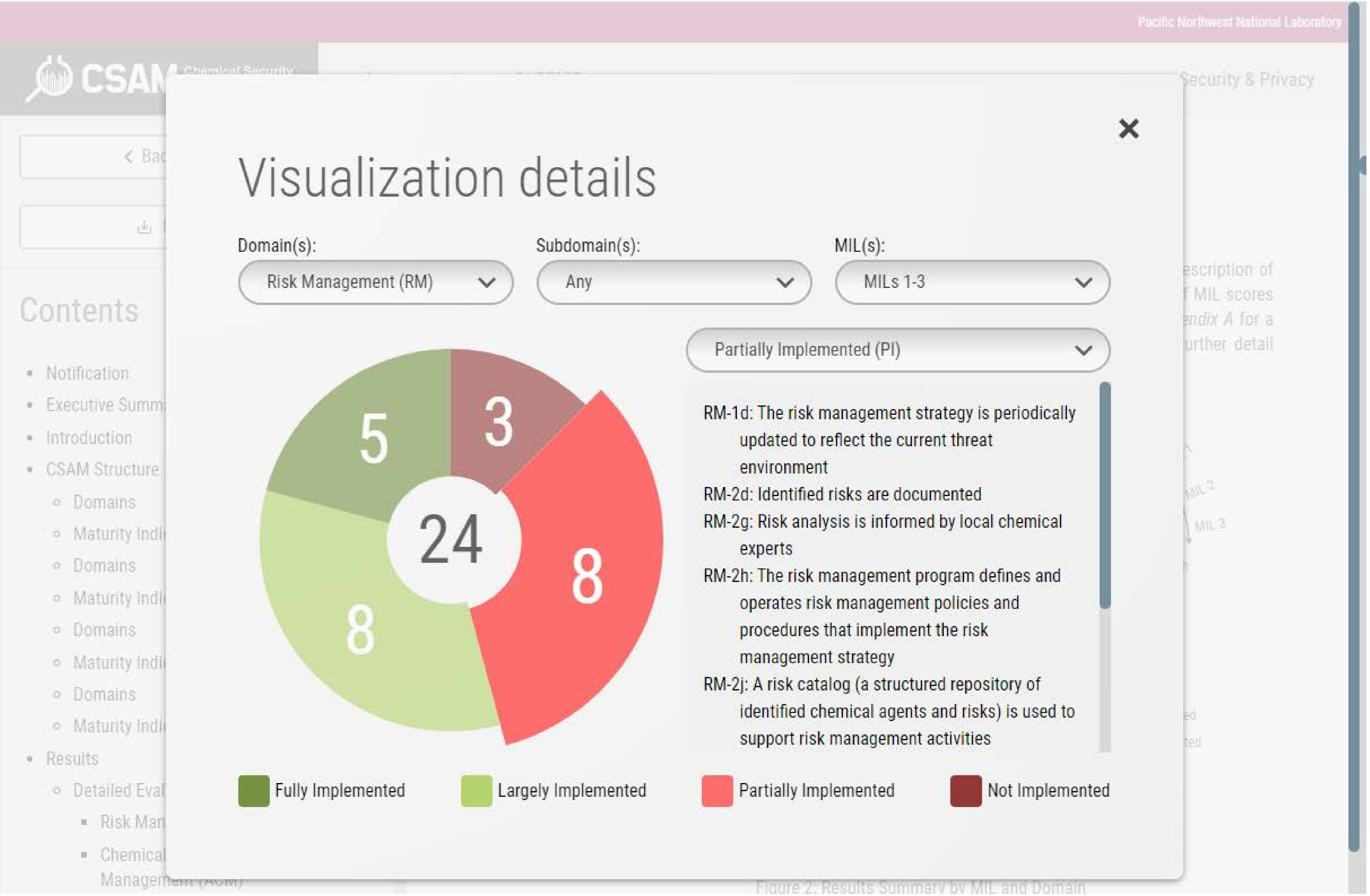


Figure 3: Results Summary by MIL and Domain







Visualization details

Domain(s): Risk Management (RM)

Subdomain(s): Any

MIL(s): MILs 1-3

Partially Implemented (PI)

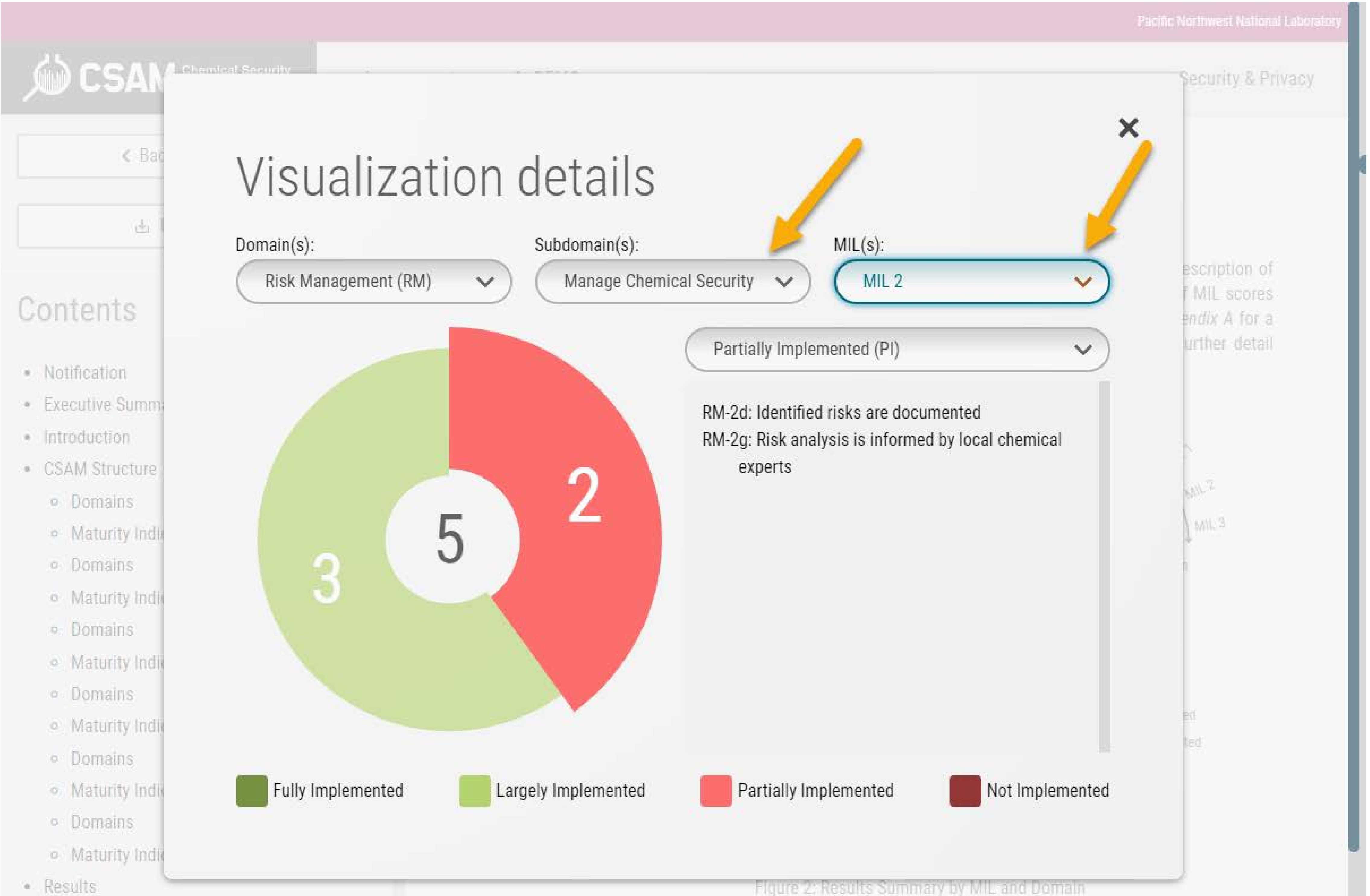
RM-1d: The risk management strategy is periodically updated to reflect the current threat environment

RM-2d: Identified risks are documented

RM-2g: Risk analysis is informed by local chemical experts

RM-2h: The risk management program defines and operates risk management policies and procedures that implement the risk management strategy

RM-2j: A risk catalog (a structured repository of identified chemical agents and risks) is used to support risk management activities



Visualization details

Domain(s): Risk Management (RM)

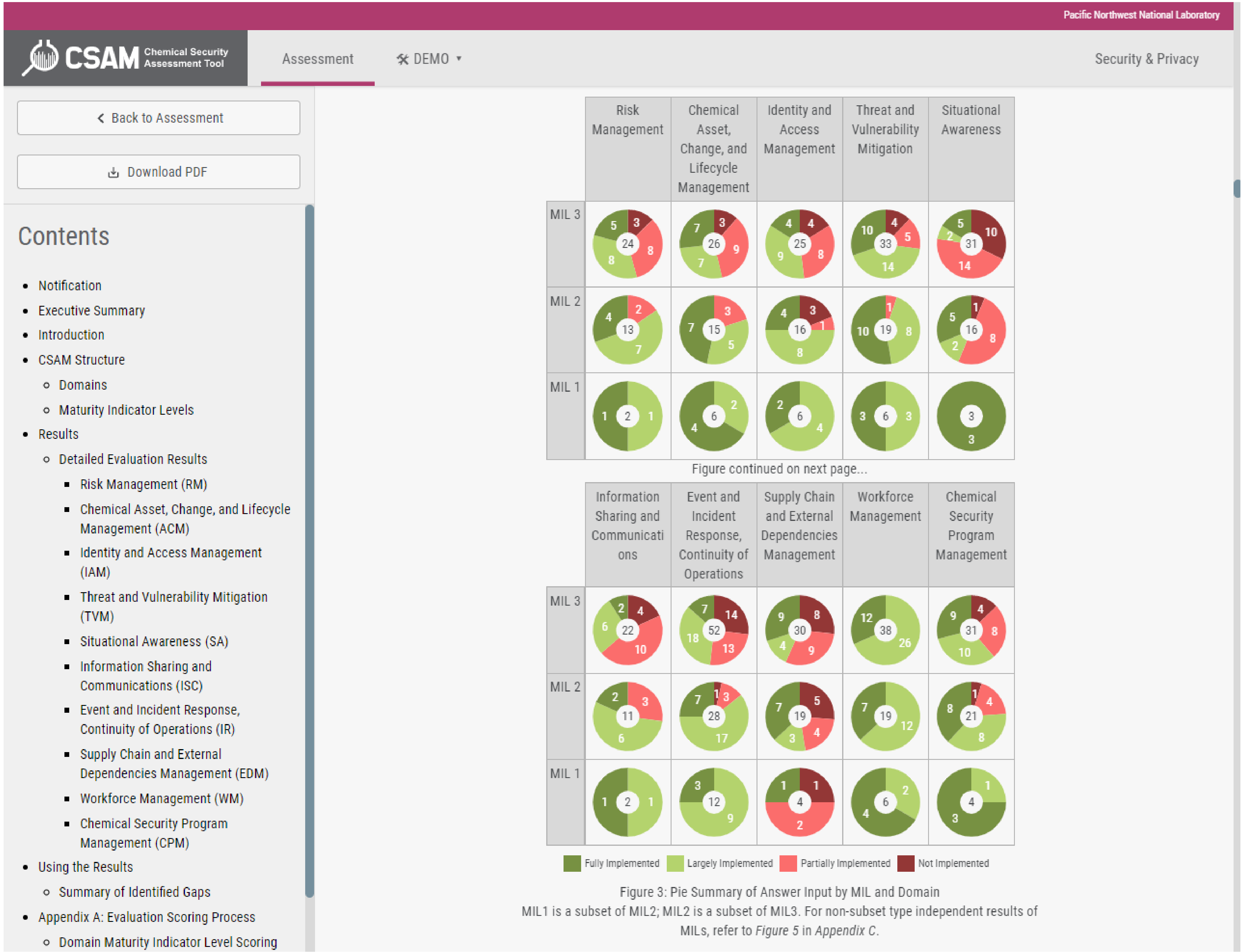
Subdomain(s): Manage Chemical Security

MIL(s): MIL 2

Partially Implemented (PI)

RM-2d: Identified risks are documented

RM-2g: Risk analysis is informed by local chemical experts



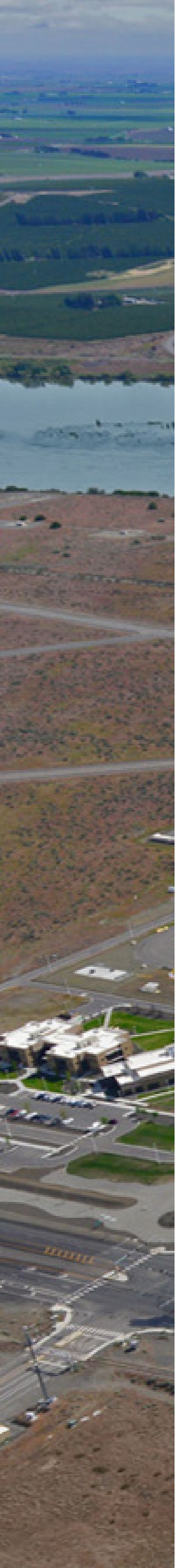
Pacific Northwest National Laboratory
CSAM Chemical Security Assessment Tool
Assessment
DEMO ▾
Security & Privacy
‹ Back to Assessment
Download PDF

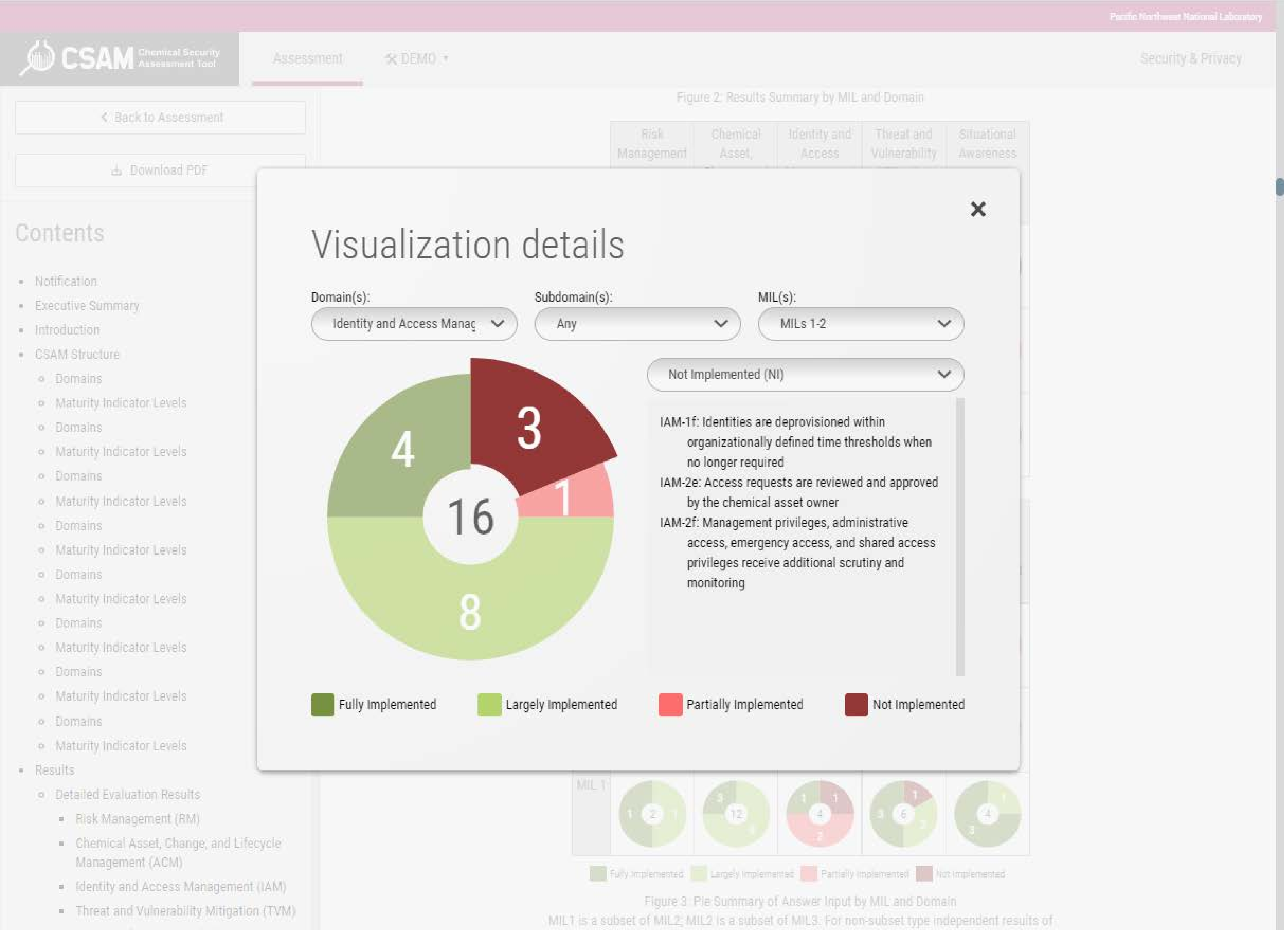
Contents

Figure continued on next page...

Information Sharing and Communications
Event and Incident Response, Continuity of Operations
Supply Chain and External Dependencies Management
Workforce Management
Chemical Security Program Management
MIL 3
2 4 6 22 10
7 14 18 52 13
9 8 30 4 9
12 38 26
9 4 31 8 10
MIL 2
2 3 11 6
7 1 3 28 17
7 5 19 3 4
7 19 12
8 1 4 21 8
MIL 1
1 2 1
3 12 9
1 1 4 2
6 2 4
4 1 3
🟩 Fully Implemented 🟩 Largely Implemented 🟥 Partially Implemented 🟥 Not Implemented

Figure 3: Pie Summary of Answer Input by MIL and Domain
MIL1 is a subset of MIL2; MIL2 is a subset of MIL3. For non-subset type independent results of MILs, refer to *Figure 5* in *Appendix C*.





Pacific Northwest National Laboratory

CSAM Chemical Security Assessment Tool

Assessment

DEMO

Security & Privacy

Back to Assessment

Download PDF

Contents

- Notification
- Executive Summary
- Introduction
- CSAM Structure
  - Domains
  - Maturity Indicator Levels
  - Domains
  - Maturity Indicator Levels
  - Domains
  - Maturity Indicator Levels
  - Domains
  - Maturity Indicator Levels
  - Domains
  - Maturity Indicator Levels
  - Domains
  - Maturity Indicator Levels
  - Domains
  - Maturity Indicator Levels
  - Domains
  - Maturity Indicator Levels
- Results
  - Detailed Evaluation Results
    - Risk Management (RM)
    - Chemical Asset, Change, and Lifecycle Management (ACM)
    - Identity and Access Management (IAM)
    - Threat and Vulnerability Mitigation (TVM)

Figure 2: Results Summary by MIL and Domain

Visualization details

Domain(s): Identity and Access Manag

Subdomain(s): Any

MIL(s): MILs 1-2

Not Implemented (NI)

IAM-1f: Identities are deprovisioned within organizationally defined time thresholds when no longer required

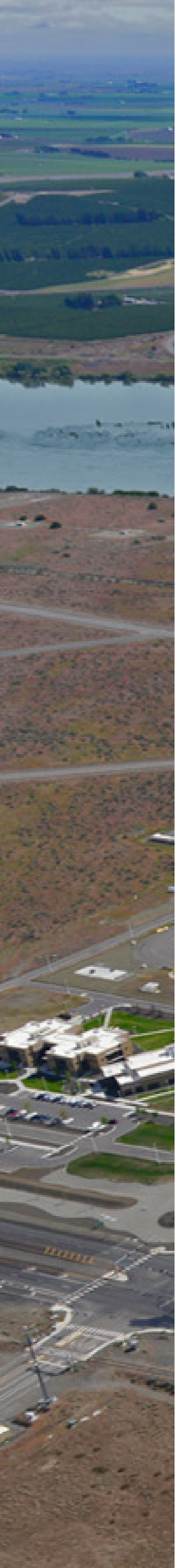
IAM-2e: Access requests are reviewed and approved by the chemical asset owner

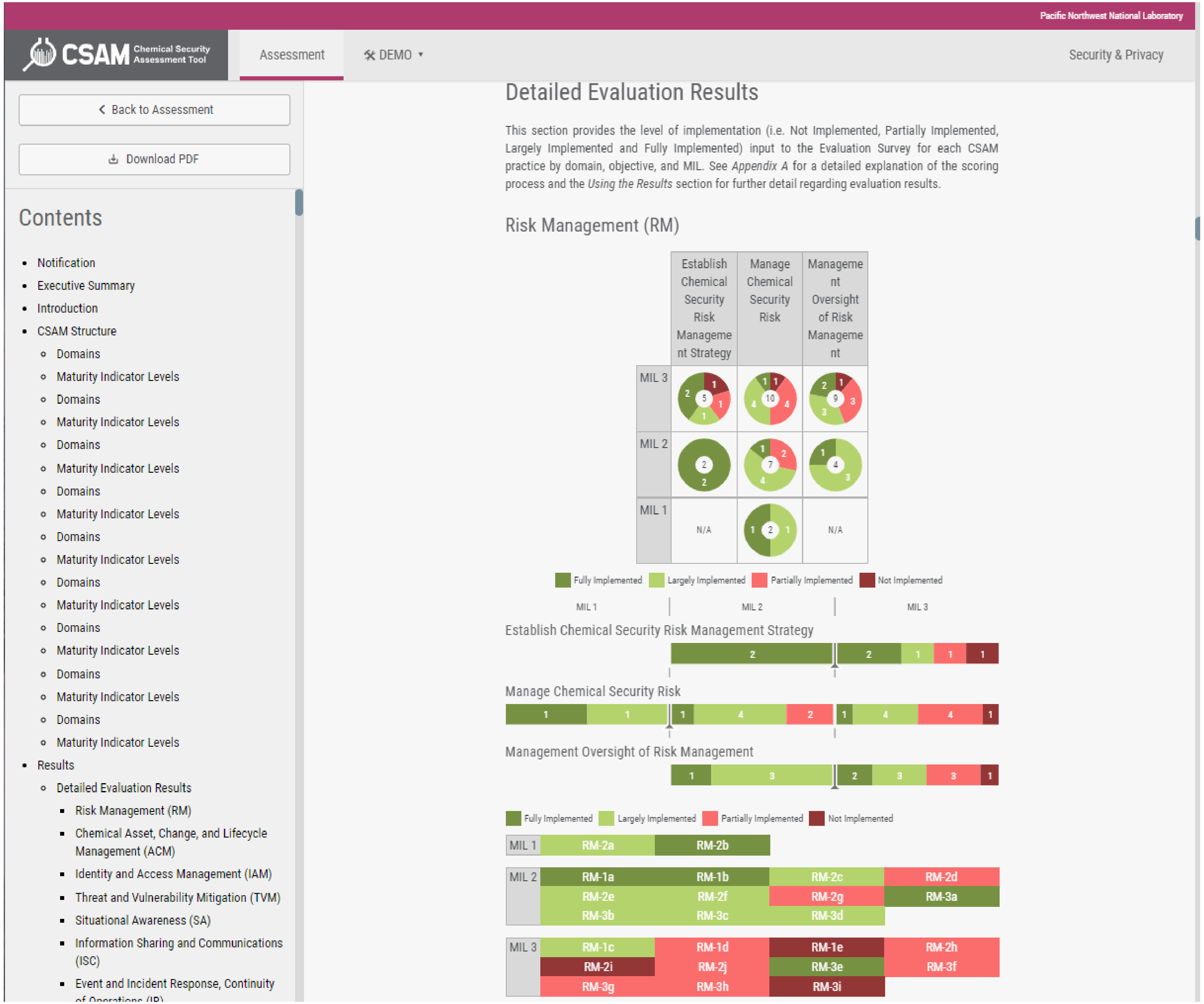
IAM-2f: Management privileges, administrative access, emergency access, and shared access privileges receive additional scrutiny and monitoring

🟩 Fully Implemented 🟩 Largely Implemented 🟥 Partially Implemented 🟥 Not Implemented

Figure 3: Pie Summary of Answer Input by MIL and Domain

MIL1 is a subset of MIL2; MIL2 is a subset of MIL3. For non-subset type independent results of





Pacific Northwest National Laboratory
CSAM Chemical Security Assessment Tool
Assessment
DEMO ▾
Security & Privacy
< Back to Assessment
Download PDF

Contents

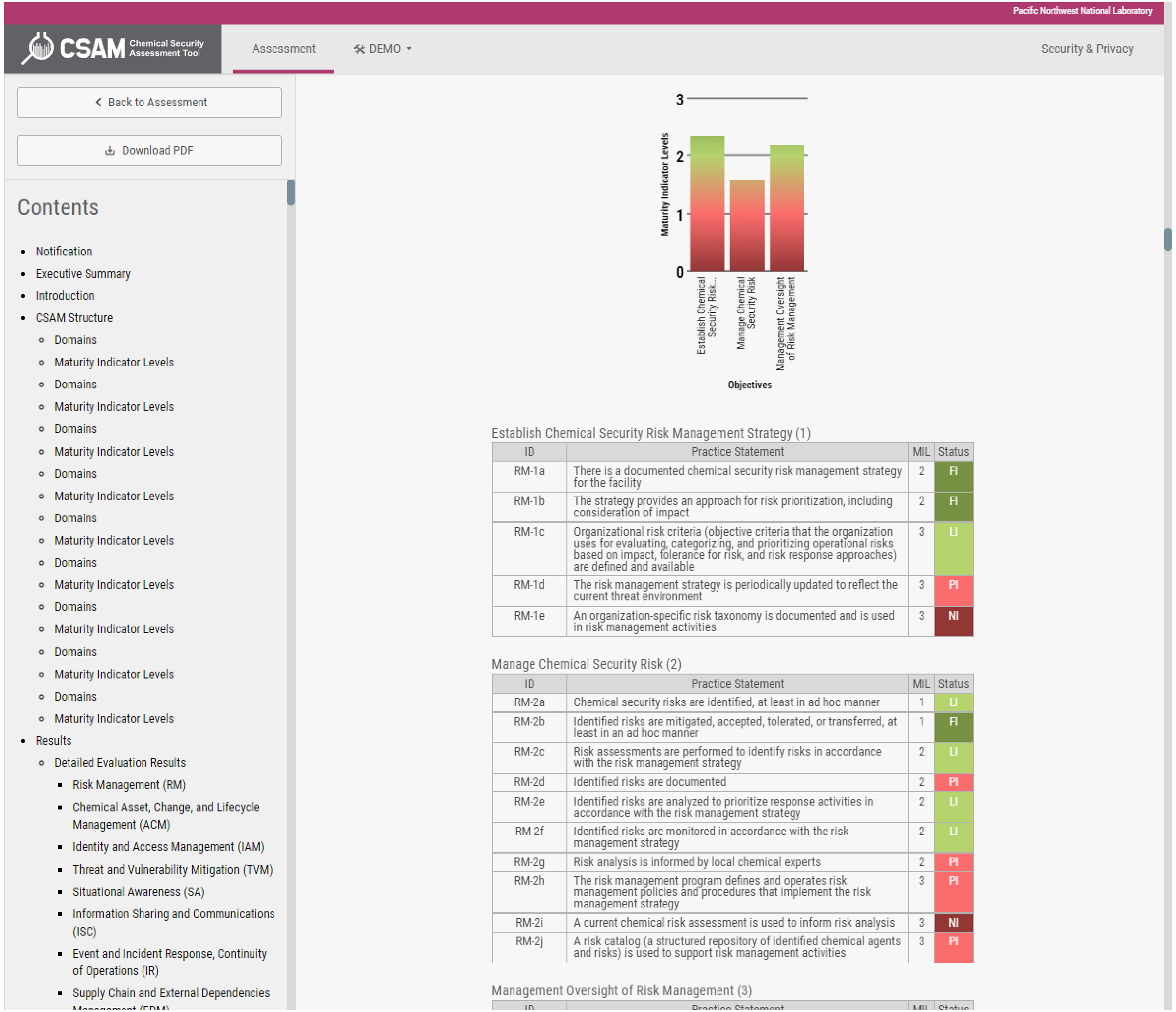
Detailed Evaluation Results

This section provides the level of implementation (i.e. Not Implemented, Partially Implemented, Largely Implemented and Fully Implemented) input to the Evaluation Survey for each CSAM practice by domain, objective, and MIL. See *Appendix A* for a detailed explanation of the scoring process and the *Using the Results* section for further detail regarding evaluation results.

Risk Management (RM)

MIL 1	RM-2a	RM-2b		
MIL 2	RM-1a	RM-1b	RM-2c	RM-2d
	RM-2e	RM-2f	RM-2g	RM-3a
	RM-3b	RM-3c	RM-3d	
MIL 3	RM-1c	RM-1d	RM-1e	RM-2h
	RM-2i	RM-2j	RM-3e	RM-3f
	RM-3g	RM-3h	RM-3i	

Pacific Northwest
NATIONAL LABORATORY


Pacific Northwest National Laboratory
CSAM Chemical Security Assessment Tool
Assessment
DEMO
Security & Privacy
Back to Assessment
Download PDF
3
2
1
0
Maturity Indicator Levels
Establish Chemical Security Risk...
Manage Chemical Security Risk
Management Oversight of Risk Management
Objectives

Contents

Establish Chemical Security Risk Management Strategy (1)

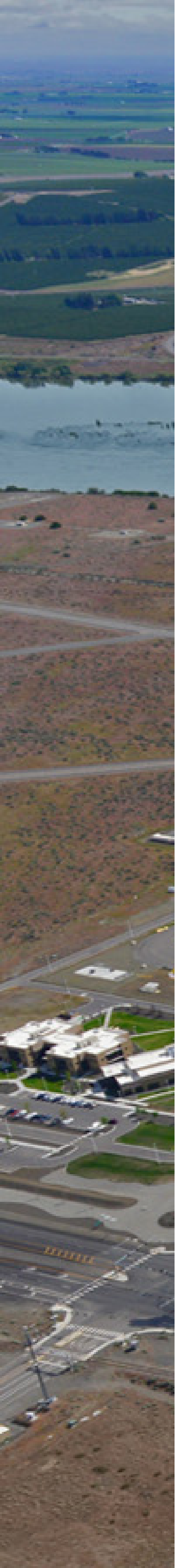
ID	Practice Statement	MIL	Status
RM-1a	There is a documented chemical security risk management strategy for the facility	2	FI
RM-1b	The strategy provides an approach for risk prioritization, including consideration of impact	2	FI
RM-1c	Organizational risk criteria (objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact, tolerance for risk, and risk response approaches) are defined and available	3	LI
RM-1d	The risk management strategy is periodically updated to reflect the current threat environment	3	PI
RM-1e	An organization-specific risk taxonomy is documented and is used in risk management activities	3	NI

Manage Chemical Security Risk (2)

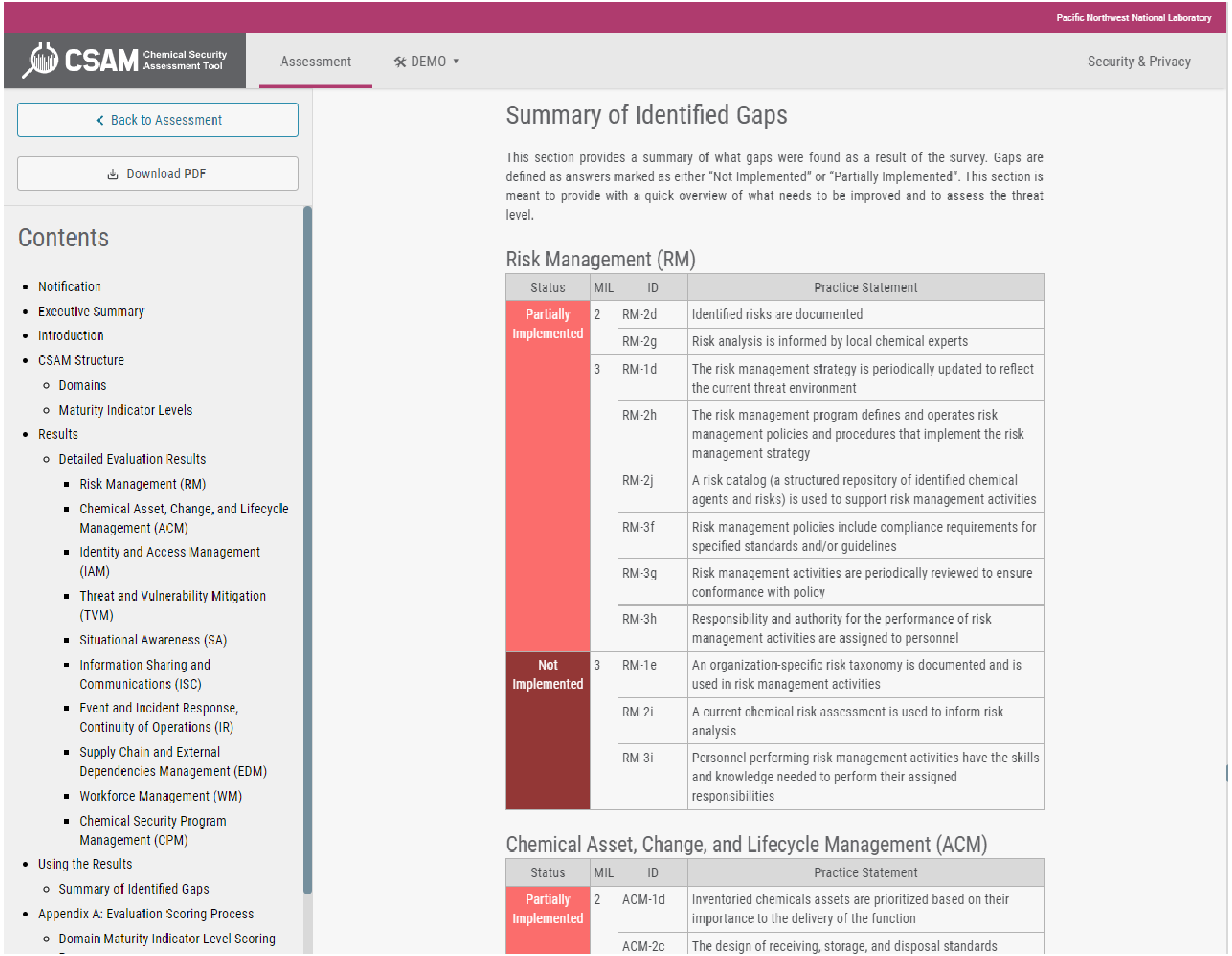
ID	Practice Statement	MIL	Status
RM-2a	Chemical security risks are identified, at least in ad hoc manner	1	LI
RM-2b	Identified risks are mitigated, accepted, tolerated, or transferred, at least in an ad hoc manner	1	FI
RM-2c	Risk assessments are performed to identify risks in accordance with the risk management strategy	2	LI
RM-2d	Identified risks are documented	2	PI
RM-2e	Identified risks are analyzed to prioritize response activities in accordance with the risk management strategy	2	LI
RM-2f	Identified risks are monitored in accordance with the risk management strategy	2	LI
RM-2g	Risk analysis is informed by local chemical experts	2	PI
RM-2h	The risk management program defines and operates risk management policies and procedures that implement the risk management strategy	3	PI
RM-2i	A current chemical risk assessment is used to inform risk analysis	3	NI
RM-2j	A risk catalog (a structured repository of identified chemical agents and risks) is used to support risk management activities	3	PI

Management Oversight of Risk Management (3)

ID	Practice Statement	MIL	Status



Pacific Northwest
NATIONAL LABORATORY



Pacific Northwest National Laboratory
CSAM Chemical Security Assessment Tool
Assessment
DEMO ▾
Security & Privacy
‹ Back to Assessment
Download PDF

Contents

Summary of Identified Gaps

This section provides a summary of what gaps were found as a result of the survey. Gaps are defined as answers marked as either "Not Implemented" or "Partially Implemented". This section is meant to provide with a quick overview of what needs to be improved and to assess the threat level.

Risk Management (RM)

Status	MIL	ID	Practice Statement
Partially Implemented	2	RM-2d	Identified risks are documented
		RM-2g	Risk analysis is informed by local chemical experts
	3	RM-1d	The risk management strategy is periodically updated to reflect the current threat environment
		RM-2h	The risk management program defines and operates risk management policies and procedures that implement the risk management strategy
		RM-2j	A risk catalog (a structured repository of identified chemical agents and risks) is used to support risk management activities
		RM-3f	Risk management policies include compliance requirements for specified standards and/or guidelines
		RM-3g	Risk management activities are periodically reviewed to ensure conformance with policy
		RM-3h	Responsibility and authority for the performance of risk management activities are assigned to personnel
Not Implemented	3	RM-1e	An organization-specific risk taxonomy is documented and is used in risk management activities
		RM-2i	A current chemical risk assessment is used to inform risk analysis
		RM-3i	Personnel performing risk management activities have the skills and knowledge needed to perform their assigned responsibilities

Chemical Asset, Change, and Lifecycle Management (ACM)

Status	MIL	ID	Practice Statement
Partially Implemented	2	ACM-1d	Inventoried chemicals assets are prioritized based on their importance to the delivery of the function
		ACM-2c	The design of receiving, storage, and disposal standards

Pacific Northwest
NATIONAL LABORATORY

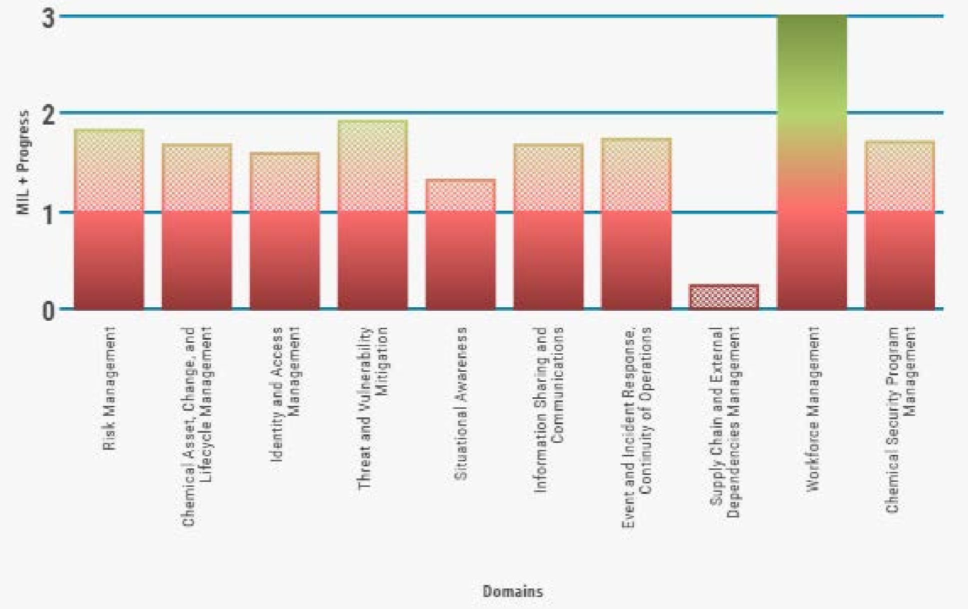
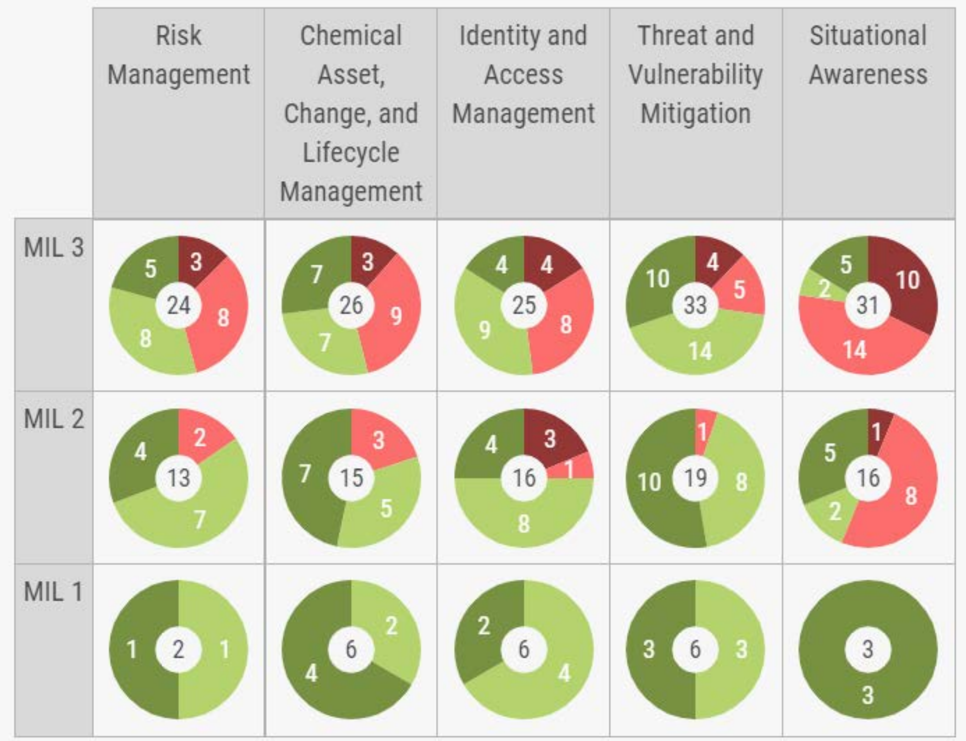
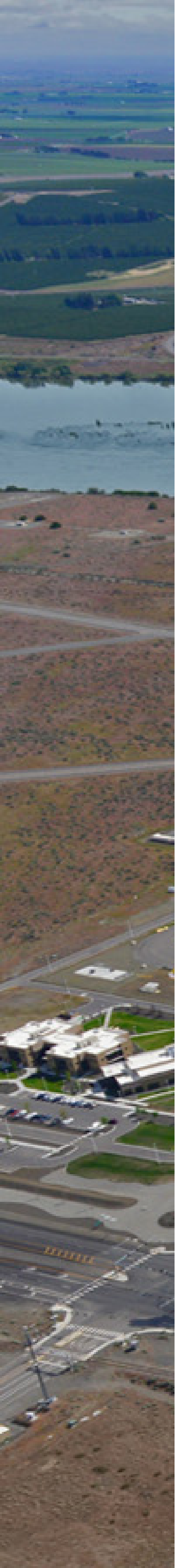

3
2
1
0
MIL + Progress
Risk Management
Chemical Asset, Change, and Lifecycle Management
Identity and Access Management
Threat and Vulnerability Mitigation
Situational Awareness
Information Sharing and Communications
Event and Incident Response, Continuity of Operations
Supply Chain and External Dependencies Management
Workforce Management
Chemical Security Program Management
Domains

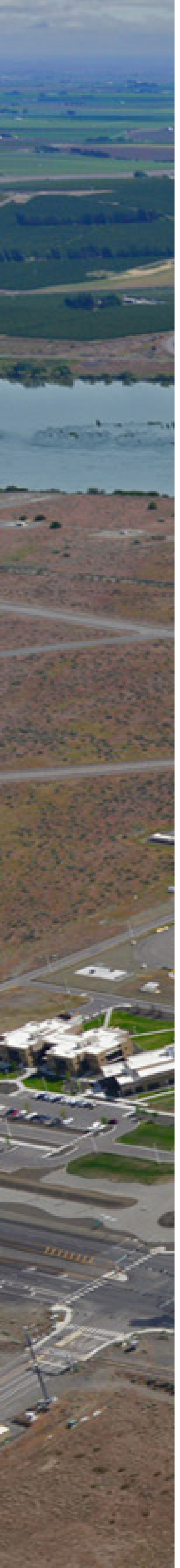
Figure 2: MIL Progression Rating – the Achieved MIL + Progress Toward the Next MIL by Domain





Pacific Northwest NATIONAL LABORATORY

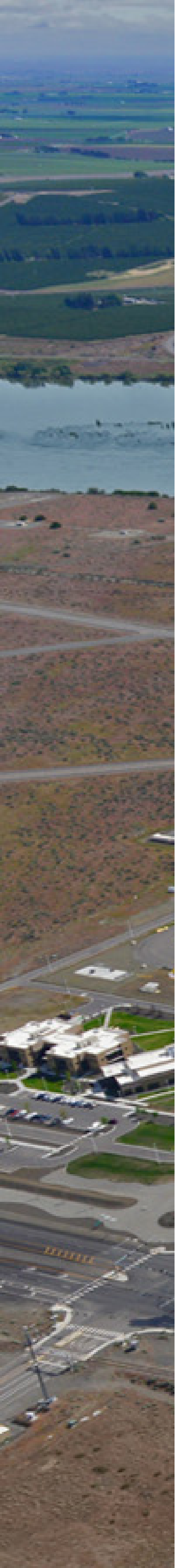
Thank you



Exercise E – Apply Chemical Security Maturity Model

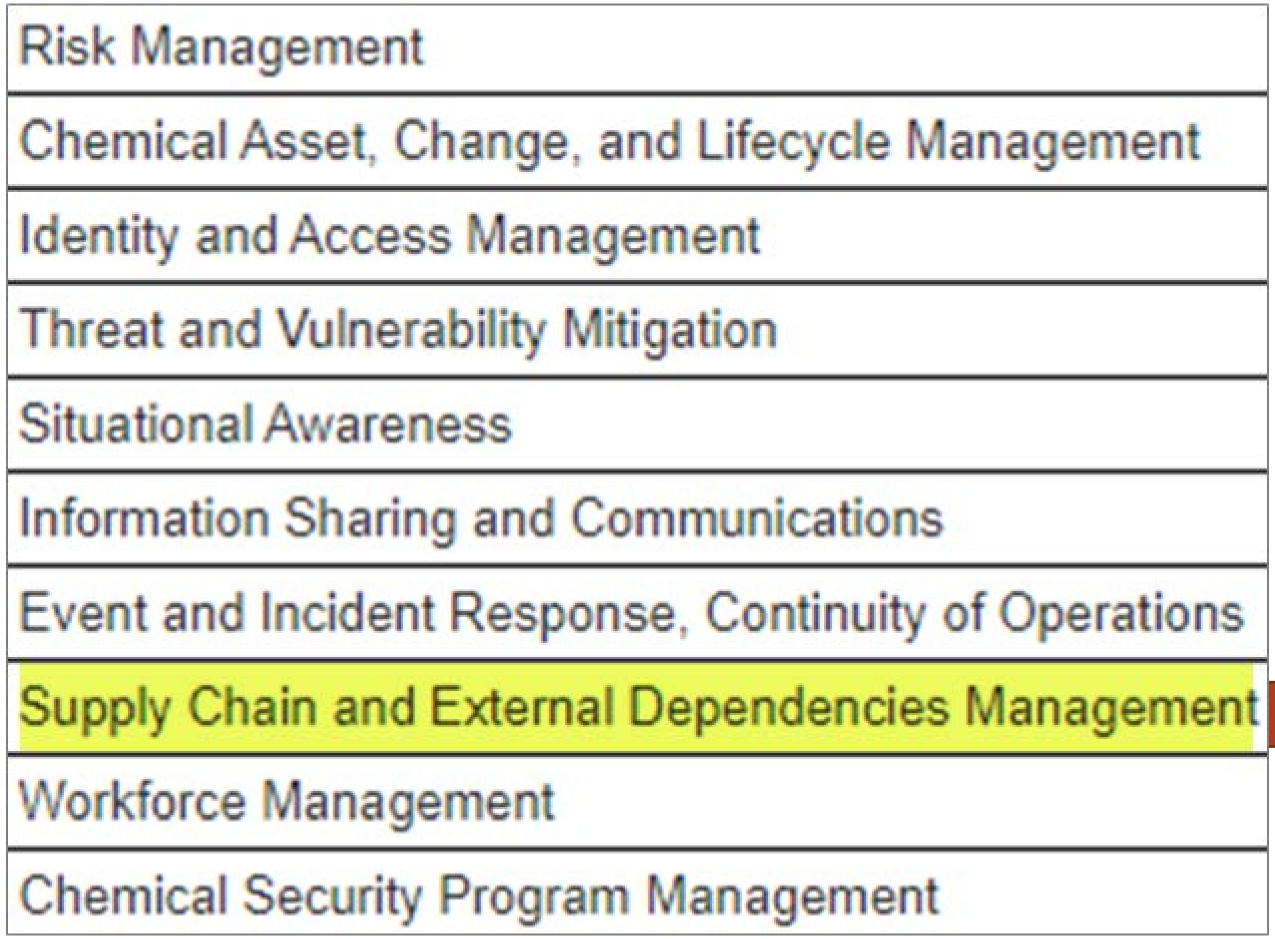
Cliff Glantz, Sri Nikhil Gourisetti,
Radha Kishan Motkuri, and John Cort
Pacific Northwest National Laboratory (PNNL)
Richland, WA, 99352
USA

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



In this Exercise: Focus on the Supply Chain Domain’s “Manage Dependency Risk” Objective

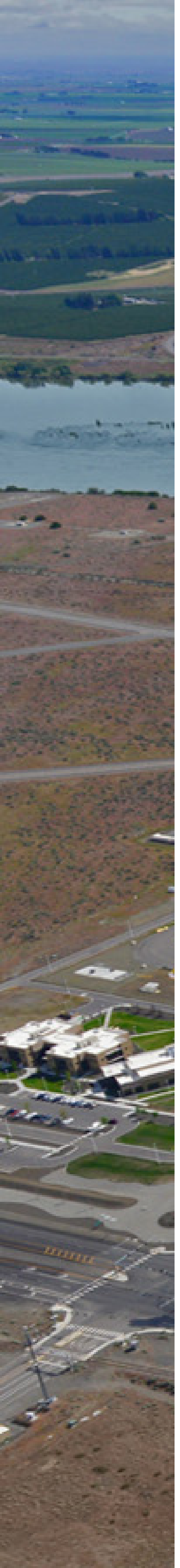
- You will apply the Chemical Security Assessment Model (CSAM) to evaluate your facility or an imaginary facility (your choice).



Risk Management
Chemical Asset, Change, and Lifecycle Management
Identity and Access Management
Threat and Vulnerability Mitigation
Situational Awareness
Information Sharing and Communications
Event and Incident Response, Continuity of Operations
Supply Chain and External Dependencies Management
Workforce Management
Chemical Security Program Management

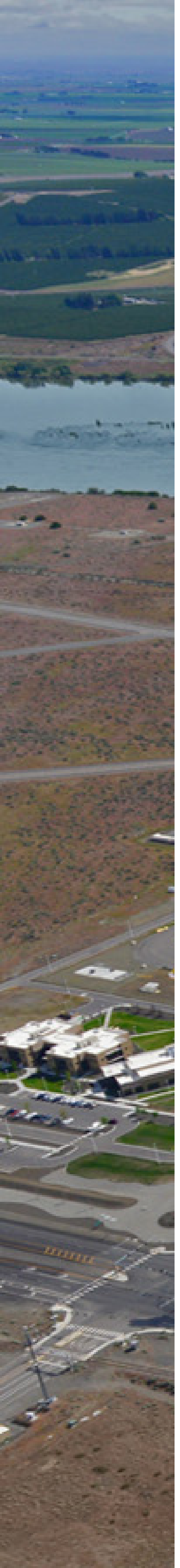
Objectives

1. Identify Dependencies
2. **Manage Dependency Risk**
3. Management Oversight of Supply Chain Risks



Each Domain Characterized by a Series of Practices.

4-point answer scale	The organization’s performance of the practice described in the model is …
Fully Implemented (FI)	Complete
Largely Implemented (LI)	Complete, but with a recognized opportunity for improvement
Partially Implemented (PI)	Incomplete; there are multiple opportunities for improvement
Not Implemented (NI)	Absent; the practice is not performed in the organization



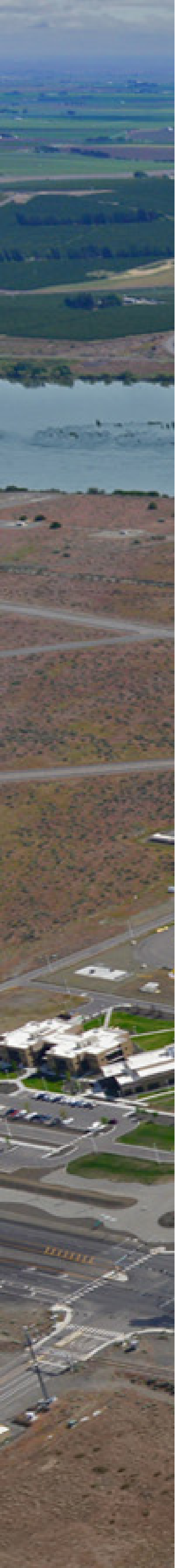
Pacific Northwest
NATIONAL LABORATORY

Instructions

- We will examine 12 supply chain practices – one-at-a-time – for the *Manage Dependencies Risk* objective.
- Evaluate each practice for your facility (or for an imaginary facility)
- Select one of four implementation scores for each practice:

○ Not Implemented	◒ Partially Implemented	◒ Largely Implemented	◉ Fully Implemented
1	**2**	**3**	**4**

- Provide your answer when each poll questions appears on your screen.



Pacific Northwest
NATIONAL LABORATORY

Supply Chain and External Dependencies: Manage Dependency Risk

1. Significant chemical security risks due to suppliers and other dependencies are identified and addressed, at least in an ad hoc manner

○ Not Implemented ◔ Partially Implemented ◑ Largely Implemented ● Fully Implemented

2. Chemical security requirements are considered, at least in an ad hoc manner, when establishing relationships with suppliers and other third parties

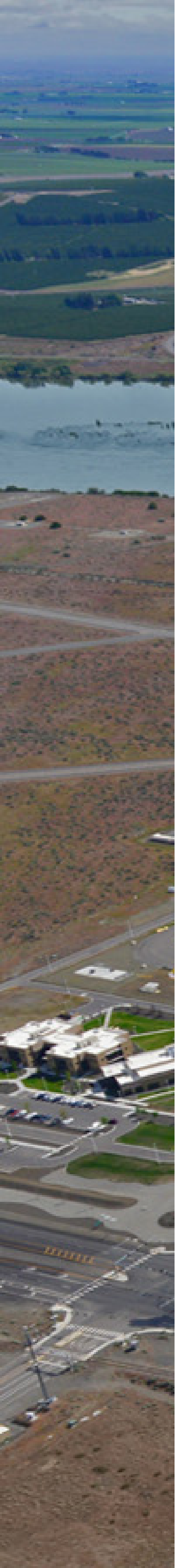
○ Not Implemented ◔ Partially Implemented ◑ Largely Implemented ● Fully Implemented

3. Identified chemical security dependency risks are entered into a risk document or database

○ Not Implemented ◔ Partially Implemented ◑ Largely Implemented ● Fully Implemented

1. Contracts and agreements with third parties incorporate sharing of chemical security threat information

○ Not Implemented ◔ Partially Implemented ◑ Largely Implemented ● Fully Implemented



Manage Dependency Risk (cont)

5. Chemical security requirements are established for suppliers

○ Not Implemented ◒ Partially Implemented ◒ Largely Implemented ◉ Fully Implemented

6. Evaluation and selection of suppliers and other external entities includes consideration of their ability to meet chemical security requirements

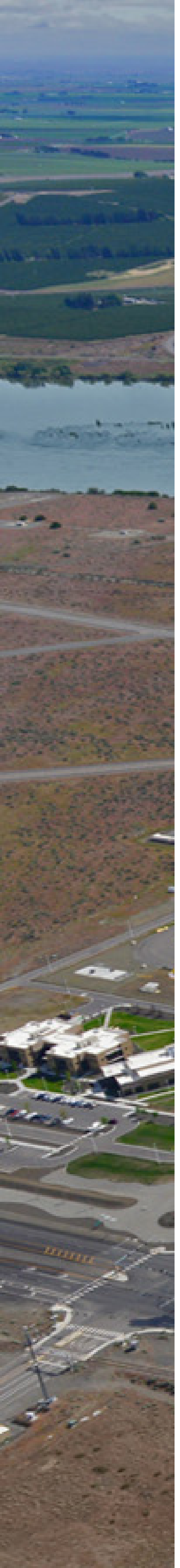
○ Not Implemented ◒ Partially Implemented ◒ Largely Implemented ◉ Fully Implemented

7. Agreements with suppliers require notification of chemical security incidents related to the delivery of the product or service

○ Not Implemented ◒ Partially Implemented ◒ Largely Implemented ◉ Fully Implemented

8. Suppliers and other external entities are periodically reviewed for their ability to continually meet chemical security requirements

○ Not Implemented ◒ Partially Implemented ◒ Largely Implemented ◉ Fully Implemented



Pacific Northwest
NATIONAL LABORATORY

Manage Dependency Risk (cont)

9. Chemical security risks due to external dependencies are managed according to the organization’s risk management process

   ○ Not Implemented ◒ Partially Implemented ◒ Largely Implemented ● Fully Implemented

10. Agreements with suppliers require notification of product defects that could result in security vulnerabilities at any point in the intended life cycle of delivered products

   ○ Not Implemented ◒ Partially Implemented ◒ Largely Implemented ● Fully Implemented

11. Procured assets are evaluated for defects that would increase chemical security risks

   ○ Not Implemented ◒ Partially Implemented ◒ Largely Implemented ● Fully Implemented

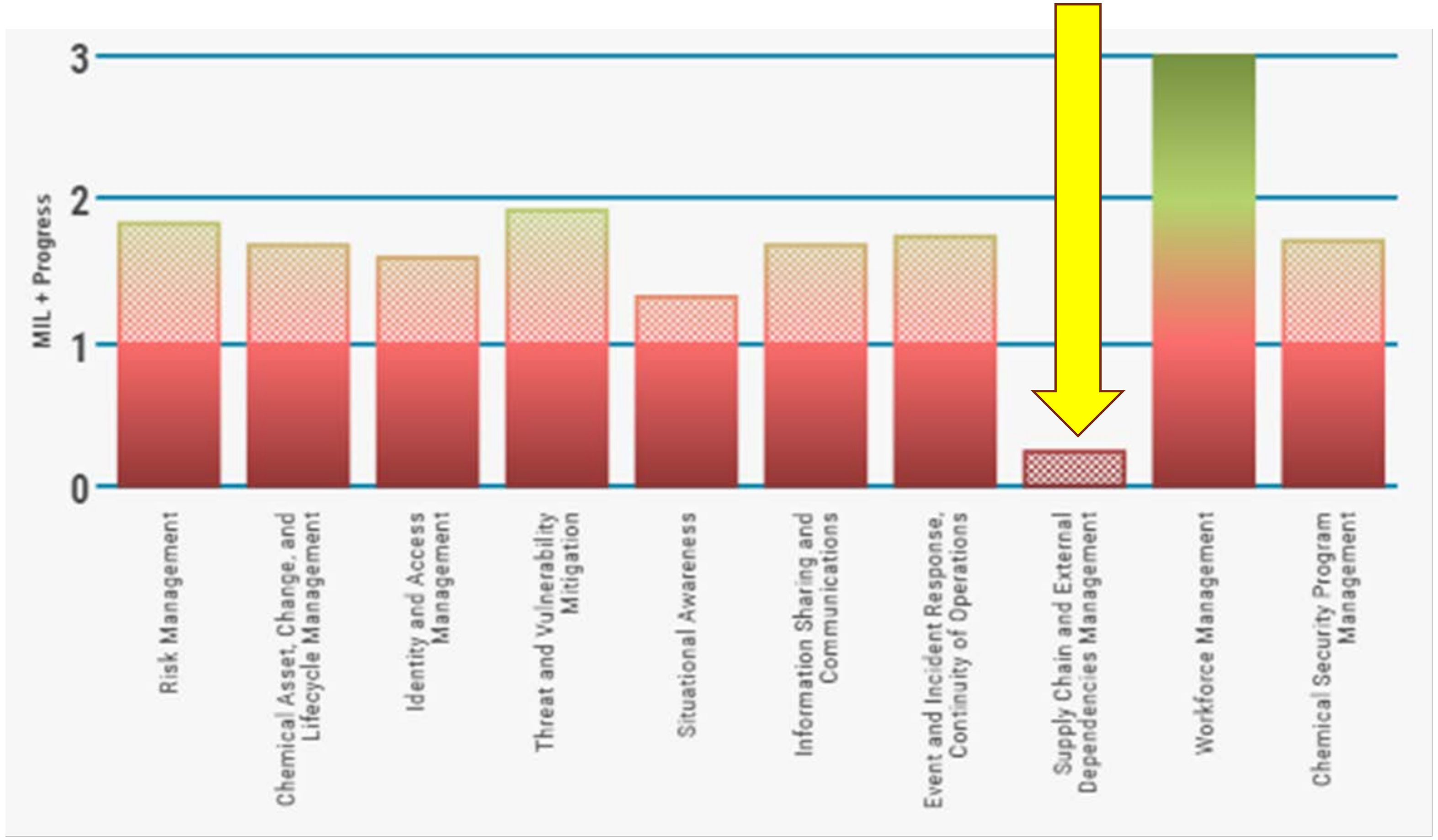
12. Information sources are monitored to identify and avoid supply chain threats (e.g., counterfeit chemicals, threats involving the theft of diversion of weaponizable chemicals)

   ○ Not Implemented ◒ Partially Implemented ◒ Largely Implemented ● Fully Implemented

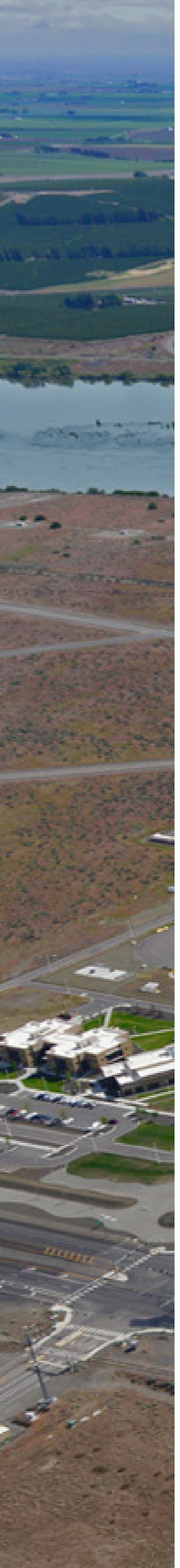
Present Results

Overall Results

- One domain ("Supply Chain…") does not achieve MIL1
- Eight domains achieve MIL1.
- One domain achieves MIL3.
- Decision makers must decide if this profile for the chemical security program is acceptable.
- One option is to accept this distribution if Supply Chain security is deemed less important than other domains.

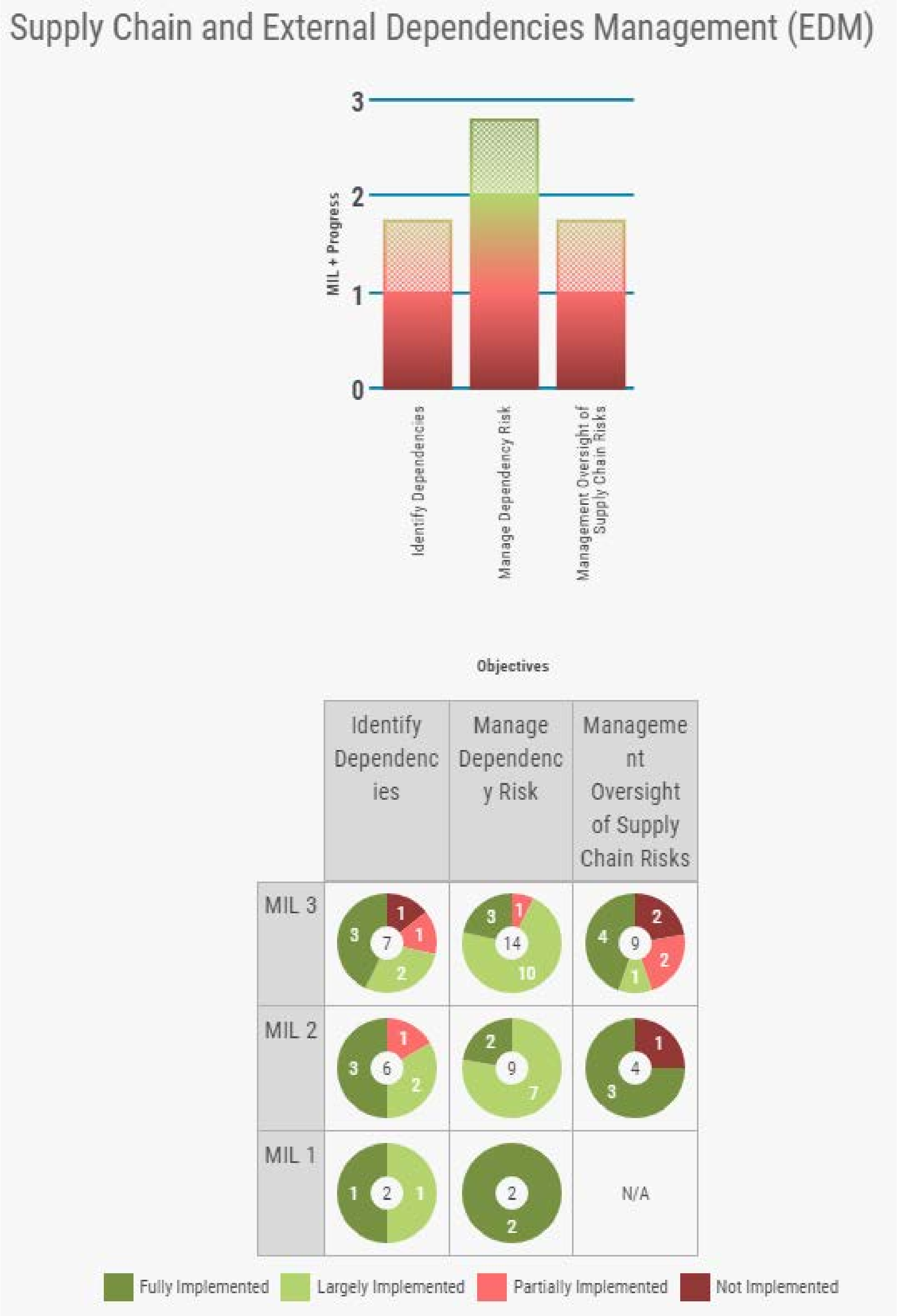


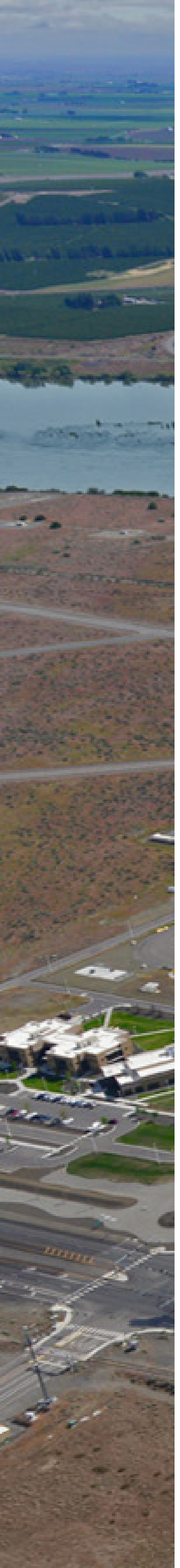
- Another option is to provide additional resources, or divert existing resources, to improve the Supply Chain performance program and bring it to MIL1 and in line with the eight domains that achieve MIL1 and are part way towards MIL2.



Supply Chain Domain

- Our exercise answers are provided for the *Manage Dependencies Risk* objective in the “Supply Chain…” domain.
- This objective achieves MIL2 and is well on its way toward achieving MIL 3.
- However, the other two objectives for this domain only achieve MIL1; though they are well along the way toward MIL2.
- Is the current distribution of sores acceptable to management?
- If improvements are warranted, determine if it is more cost effective to improve performance in the higher scoring *Manage Dependencies Risk* objective or in the other objectives.





Pacific Northwest
NATIONAL LABORATORY

Thank you

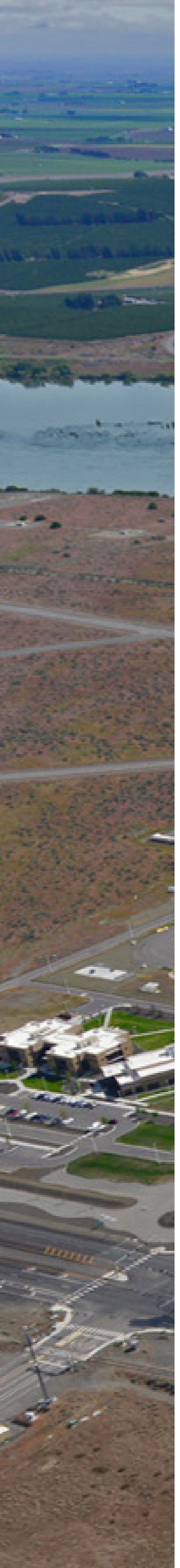
Pacific Northwest NATIONAL LABORATORY

Lesson 8: Assessing Security Continued -- Making Cost Effective Security Decisions and Evaluating Life Cycle and Supply Chain Security

Cliff Glantz, John Cort,
Radha K Motkuri, and Sri Nikhil Gourisetti
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

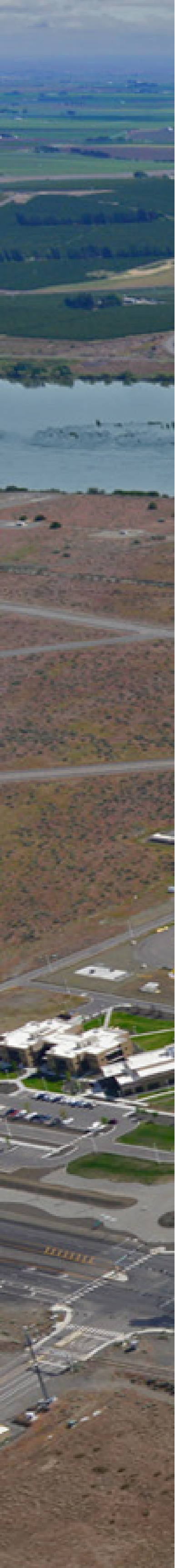


Pacific Northwest
NATIONAL LABORATORY

Return on Investment (ROI)

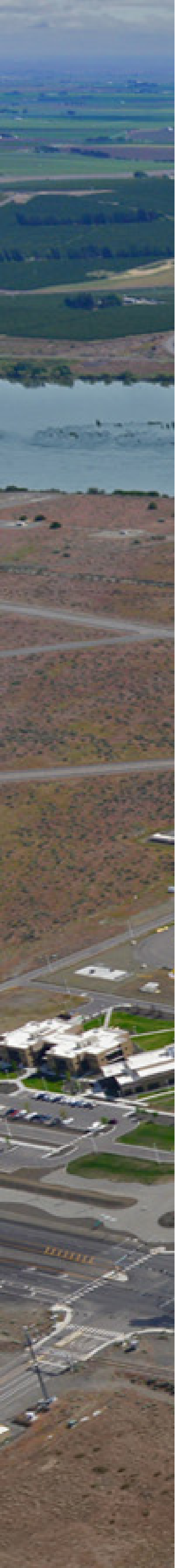
- Investment decisions in business are often based on **Return on Investment (ROI).**
  - A key goal of chemical or pharmaceutical companies is to **make money**, so they tend to pursue investments that offer the greatest possible return.
  - ROI is a commonly used profitability ratio that measures the amount of return, or profit, an investment generates relative to its cost.
  - ROI is expressed as a percentage and is useful in evaluating individual investments or competing investments.
  - To calculate ROI, the profit (return) from an investment is divided by the cost of that investment, as shown in the following formula:

$$\text{ROI} = (\text{gain} – \text{cost of investment}) / \text{cost of investment}$$



ROI (cont)

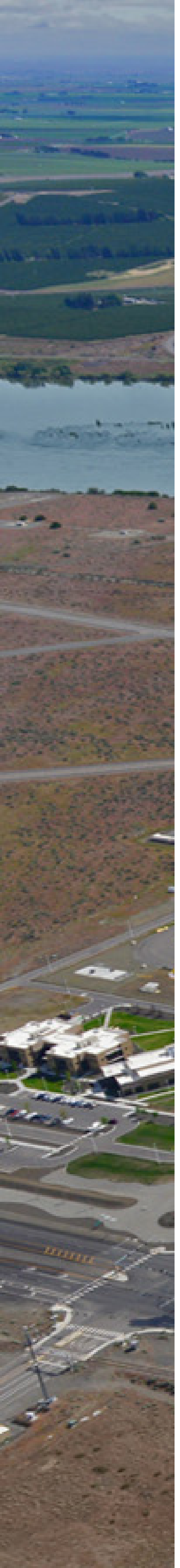
- While ROI is a great way to compare investment opportunities, ROI does **not** factor “risk” into the equation.
- ROI is a good way to measure what you potentially have to gain from an investment, but it **doesn't tell you what you have to lose from failing to make an investment**.
- Security improvements don’t often show up as a positive when using ROI because security does not typically enhance productivity (and it sometimes reduces productivity). However, security improvements can prevent companies from experiencing **big losses** that are hard to predict.
- For making security decisions, much like safety decisions, we have to consider risk.



Pacific Northwest NATIONAL LABORATORY

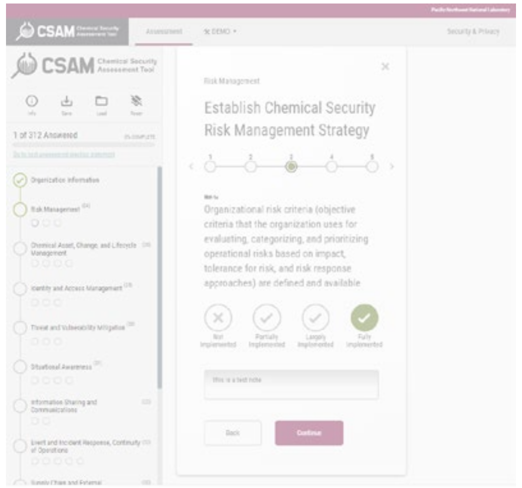
How do you Present Security Risk Assessments to Decision Makers?

- When presenting security options to decision makers it is **important for them to be aware of security risks.**
- This includes keeping decision makers informed of:
    - Emerging threats
    - Vulnerabilities
    - Potential consequences
    - Probabilities of incidents (it can be as simple a characterization as “near certain”, “good chance”, “unlikely but not negligible”, “remote possibility”)
- Remind the decision makers that **security does not fit into the traditional ROI framework, but it can protect against big losses** that could impact the company’s long-term profitability and its relationship with stakeholders (including customers, regulators, and suppliers).



Today We Introduce Two New Maturity Models

- The **Chemical Security Assessment Model (CSAM)** is designed to assist chemical facilities and laboratories in identifying the maturity of the chemical security program, and to identify programmatic areas to strengthen and maintain a desired level of security throughout the chemical life cycle.

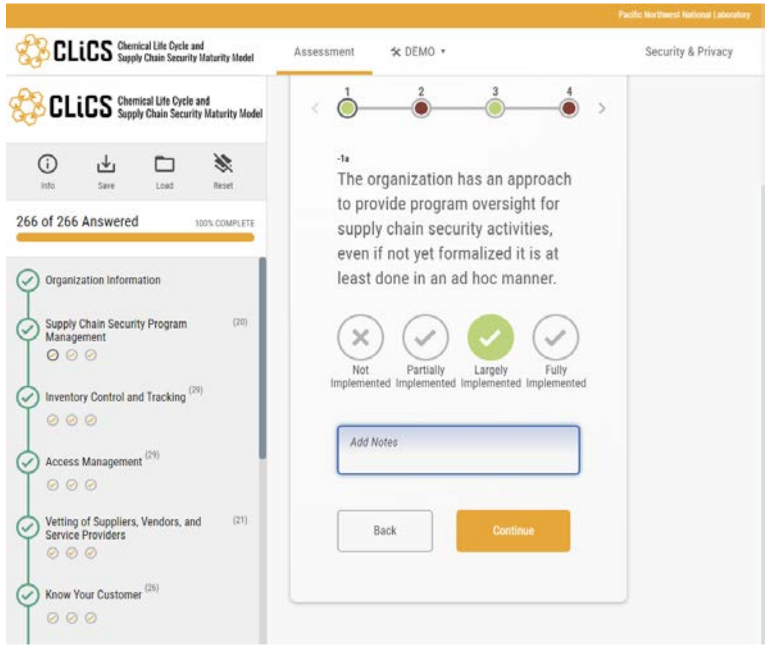

Pacific Northwest National Laboratory
CSAM Chemical Security Assessment Tool
Assessment
DEMO
Security & Privacy
CSAM Chemical Security Assessment Tool
Info
Save
Load
Reset
1 of 312 Answered
Organization Information
Risk Management
Chemical Asset, Change, and Lifecycle Management
Identity and Access Management
Threat and Vulnerability Mitigation
Situational Awareness
Information Sharing and Communications
Event and Incident Response, Continuity of Operations
Supply Chain and External
Risk Management
1
2
3
4
5
Not Implemented
Partially Implemented
Largely Implemented
Fully Implemented
Back
Continue

Establish Chemical Security Risk Management Strategy

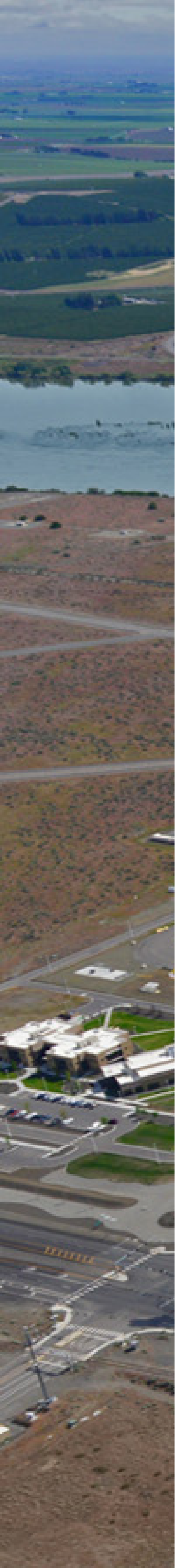
Organizational risk criteria (objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact, tolerance for risk, and risk response approaches) are defined and available

This is a test note

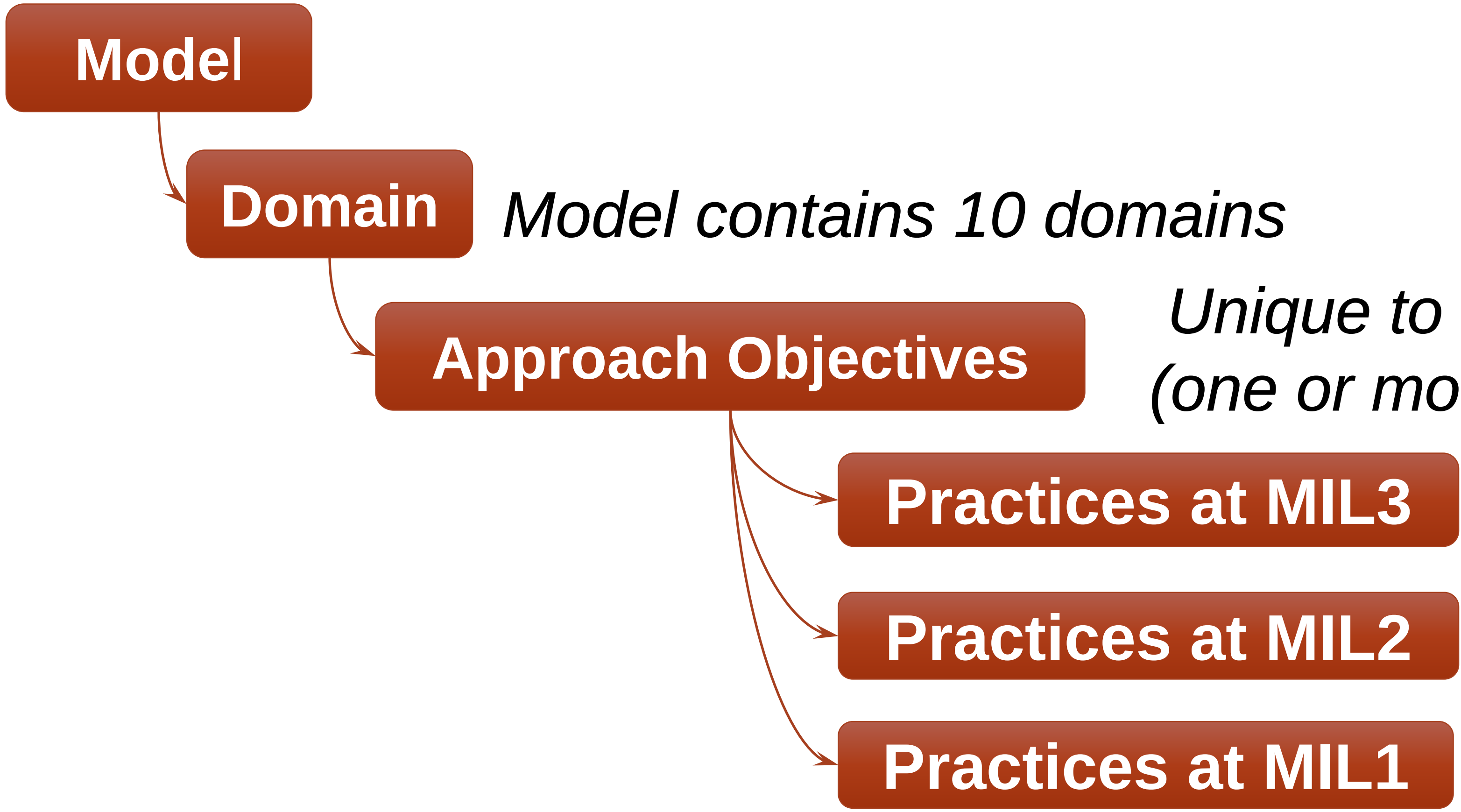
- The **Chemical Life Cycle and Supply Chain Security** (CLiCS) Maturity Model focuses on chemical security throughout the product life cycle, with an emphasis on supply chain and “know your customer” security objectives.


Pacific Northwest National Laboratory
CLiCS Chemical Life Cycle and Supply Chain Security Maturity Model
Assessment
DEMO
Security & Privacy
CLiCS Chemical Life Cycle and Supply Chain Security Maturity Model
Info
Save
Load
Reset
266 of 266 Answered
100% COMPLETE
Organization Information
Supply Chain Security Program Management (20)
Inventory Control and Tracking (29)
Access Management (29)
Vetting of Suppliers, Vendors, and Service Providers (21)
Know Your Customer (26)
1
2
3
4
-1a
Not Implemented
Partially Implemented
Largely Implemented
Fully Implemented
Add Notes
Back
Continue

The organization has an approach to provide program oversight for supply chain security activities, even if not yet formalized it is at least done in an ad hoc manner.



Organization of the CLiCS Maturity Model



Model

Domain

Approach Objectives

Practices at MIL3

Practices at MIL2

Practices at MIL1

Model contains 10 domains

Unique to each domain (one or more per domain)

Approach objectives are supported by a progression of practices that are unique to the domain

Pacific Northwest
NATIONAL LABORATORY

The CLiCS Features 10 Domains

Risk Management

Inventory Control and Tracking

Access Management

Cyber, Physical, and Personnel Security

Vetting of Suppliers, Vendors, and Service Providers

Transportation Security Management

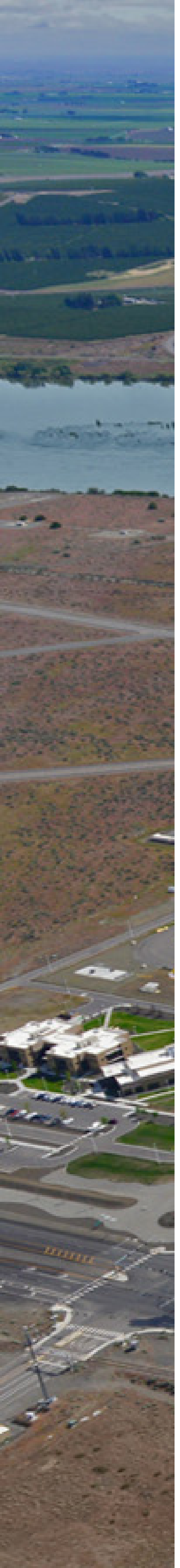
Security Incident Response and Recovery

Know Your Customer

Workforce Management

Supply Chain Security Program Management

Domains are logical groupings of cybersecurity practices



CLiCS Domains

Risk Management

- Identify threats, vulnerabilities, and consequences and apply risk management principles.

Inventory Control and Tracking

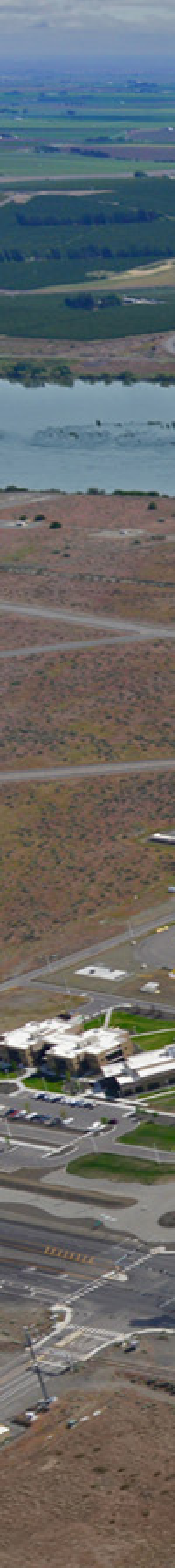
- Develop and implement a method to control and track physical and digital assets and chemical products.

Access Management

- Restrict physical access to facilities, information, and products to authorized personnel.

Cyber, Physical, and Personnel Security

- The life-cycle protection of assets and products involves an explicit consideration of physical, cyber, and personnel security.



Pacific Northwest
NATIONAL LABORATORY

CLiCS Domains (cont)

Vetting of Suppliers, Vendors, and Service Providers

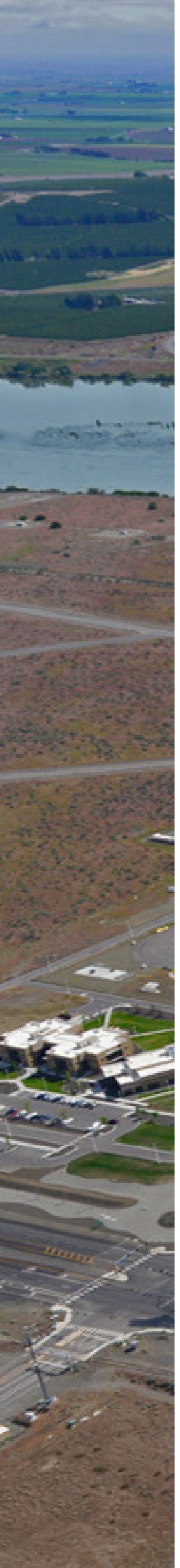
- Ensure that suppliers and vendors are reputable
- Appropriately restrict physical and digital access to your systems and information
- Monitor supplier, vendors, and service providers to determine if they are following the provisions in their contract.

Transportation Security Management

- Provide adequate security and tamper protection during transport
- Track products during their transport
- Verify that products are transported in a safe and security manner.

Security Incident Response and Recovery

- Security events are identified, assessed, and responded to in an appropriate manner.



CLiCS Domains (cont)

Know Your Customer

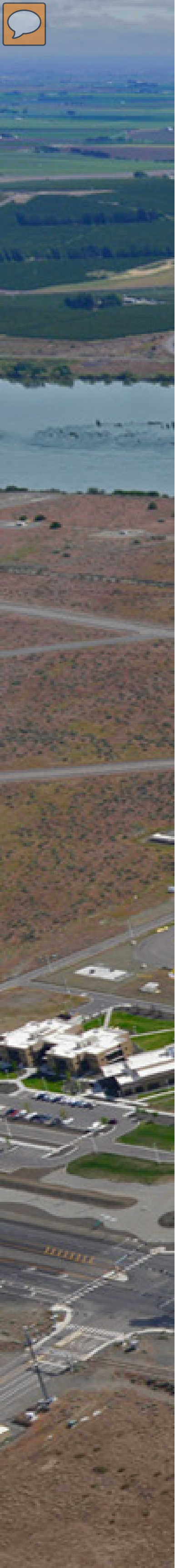
- Ensure that customers are legitimate businesses
- Monitor to see if the they are doing what they say they are doing with your products (practicing ethical behavior).

Workforce Management

- All company staff receive appropriate and position-specific safety and security training needed to help prevent sabotage, theft or diversion of materials, theft of information, and malicious insider actions.

Supply Chain Security Program Management

- Develop chemical life cycle and supply chain security policies.
- Ensure roles and responsibilities for all aspects of chemical life cycle and supply chain security are clearly established and implemented.



Pacific Northwest
NATIONAL LABORATORY

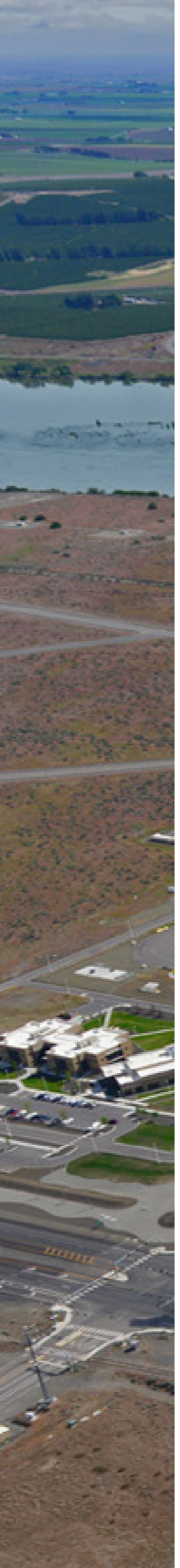
Maturity Indicator Level (MIL) Indicates the Maturity Level in Each Domain

MIL 3 - Guided & reviewed in conformance with policy. Responsibility and authority assigned to appropriately skilled personnel.

MIL 2 - Practices documented, stakeholders involved, and adequate resources provided and used

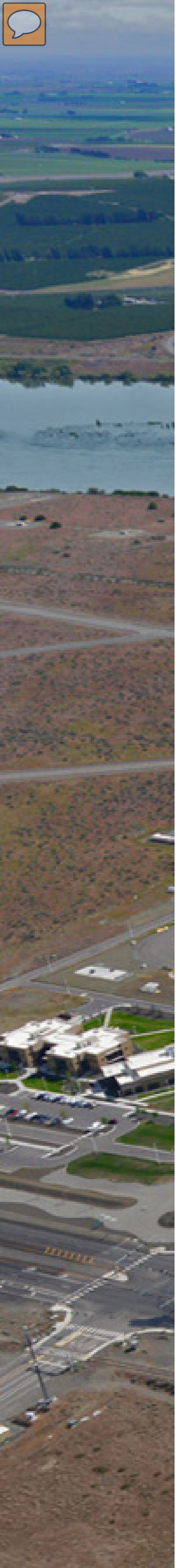
MIL 1 - Initial practices performed maybe in ad hoc manner (i.e., makeshift, improvised, undocumented)

MIL 0 – Not Achieved

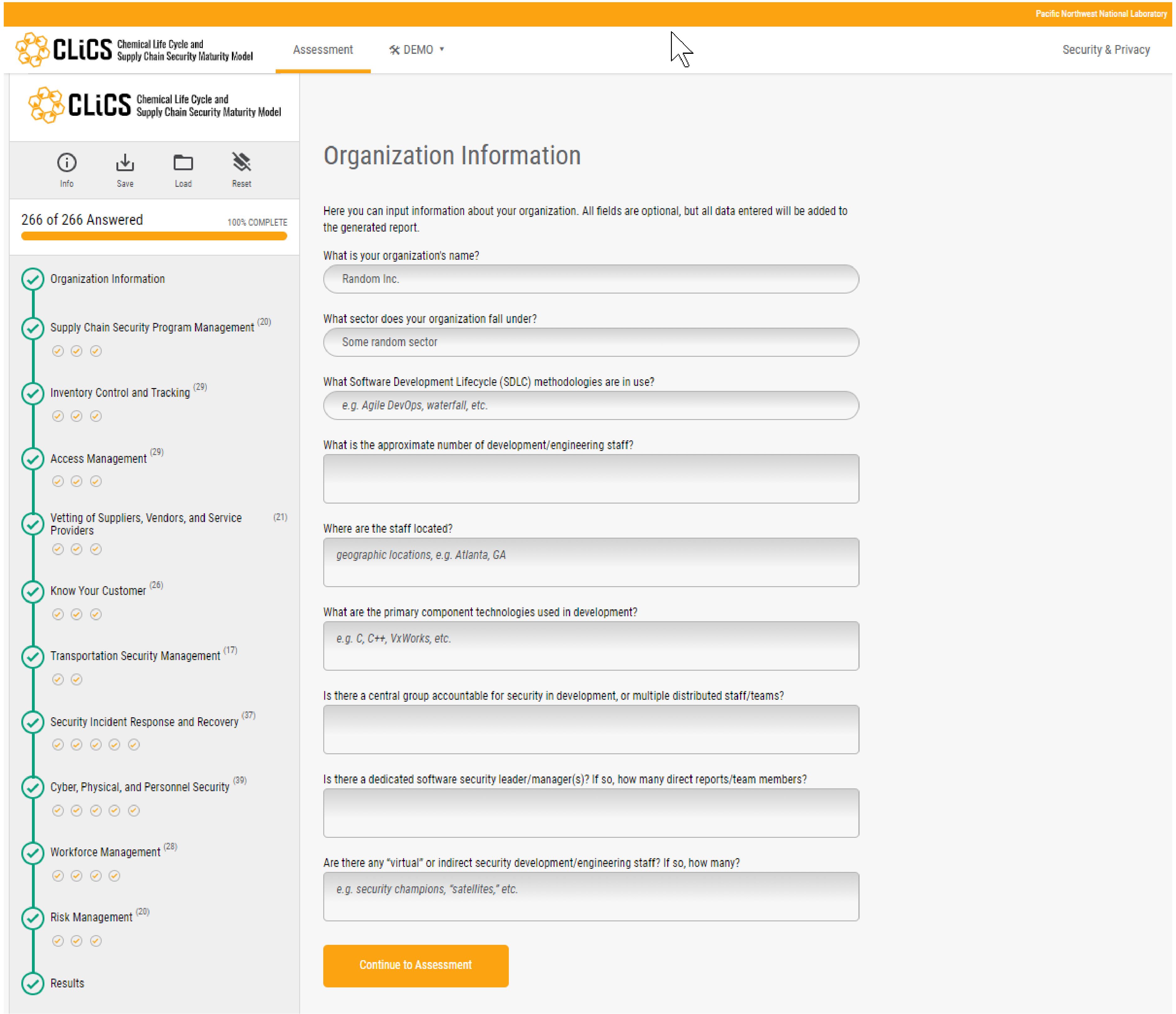


Each Domain Characterized by a Series of Practices.

4-point answer scale	The organization’s performance of the practice described in the model is …
Fully Implemented (FI)	Complete
Largely Implemented (LI)	Complete, but with a recognized opportunity for improvement
Partially Implemented (PI)	Incomplete; there are multiple opportunities for improvement
Not Implemented (NI)	Absent; the practice is not performed in the organization



Pacific Northwest
NATIONAL LABORATORY



Pacific Northwest National Laboratory
CLiCS Chemical Life Cycle and Supply Chain Security Maturity Model
Assessment
DEMO ▾
Security & Privacy
Info
Save
Load
Reset

266 of 266 Answered — 100% COMPLETE

- ✓ Organization Information
- ✓ Supply Chain Security Program Management (20)
- ✓ Inventory Control and Tracking (29)
- ✓ Access Management (29)
- ✓ Vetting of Suppliers, Vendors, and Service Providers (21)
- ✓ Know Your Customer (26)
- ✓ Transportation Security Management (17)
- ✓ Security Incident Response and Recovery (37)
- ✓ Cyber, Physical, and Personnel Security (39)
- ✓ Workforce Management (28)
- ✓ Risk Management (20)
- ✓ Results

Organization Information

Here you can input information about your organization. All fields are optional, but all data entered will be added to the generated report.

What is your organization's name?
Random Inc.

What sector does your organization fall under?
Some random sector

What Software Development Lifecycle (SDLC) methodologies are in use?
e.g. Agile DevOps, waterfall, etc.

What is the approximate number of development/engineering staff?

Where are the staff located?
geographic locations, e.g. Atlanta, GA

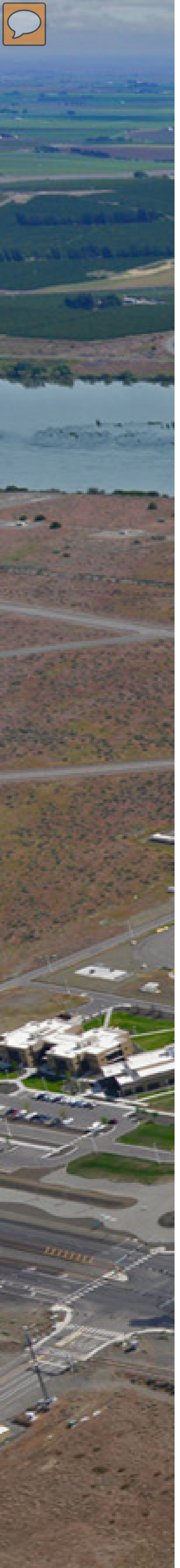
What are the primary component technologies used in development?
e.g. C, C++, VxWorks, etc.

Is there a central group accountable for security in development, or multiple distributed staff/teams?

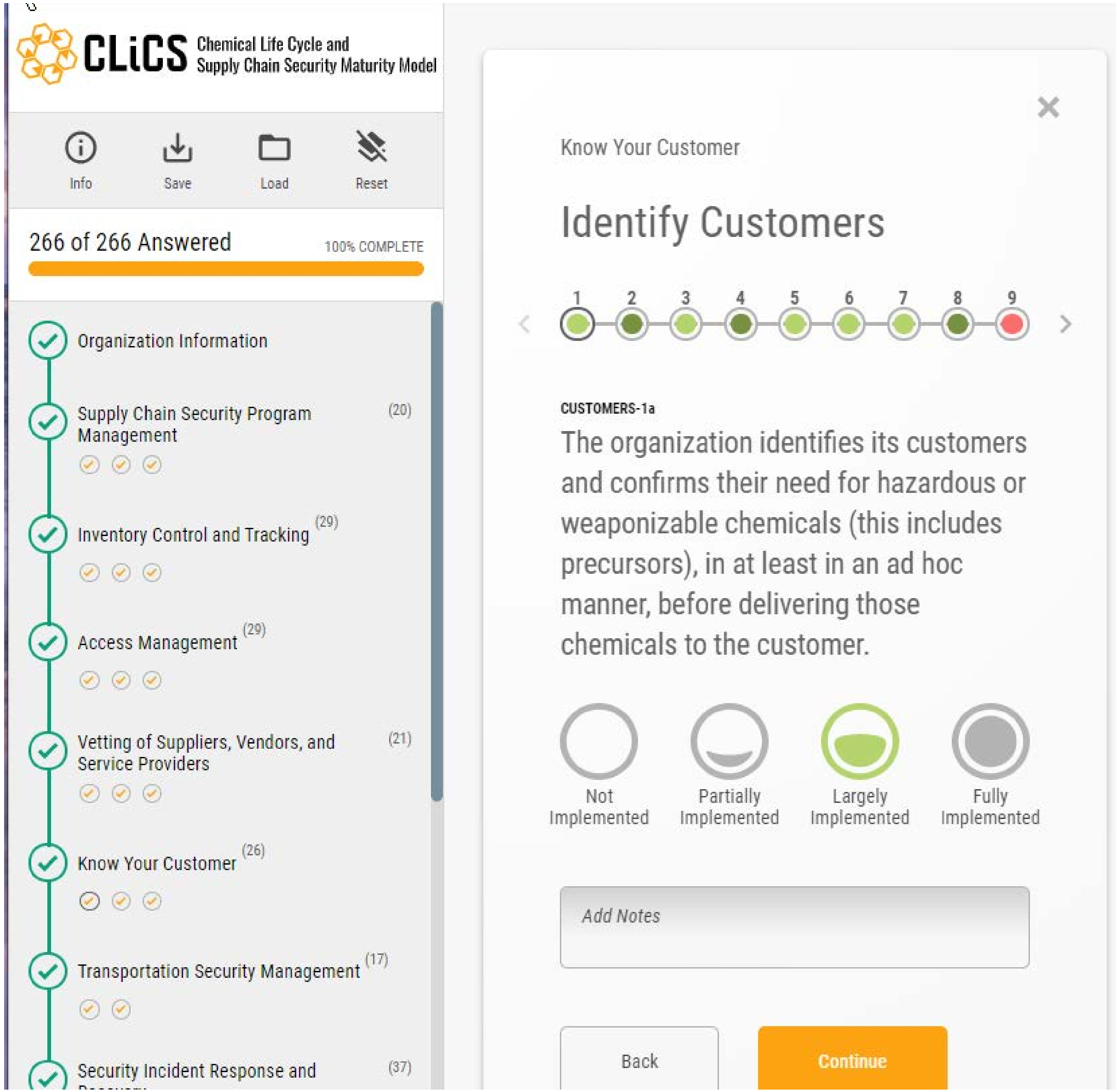
Is there a dedicated software security leader/manager(s)? If so, how many direct reports/team members?

Are there any "virtual" or indirect security development/engineering staff? If so, how many?
e.g. security champions, "satellites," etc.

Continue to Assessment



Pacific Northwest
NATIONAL LABORATORY



CLiCS Chemical Life Cycle and Supply Chain Security Maturity Model

266 of 266 Answered 100% COMPLETE

- ✓ Organization Information
- ✓ Supply Chain Security Program Management (20)
- ✓ Inventory Control and Tracking (29)
- ✓ Access Management (29)
- ✓ Vetting of Suppliers, Vendors, and Service Providers (21)
- ✓ Know Your Customer (26)
- ✓ Transportation Security Management (17)
- ✓ Security Incident Response and Recovery (37)

Know Your Customer

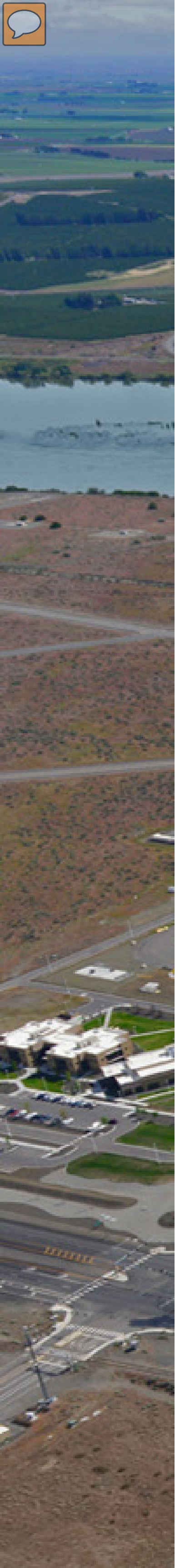
Identify Customers

CUSTOMERS-1a

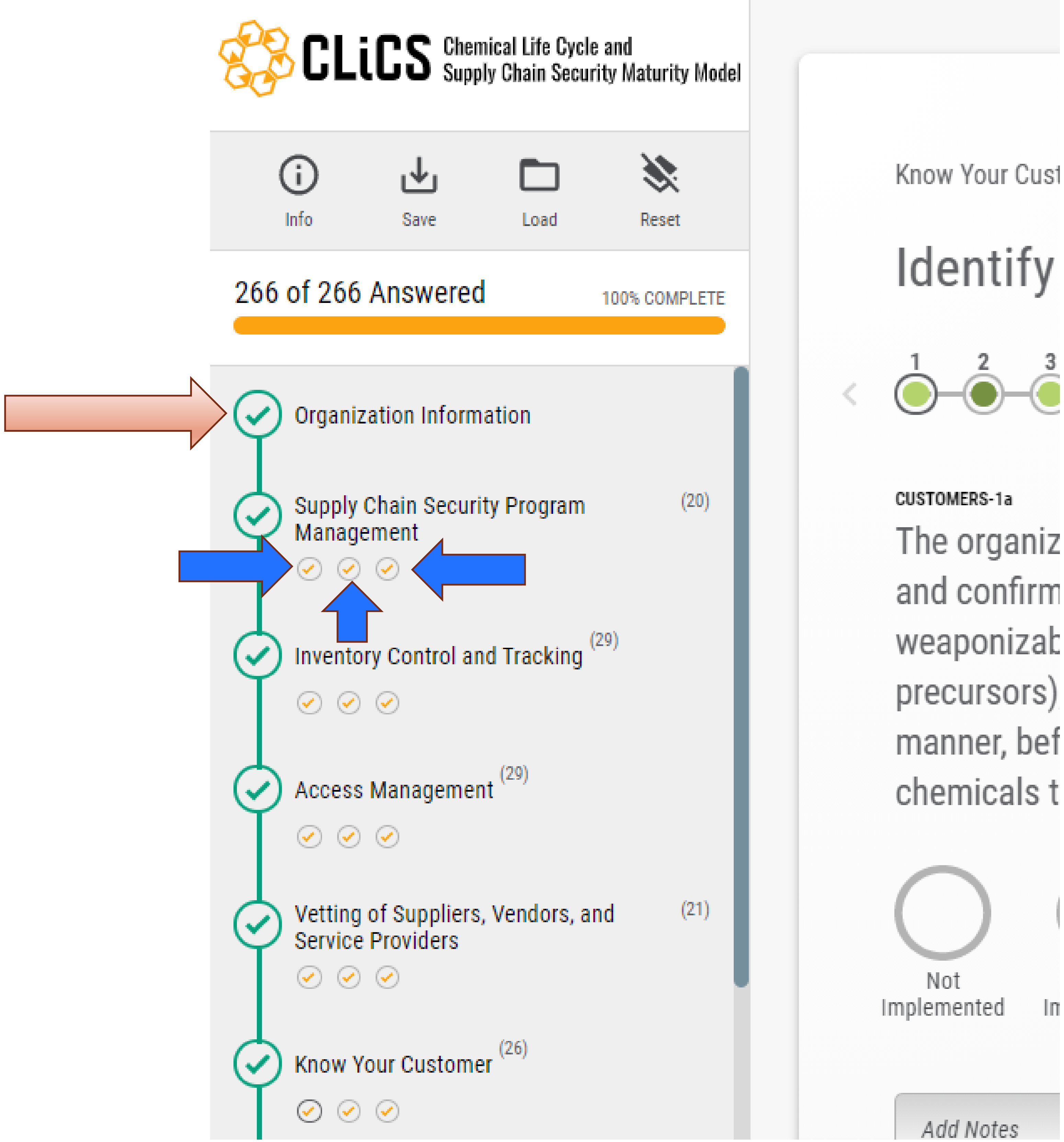
The organization identifies its customers and confirms their need for hazardous or weaponizable chemicals (this includes precursors), in at least in an ad hoc manner, before delivering those chemicals to the customer.

○ Not Implemented ○ Partially Implemented ● Largely Implemented ○ Fully Implemented

Add Notes



Pacific Northwest
NATIONAL LABORATORY



CLiCS Chemical Life Cycle and Supply Chain Security Maturity Model

266 of 266 Answered 100% COMPLETE

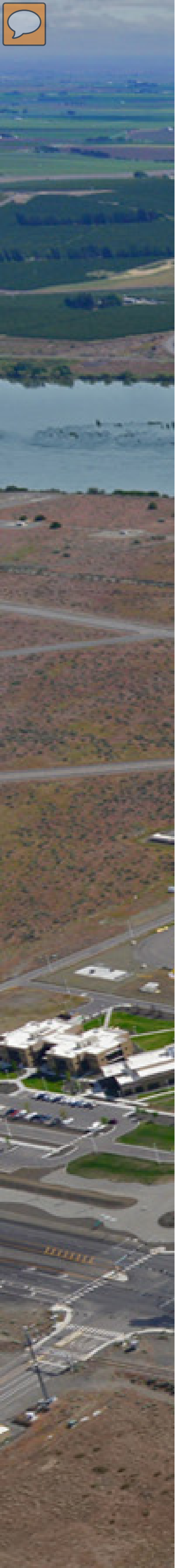
- Organization Information
- Supply Chain Security Program Management (20)
- Inventory Control and Tracking (29)
- Access Management (29)
- Vetting of Suppliers, Vendors, and Service Providers (21)
- Know Your Customer (26)

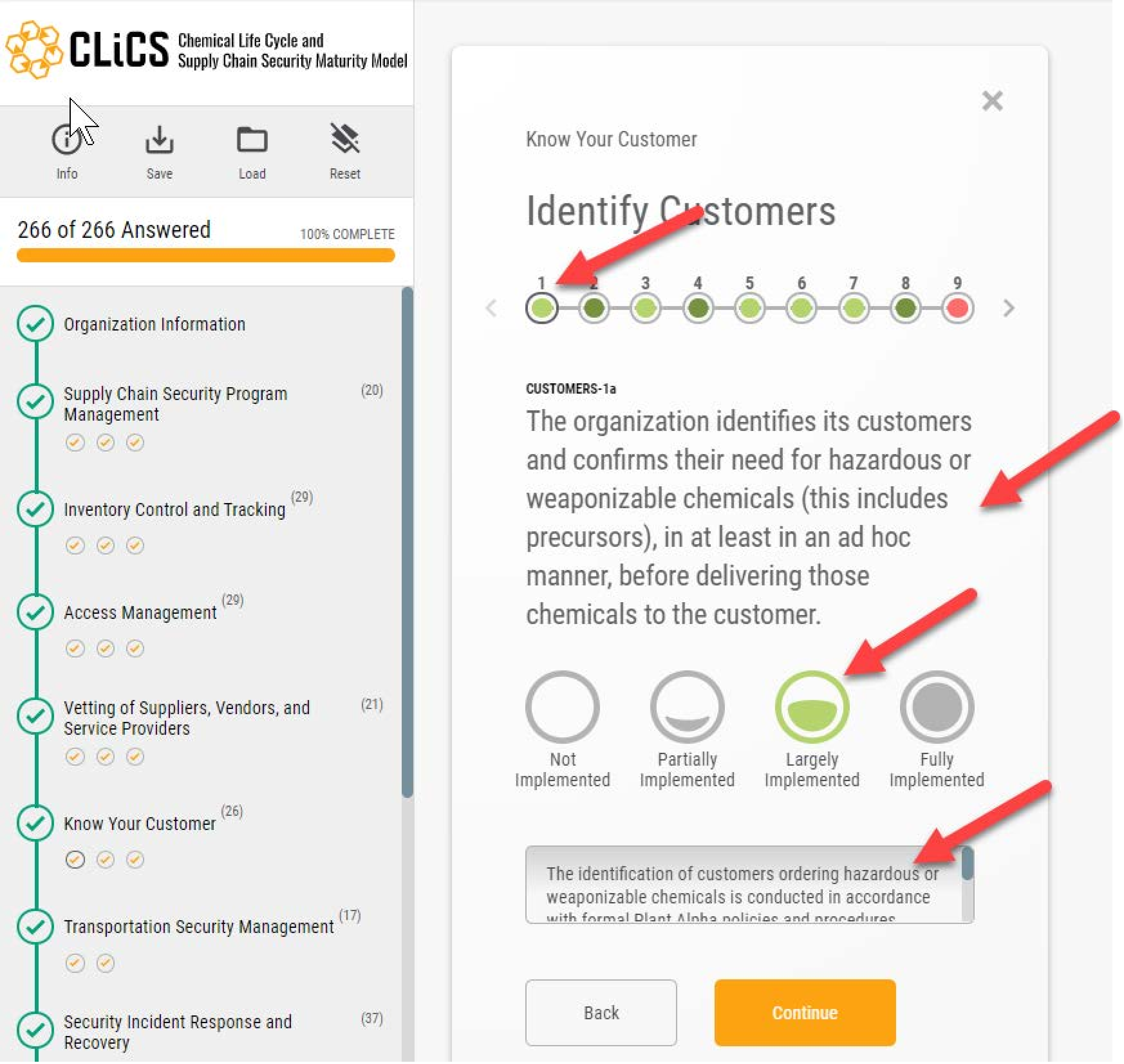
Know Your Cust

Identify

CUSTOMERS-1a

The organiz
and confirm
weaponizat
precursors)
manner, bef
chemicals t





CLiCS Chemical Life Cycle and Supply Chain Security Maturity Model
Info
Save
Load
Reset
266 of 266 Answered
100% COMPLETE
Organization Information
Supply Chain Security Program Management (20)
Inventory Control and Tracking (29)
Access Management (29)
Vetting of Suppliers, Vendors, and Service Providers (21)
Know Your Customer (26)
Transportation Security Management (17)
Security Incident Response and Recovery (37)
1
2
3
4
5
6
7
8
9
Back
Continue

Know Your Customer

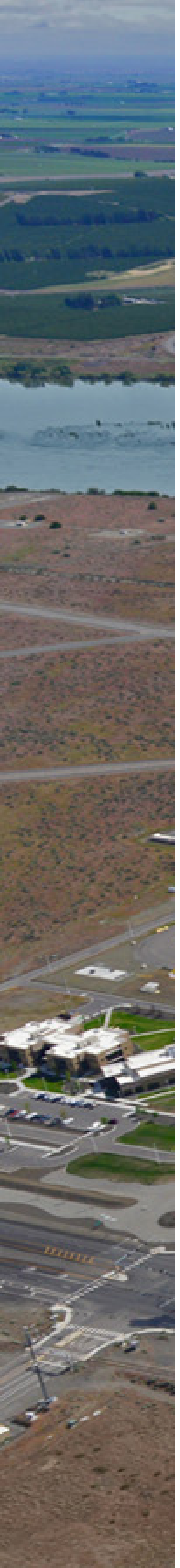
Identify Customers

CUSTOMERS-1a

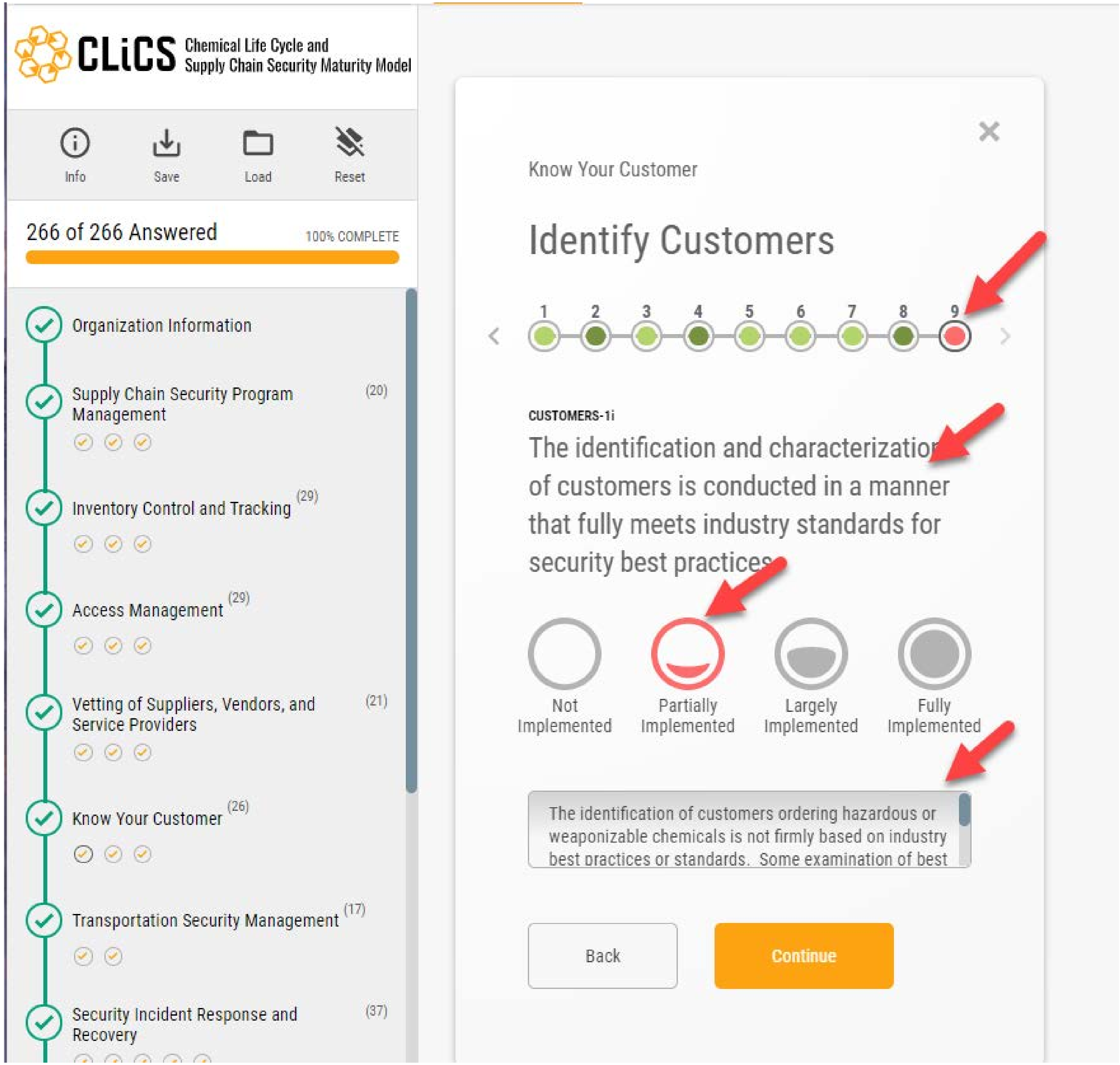
The organization identifies its customers and confirms their need for hazardous or weaponizable chemicals (this includes precursors), in at least in an ad hoc manner, before delivering those chemicals to the customer.

○ Not Implemented ○ Partially Implemented ● Largely Implemented ○ Fully Implemented

The identification of customers ordering hazardous or weaponizable chemicals is conducted in accordance with formal Plant Alpha policies and procedures



Pacific Northwest
NATIONAL LABORATORY



CLiCS Chemical Life Cycle and Supply Chain Security Maturity Model
Info
Save
Load
Reset

266 of 266 Answered
100% COMPLETE

- Organization Information
- Supply Chain Security Program Management (20)
- Inventory Control and Tracking (29)
- Access Management (29)
- Vetting of Suppliers, Vendors, and Service Providers (21)
- Know Your Customer (26)
- Transportation Security Management (17)
- Security Incident Response and Recovery (37)

Know Your Customer

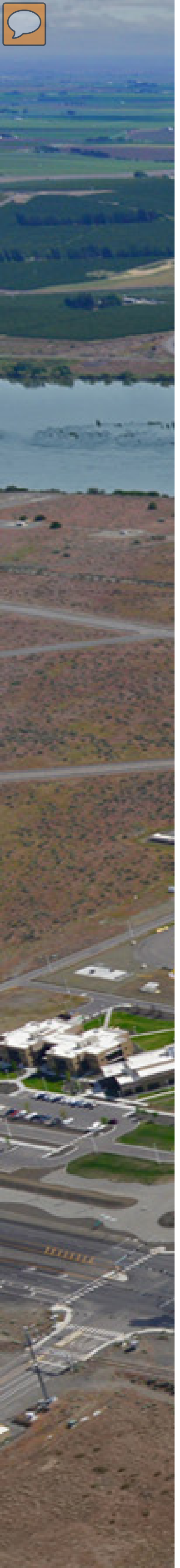
Identify Customers

CUSTOMERS-1i

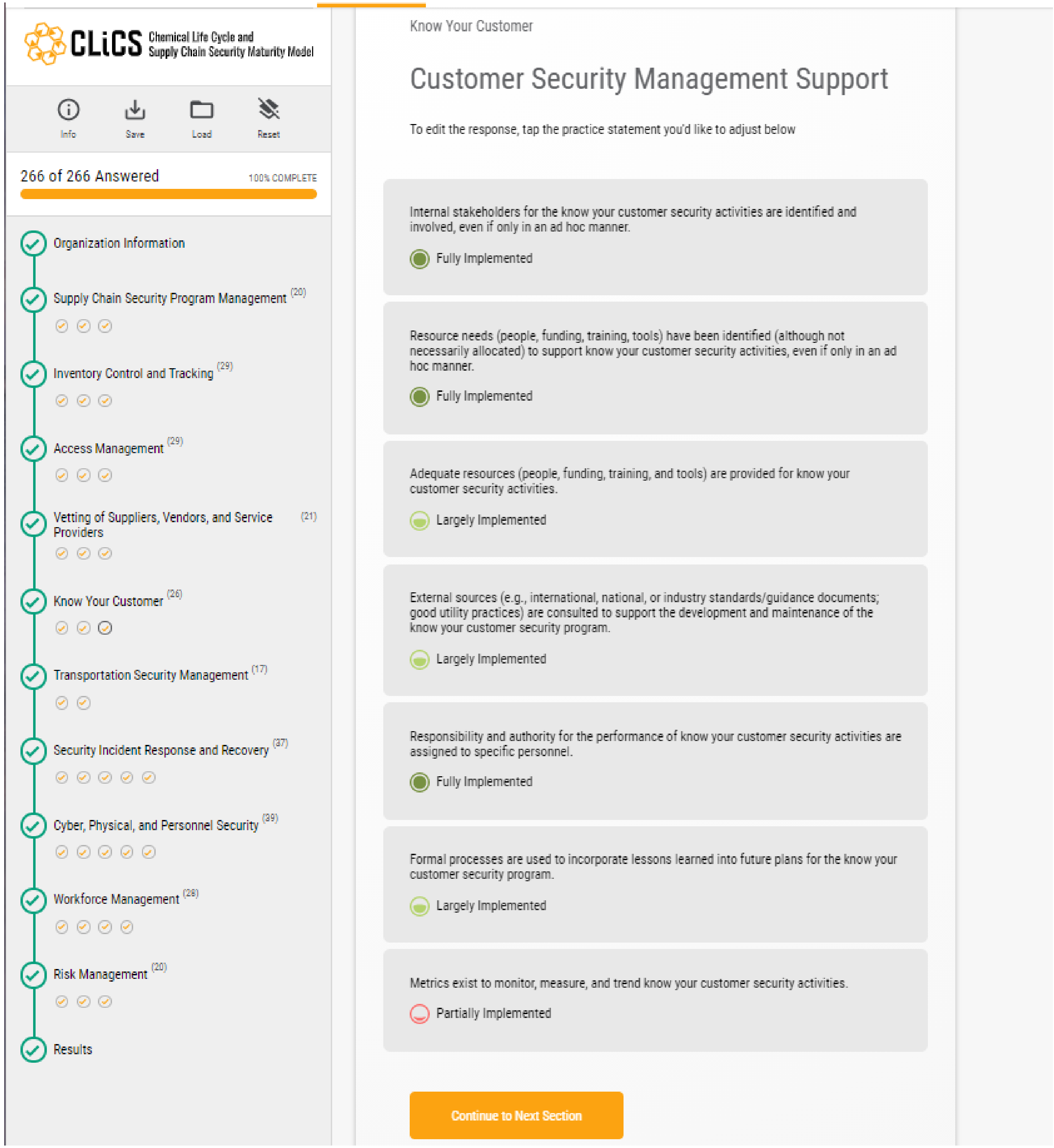
The identification and characterization of customers is conducted in a manner that fully meets industry standards for security best practices

○ Not Implemented
● Partially Implemented
○ Largely Implemented
○ Fully Implemented

The identification of customers ordering hazardous or weaponizable chemicals is not firmly based on industry best practices or standards. Some examination of best



Pacific Northwest
NATIONAL LABORATORY



CLiCS Chemical Life Cycle and Supply Chain Security Maturity Model
Info
Save
Load
Reset
266 of 266 Answered
100% COMPLETE
Organization Information
Supply Chain Security Program Management (20)
Inventory Control and Tracking (29)
Access Management (29)
Vetting of Suppliers, Vendors, and Service Providers (21)
Know Your Customer (26)
Transportation Security Management (17)
Security Incident Response and Recovery (37)
Cyber, Physical, and Personnel Security (39)
Workforce Management (28)
Risk Management (20)
Results

Know Your Customer

Customer Security Management Support

To edit the response, tap the practice statement you'd like to adjust below

Internal stakeholders for the know your customer security activities are identified and involved, even if only in an ad hoc manner.

● Fully Implemented

Resource needs (people, funding, training, tools) have been identified (although not necessarily allocated) to support know your customer security activities, even if only in an ad hoc manner.

● Fully Implemented

Adequate resources (people, funding, training, and tools) are provided for know your customer security activities.

◐ Largely Implemented

External sources (e.g., international, national, or industry standards/guidance documents; good utility practices) are consulted to support the development and maintenance of the know your customer security program.

◐ Largely Implemented

Responsibility and authority for the performance of know your customer security activities are assigned to specific personnel.

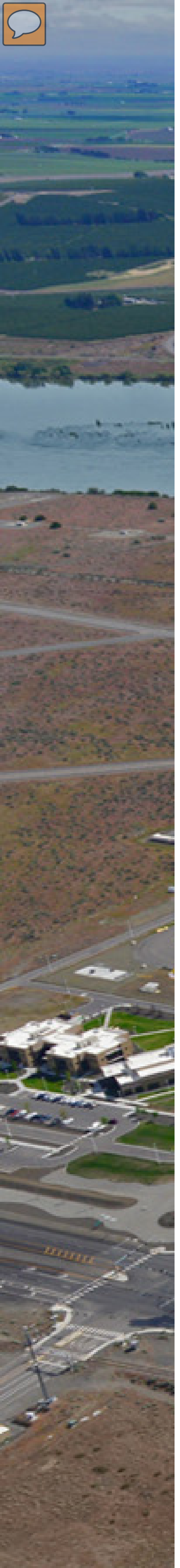
● Fully Implemented

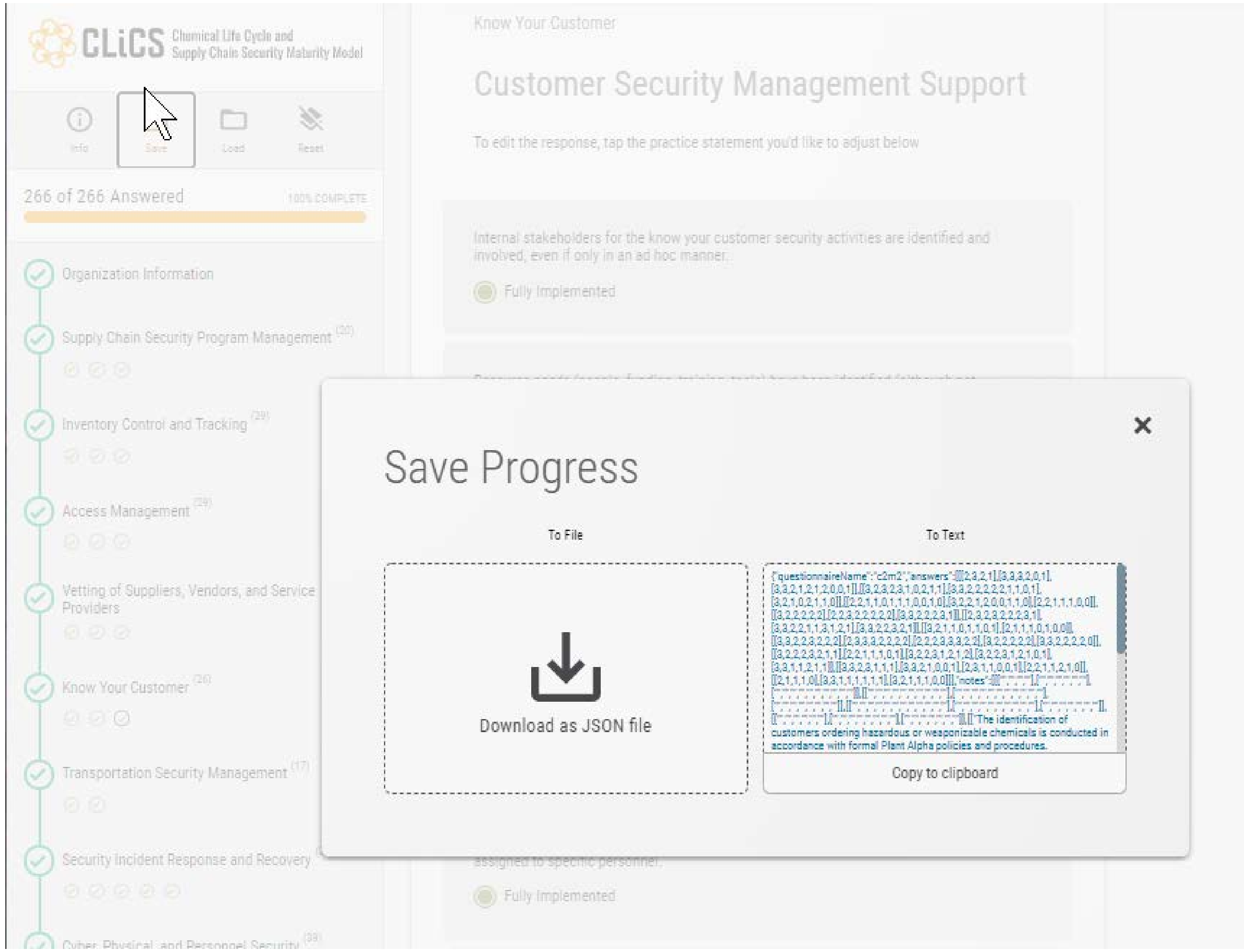
Formal processes are used to incorporate lessons learned into future plans for the know your customer security program.

◐ Largely Implemented

Metrics exist to monitor, measure, and trend know your customer security activities.

○ Partially Implemented





CLiCS Chemical Life Cycle and Supply Chain Security Maturity Model
Info
Save
Load
Reset
266 of 266 Answered
100% COMPLETE
Organization Information
Supply Chain Security Program Management (20)
Inventory Control and Tracking (29)
Access Management (29)
Vetting of Suppliers, Vendors, and Service Providers
Know Your Customer (26)
Transportation Security Management (17)
Security Incident Response and Recovery
Cyber, Physical, and Personnel Security (39)
Know Your Customer

Customer Security Management Support

To edit the response, tap the practice statement you'd like to adjust below

Internal stakeholders for the know your customer security activities are identified and involved, even if only in an ad hoc manner.

Fully Implemented

Save Progress

To File

Download as JSON file

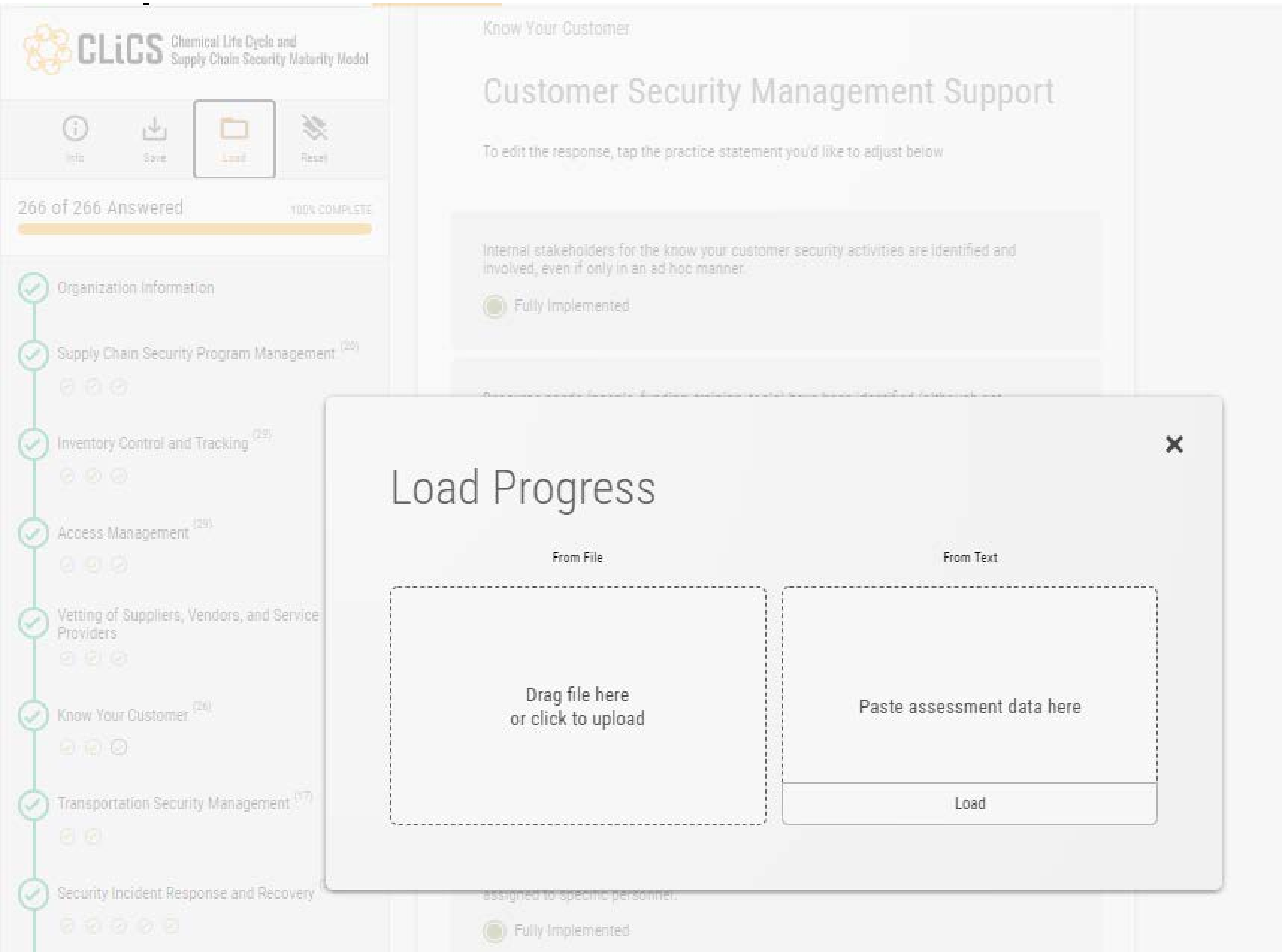
To Text

{"questionnaireName":"c2m2","answers":[[[2,3,2,1],[3,3,3,2,0,1],[3,3,2,1,2,1,2,0,0,1]],[[3,2,3,2,3,1,0,2,1,1],[3,3,2,2,2,2,2,1,1,0,1],[3,2,1,0,2,1,1,0]],[[2,2,1,1,0,1,1,1,0,0,1,0],[3,2,2,1,2,0,0,1,1,0],[2,2,1,1,1,0,0]],[[3,2,2,2,2,2],[2,2,3,2,2,2,2,2],[3,3,2,2,2,3,1]],[[2,3,2,3,2,2,2,3,1],[3,3,2,2,1,1,3,1,2,1],[3,3,2,2,3,2,1]],[[3,2,1,1,0,1,1,0,1],[2,1,1,1,0,1,0,0]],[[3,3,2,2,3,2,2,2],[2,3,3,3,2,2,2,2],[2,2,2,3,3,3,2,2],[3,2,2,2,2,2],[3,3,2,2,2,2,0]],[[3,2,2,2,3,2,1,1],[2,2,1,1,1,0,1]],[3,2,2,3,1,2,1,2],[3,2,2,3,1,2,1,0,1],[3,3,1,1,2,1,1]],[[3,3,2,3,1,1,1],[3,3,2,1,0,0,1],[2,3,1,1,0,0,1],[2,2,1,1,2,1,0]],[[2,1,1,1,0],[3,3,1,1,1,1,1,1],[3,2,1,1,1,0,0]]],"notes":[[["","","",""],["","","","","","",""]],[["","","","","","","","","",""]],[["","","","","","","","","",""],["","","","","","","","","",""]],[["","","","","","","",""],["","","","","","","","","",""],["","","","","","","","","",""],["","","","","","",""]],[["","","","","",""],["","","","","","","",""],["","","","","","","","",""]],["The identification of customers ordering hazardous or weaponizable chemicals is conducted in accordance with formal Plant Alpha policies and procedures.

Copy to clipboard

assigned to specific personnel.

Fully Implemented



CLiCS Chemical Life Cycle and Supply Chain Security Maturity Model
Info
Save
Load
Reset
266 of 266 Answered
100% COMPLETE
Organization Information
Supply Chain Security Program Management (20)
Inventory Control and Tracking (29)
Access Management (29)
Vetting of Suppliers, Vendors, and Service Providers
Know Your Customer (26)
Transportation Security Management (17)
Security Incident Response and Recovery
Know Your Customer

Customer Security Management Support

To edit the response, tap the practice statement you'd like to adjust below

Internal stakeholders for the know your customer security activities are identified and involved, even if only in an ad hoc manner.

Fully Implemented

Load Progress

From File

Drag file here
or click to upload

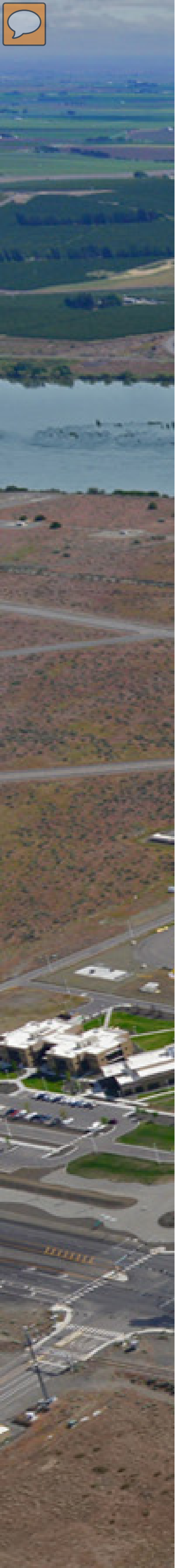
From Text

Paste assessment data here

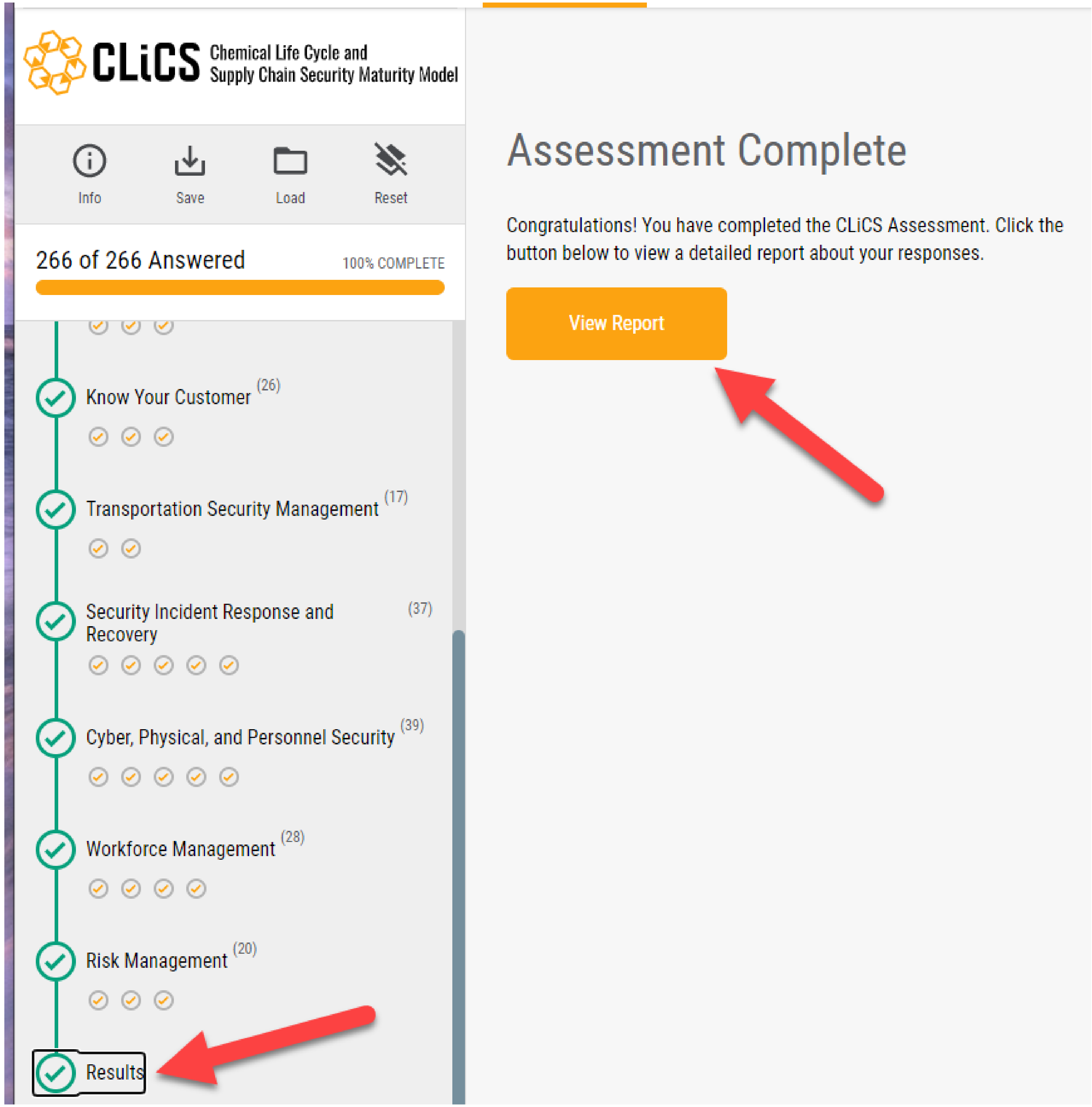
Load

assigned to specific personnel.

Fully Implemented



Pacific Northwest
NATIONAL LABORATORY



CLiCS Chemical Life Cycle and Supply Chain Security Maturity Model

266 of 266 Answered 100% COMPLETE

Know Your Customer (26)

Transportation Security Management (17)

Security Incident Response and Recovery (37)

Cyber, Physical, and Personnel Security (39)

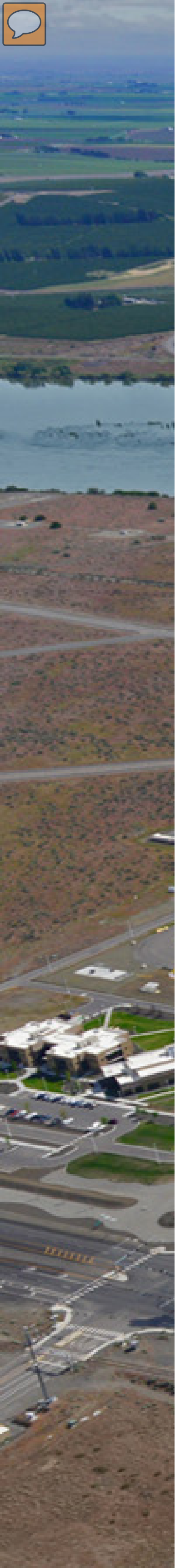
Workforce Management (28)

Risk Management (20)

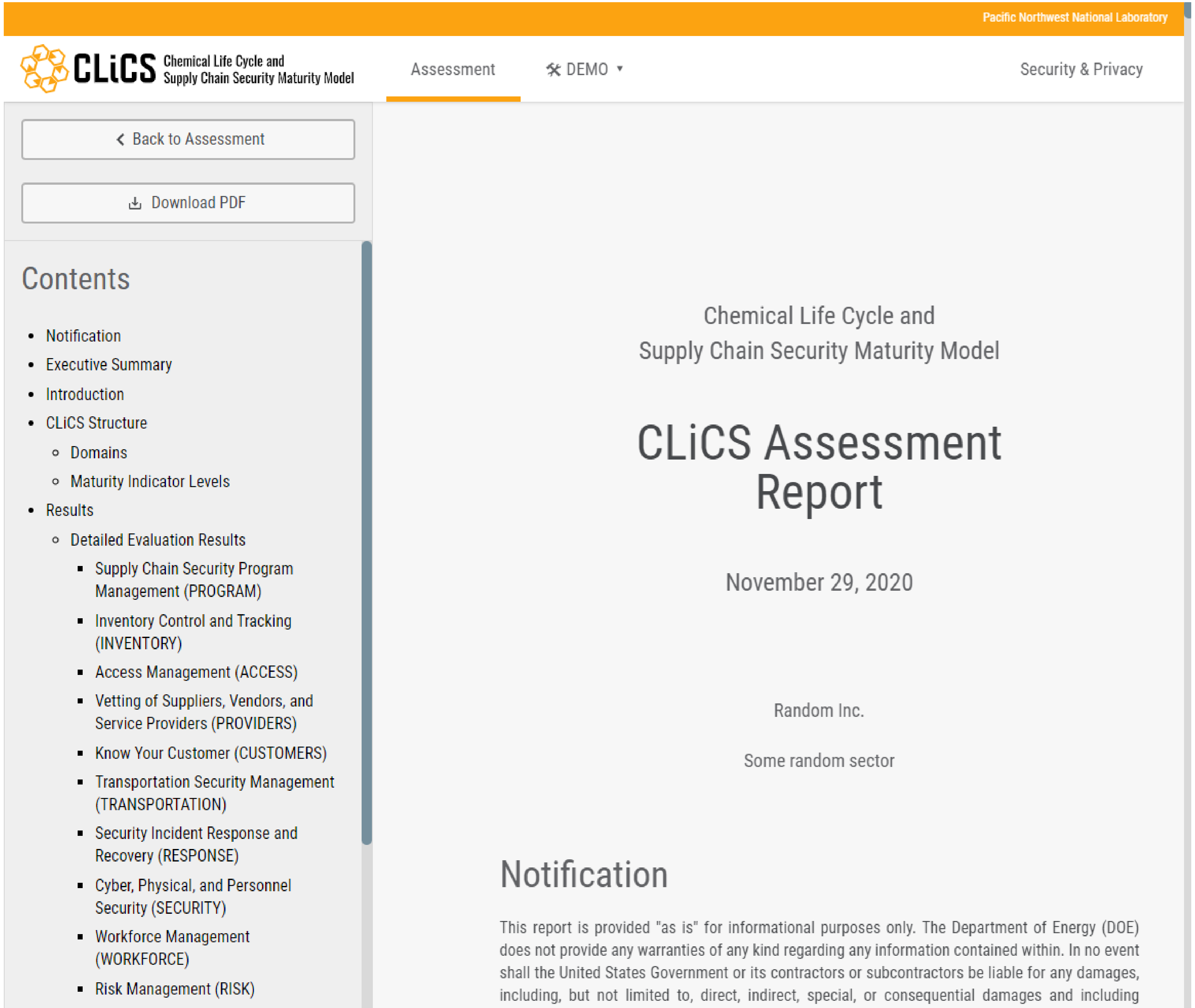
Results

Assessment Complete

Congratulations! You have completed the CLiCS Assessment. Click the button below to view a detailed report about your responses.



Pacific Northwest
NATIONAL LABORATORY



Pacific Northwest National Laboratory
CLiCS Chemical Life Cycle and Supply Chain Security Maturity Model
Assessment
DEMO ▾
Security & Privacy
‹ Back to Assessment
Download PDF

Contents

Chemical Life Cycle and
Supply Chain Security Maturity Model

CLiCS Assessment Report

November 29, 2020

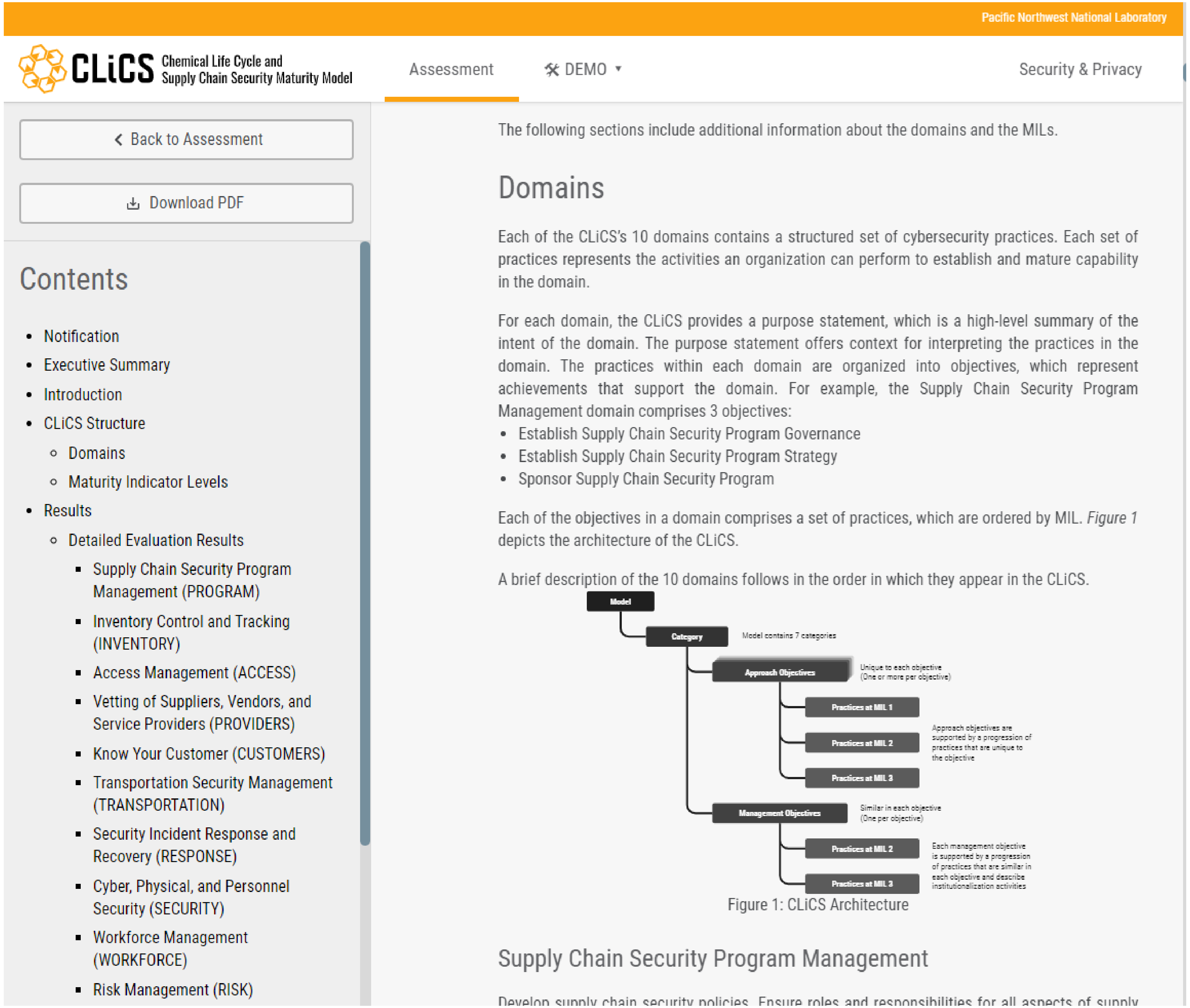
Random Inc.

Some random sector

Notification

This report is provided "as is" for informational purposes only. The Department of Energy (DOE) does not provide any warranties of any kind regarding any information contained within. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including, but not limited to, direct, indirect, special, or consequential damages and including

Pacific Northwest
NATIONAL LABORATORY



Pacific Northwest National Laboratory
CLiCS Chemical Life Cycle and Supply Chain Security Maturity Model
Assessment
DEMO ▾
Security & Privacy
Back to Assessment
Download PDF

Contents

The following sections include additional information about the domains and the MILs.

Domains

Each of the CLiCS's 10 domains contains a structured set of cybersecurity practices. Each set of practices represents the activities an organization can perform to establish and mature capability in the domain.

For each domain, the CLiCS provides a purpose statement, which is a high-level summary of the intent of the domain. The purpose statement offers context for interpreting the practices in the domain. The practices within each domain are organized into objectives, which represent achievements that support the domain. For example, the Supply Chain Security Program Management domain comprises 3 objectives:

- Establish Supply Chain Security Program Governance
- Establish Supply Chain Security Program Strategy
- Sponsor Supply Chain Security Program

Each of the objectives in a domain comprises a set of practices, which are ordered by MIL. *Figure 1* depicts the architecture of the CLiCS.

A brief description of the 10 domains follows in the order in which they appear in the CLiCS.

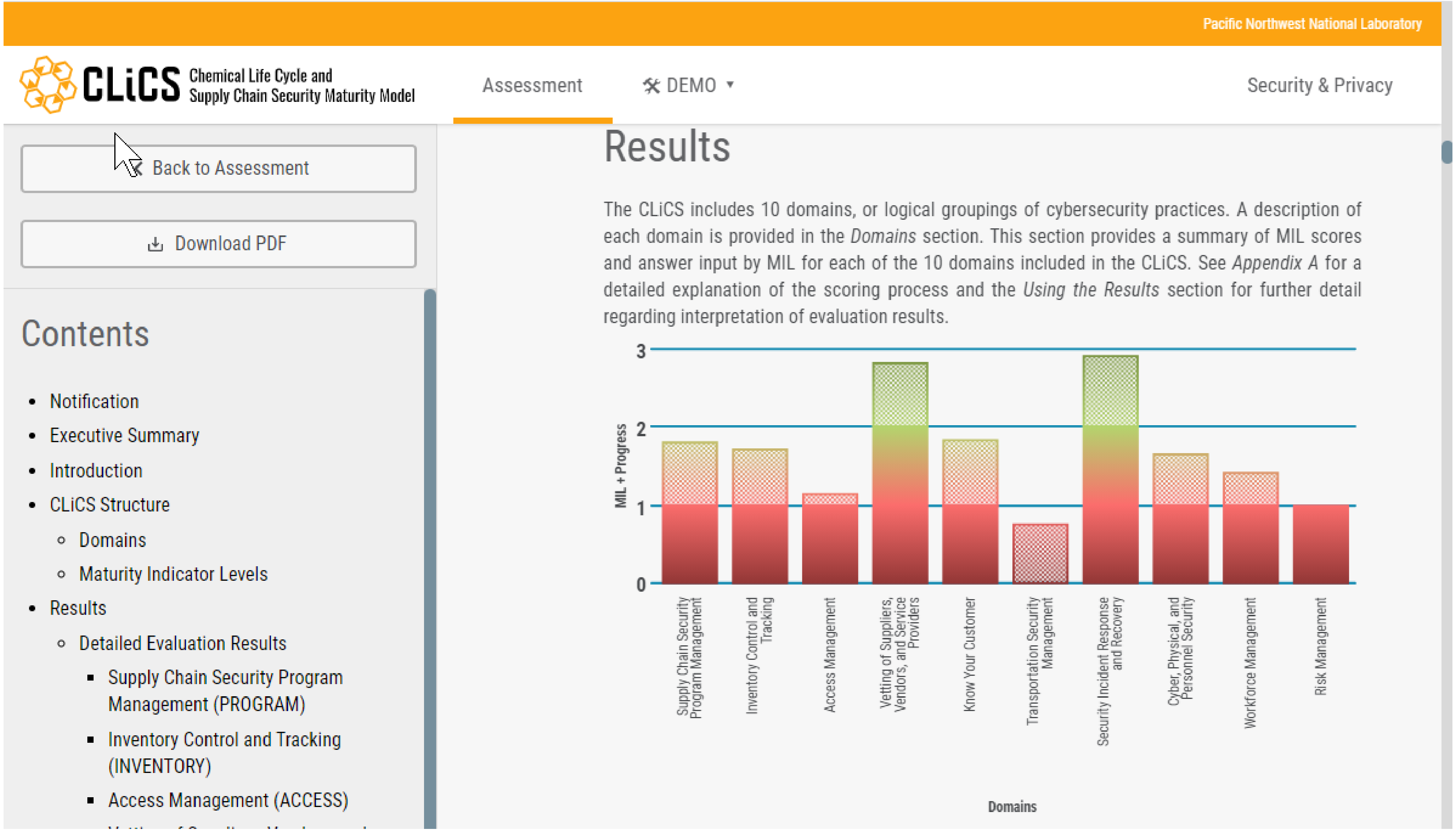
Model
Category
Model contains 7 categories
Approach Objectives
Unique to each objective
(One or more per objective)
Practices at MIL 1
Practices at MIL 2
Practices at MIL 3
Approach objectives are supported by a progression of practices that are unique to the objective
Management Objectives
Similar in each objective
(One per objective)
Practices at MIL 2
Practices at MIL 3
Each management objective is supported by a progression of practices that are similar in each objective and describe institutionalization activities

Figure 1: CLiCS Architecture

Supply Chain Security Program Management

Develop supply chain security policies. Ensure roles and responsibilities for all aspects of supply

Pacific Northwest
NATIONAL LABORATORY



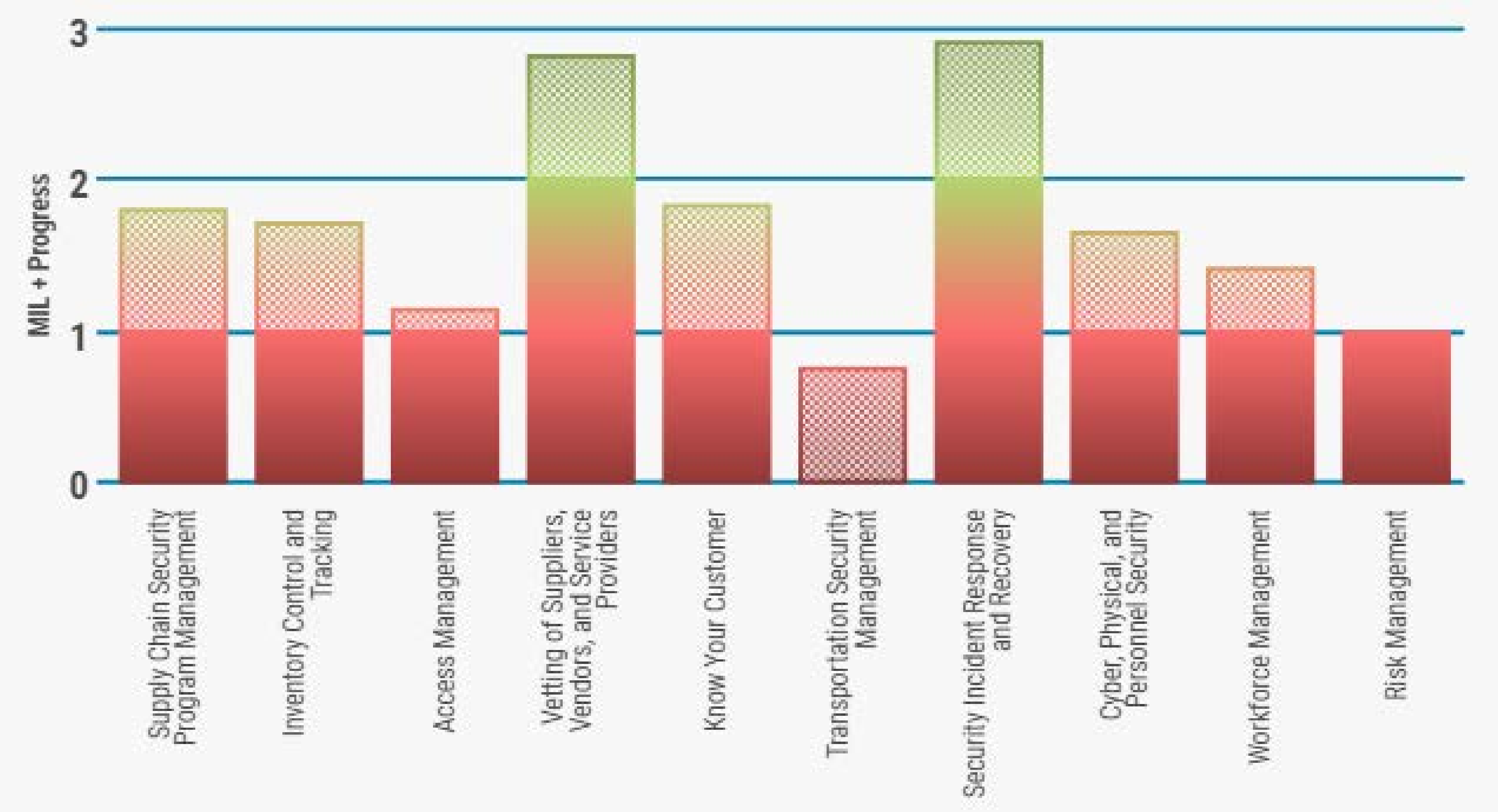
Pacific Northwest National Laboratory
CLiCS Chemical Life Cycle and Supply Chain Security Maturity Model
Assessment
DEMO ▾
Security & Privacy
Back to Assessment
Download PDF

Contents

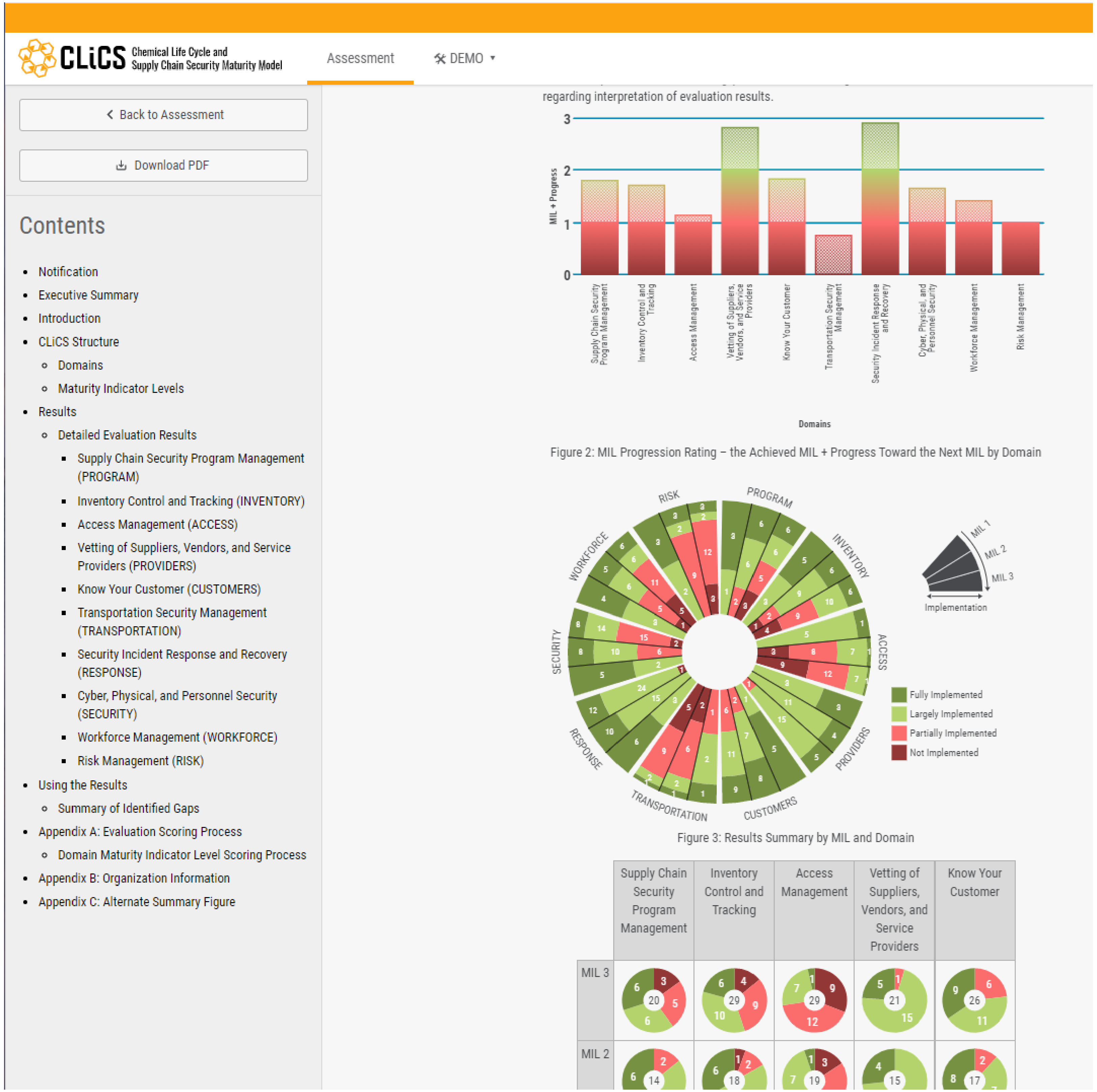
Results

The CLiCS includes 10 domains, or logical groupings of cybersecurity practices. A description of each domain is provided in the *Domains* section. This section provides a summary of MIL scores and answer input by MIL for each of the 10 domains included in the CLiCS. See *Appendix A* for a detailed explanation of the scoring process and the *Using the Results* section for further detail regarding interpretation of evaluation results.

MIL + Progress
0
1
2
3
Supply Chain Security Program Management
Inventory Control and Tracking
Access Management
Vetting of Suppliers, Vendors, and Service Providers
Know Your Customer
Transportation Security Management
Security Incident Response and Recovery
Cyber, Physical, and Personnel Security
Workforce Management
Risk Management
Domains


MIL + Progress
3
2
1
0
Supply Chain Security Program Management
Inventory Control and Tracking
Access Management
Vetting of Suppliers, Vendors, and Service Providers
Know Your Customer
Transportation Security Management
Security Incident Response and Recovery
Cyber, Physical, and Personnel Security
Workforce Management
Risk Management

Pacific Northwest
NATIONAL LABORATORY


CLiCS Chemical Life Cycle and Supply Chain Security Maturity Model
Assessment
DEMO
Back to Assessment
Download PDF

Contents

regarding interpretation of evaluation results.

3
2
1
0
MIL + Progress
Supply Chain Security Program Management
Inventory Control and Tracking
Access Management
Vetting of Suppliers, Vendors, and Service Providers
Know Your Customer
Transportation Security Management
Security Incident Response and Recovery
Cyber, Physical, and Personnel Security
Workforce Management
Risk Management
Domains

Figure 2: MIL Progression Rating – the Achieved MIL + Progress Toward the Next MIL by Domain

Figure 3: Results Summary by MIL and Domain

	Supply Chain Security Program Management	Inventory Control and Tracking	Access Management	Vetting of Suppliers, Vendors, and Service Providers	Know Your Customer
MIL 3					
MIL 2					

Pacific Northwest
NATIONAL LABORATORY

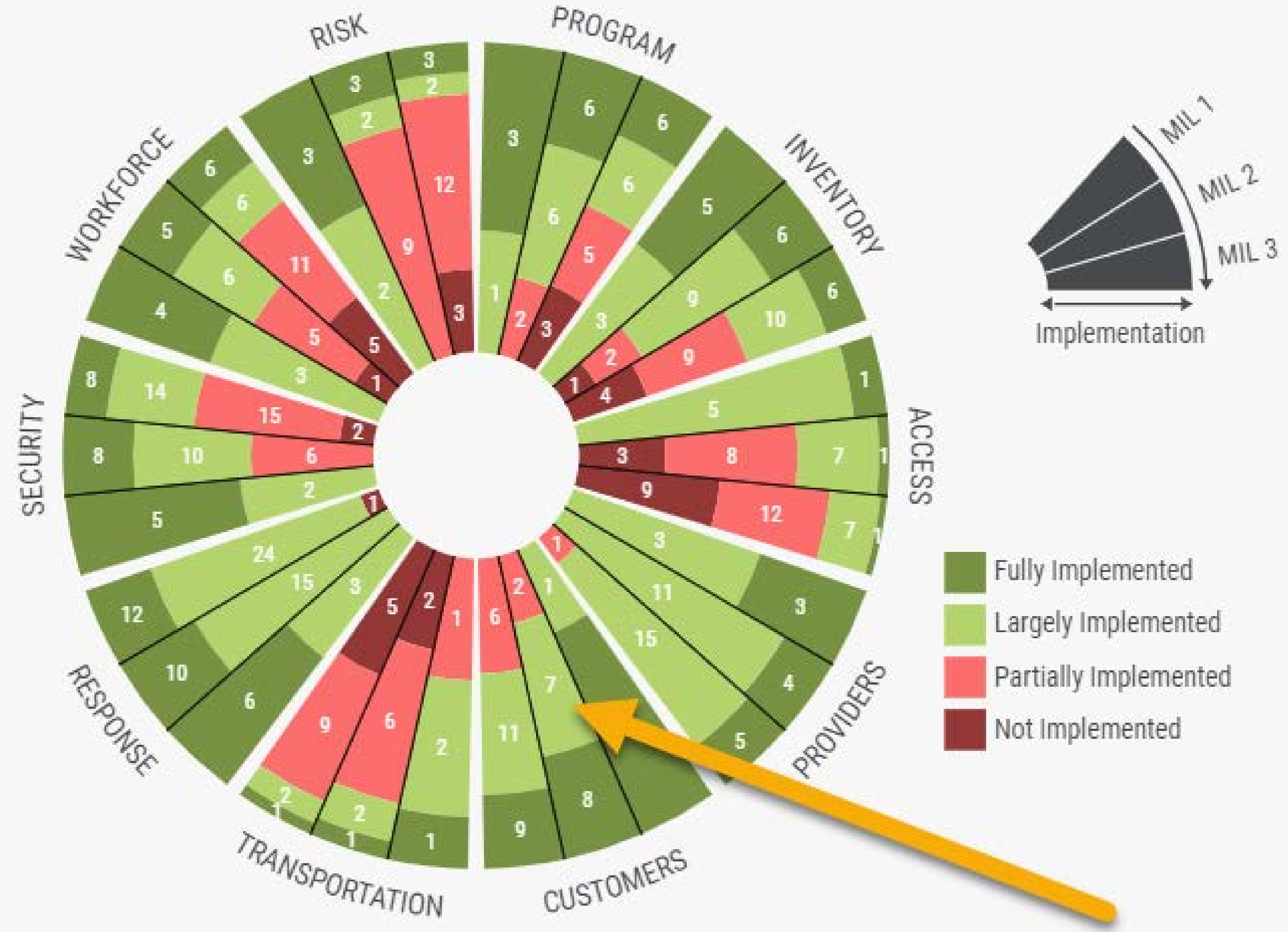
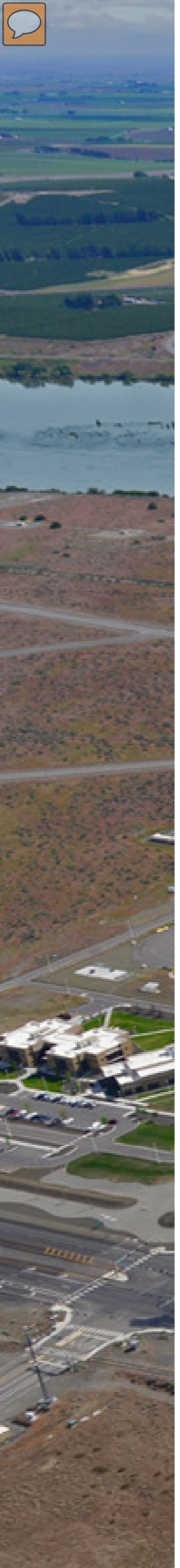
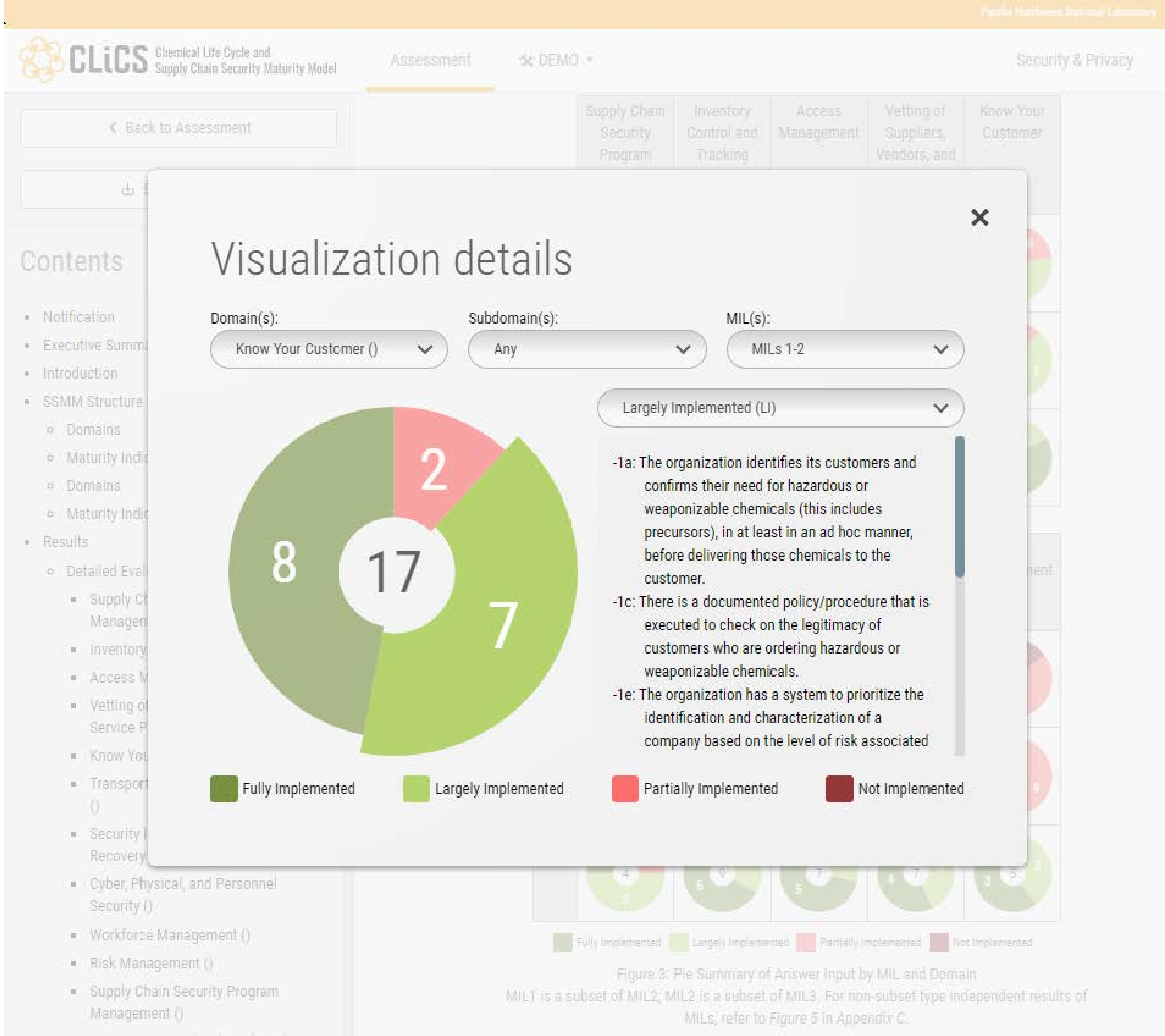


Figure 3: Results Summary by MIL and Domain



Pacific Northwest
NATIONAL LABORATORY


Pacific Northwest National Laboratory
CLiCS Chemical Life Cycle and Supply Chain Security Maturity Model
Assessment
DEMO
Security & Privacy
Back to Assessment
Supply Chain Security Program
Inventory Control and Tracking
Access Management
Vetting of Suppliers, Vendors, and
Know Your Customer
Contents
Notification
Executive Summ
Introduction
SSMM Structure
Domains
Maturity Indi
Domains
Maturity Indi
Results
Detailed Eval
Supply Cl Managem
Inventory
Access M
Vetting of Service P
Know You
Transport ()
Security Recovery
Cyber, Physical, and Personnel Security ()
Workforce Management ()
Risk Management ()
Supply Chain Security Program Management ()
Fully Implemented
Largely Implemented
Partially Implemented
Not Implemented
Figure 3: Pie Summary of Answer Input by MIL and Domain
MIL1 is a subset of MIL2; MIL2 is a subset of MIL3. For non-subset type independent results of MILs, refer to Figure 5 in Appendix C.
×

Visualization details

Domain(s): Know Your Customer ()

Subdomain(s): Any

MIL(s): MILs 1-2

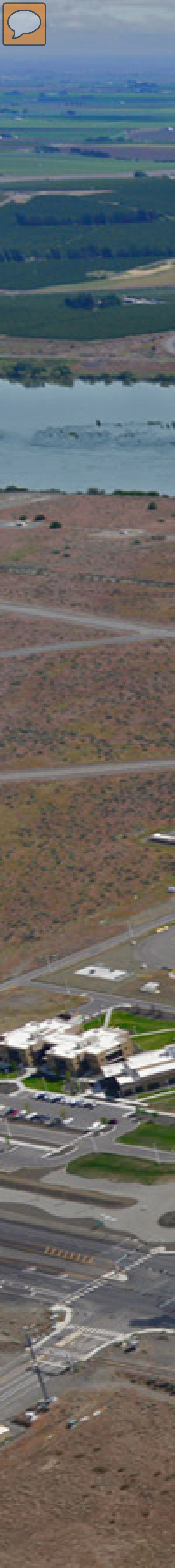
Largely Implemented (LI)

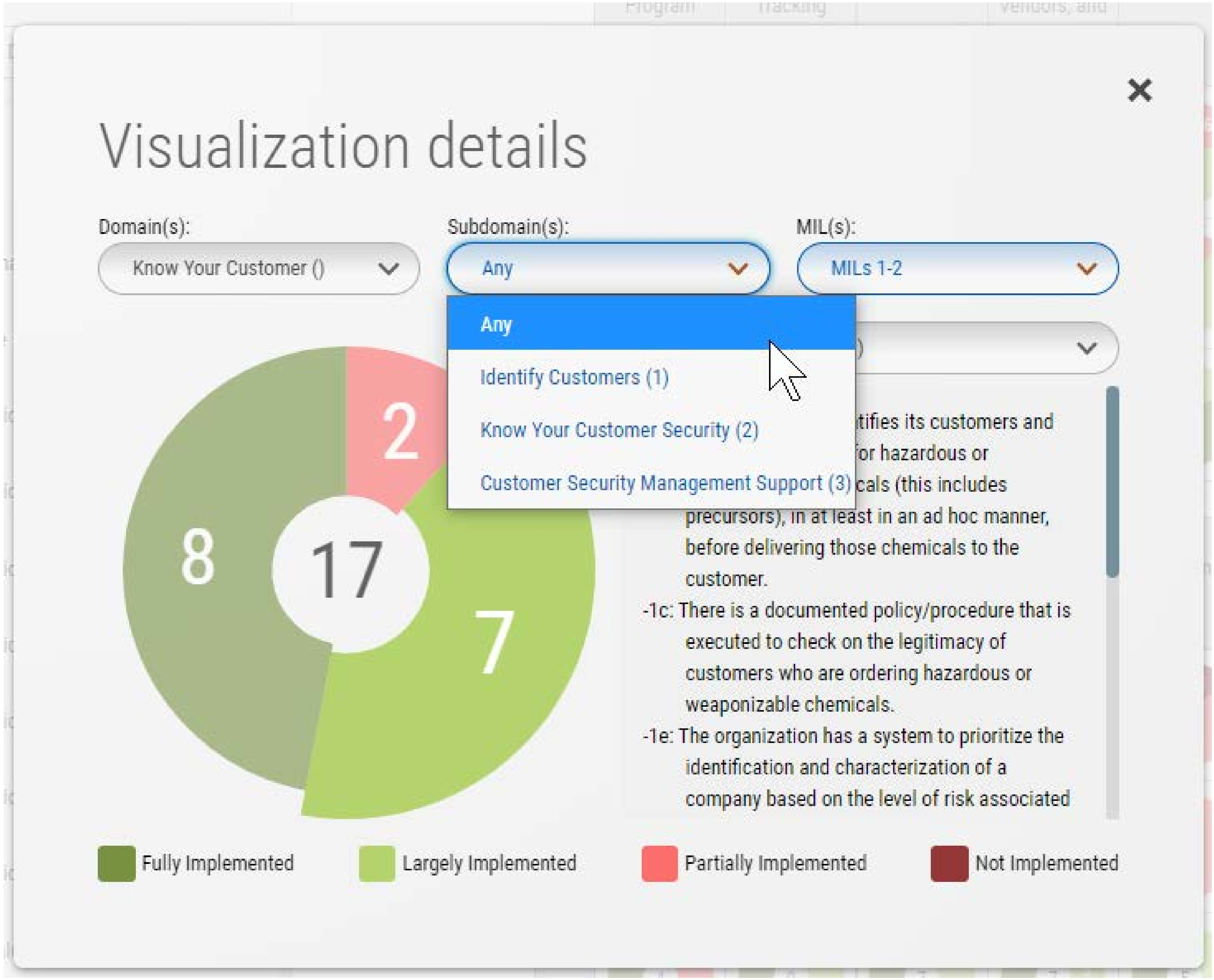
-1a: The organization identifies its customers and confirms their need for hazardous or weaponizable chemicals (this includes precursors), in at least in an ad hoc manner, before delivering those chemicals to the customer.

-1c: There is a documented policy/procedure that is executed to check on the legitimacy of customers who are ordering hazardous or weaponizable chemicals.

-1e: The organization has a system to prioritize the identification and characterization of a company based on the level of risk associated

🟩 Fully Implemented 🟩 Largely Implemented 🟥 Partially Implemented 🟥 Not Implemented





Visualization details

Domain(s): Know Your Customer ()

Subdomain(s): Any

MIL(s): MILs 1-2

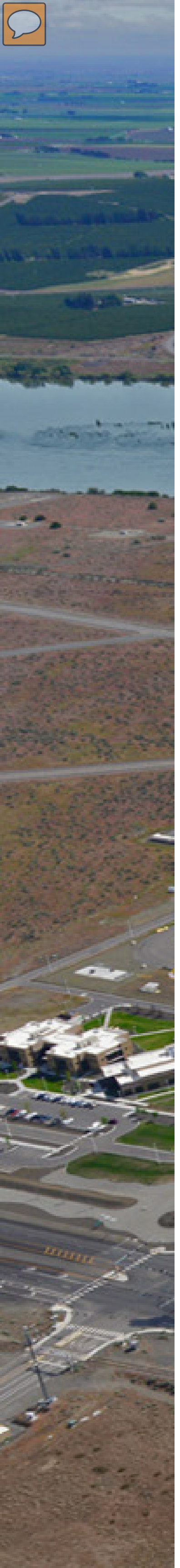
Any
Identify Customers (1)
Know Your Customer Security (2)
Customer Security Management Support (3)
2
8
17
7
✕

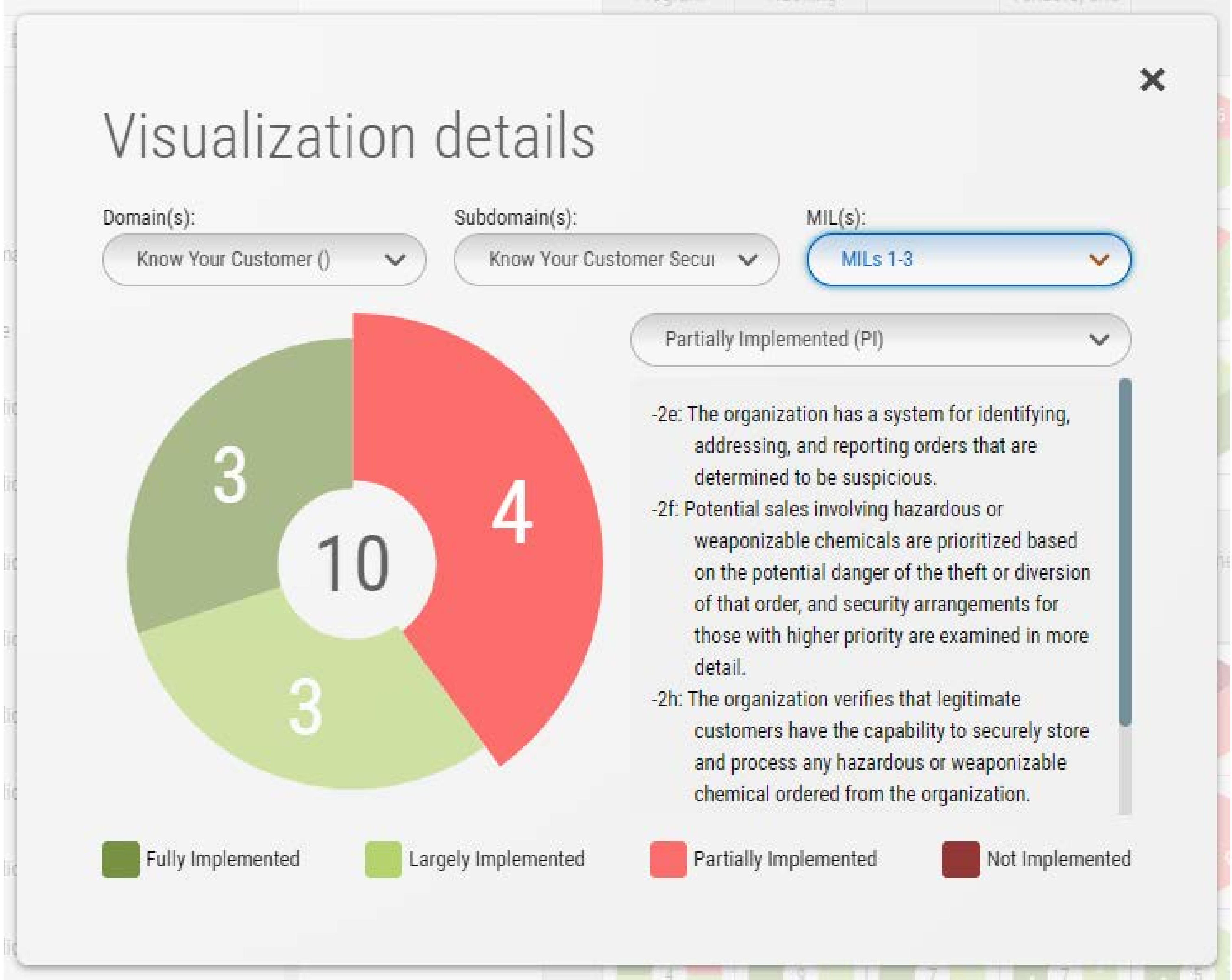
…tifies its customers and …for hazardous or …cals (this includes precursors), in at least in an ad hoc manner, before delivering those chemicals to the customer.

-1c: There is a documented policy/procedure that is executed to check on the legitimacy of customers who are ordering hazardous or weaponizable chemicals.

-1e: The organization has a system to prioritize the identification and characterization of a company based on the level of risk associated

🟩 Fully Implemented 🟩 Largely Implemented 🟥 Partially Implemented 🟥 Not Implemented





Visualization details

Domain(s): Know Your Customer ()

Subdomain(s): Know Your Customer Secui

MIL(s): MILs 1-3

Partially Implemented (PI)

-2e: The organization has a system for identifying, addressing, and reporting orders that are determined to be suspicious.

-2f: Potential sales involving hazardous or weaponizable chemicals are prioritized based on the potential danger of the theft or diversion of that order, and security arrangements for those with higher priority are examined in more detail.

-2h: The organization verifies that legitimate customers have the capability to securely store and process any hazardous or weaponizable chemical ordered from the organization.

🟩 Fully Implemented 🟩 Largely Implemented 🟥 Partially Implemented 🟥 Not Implemented

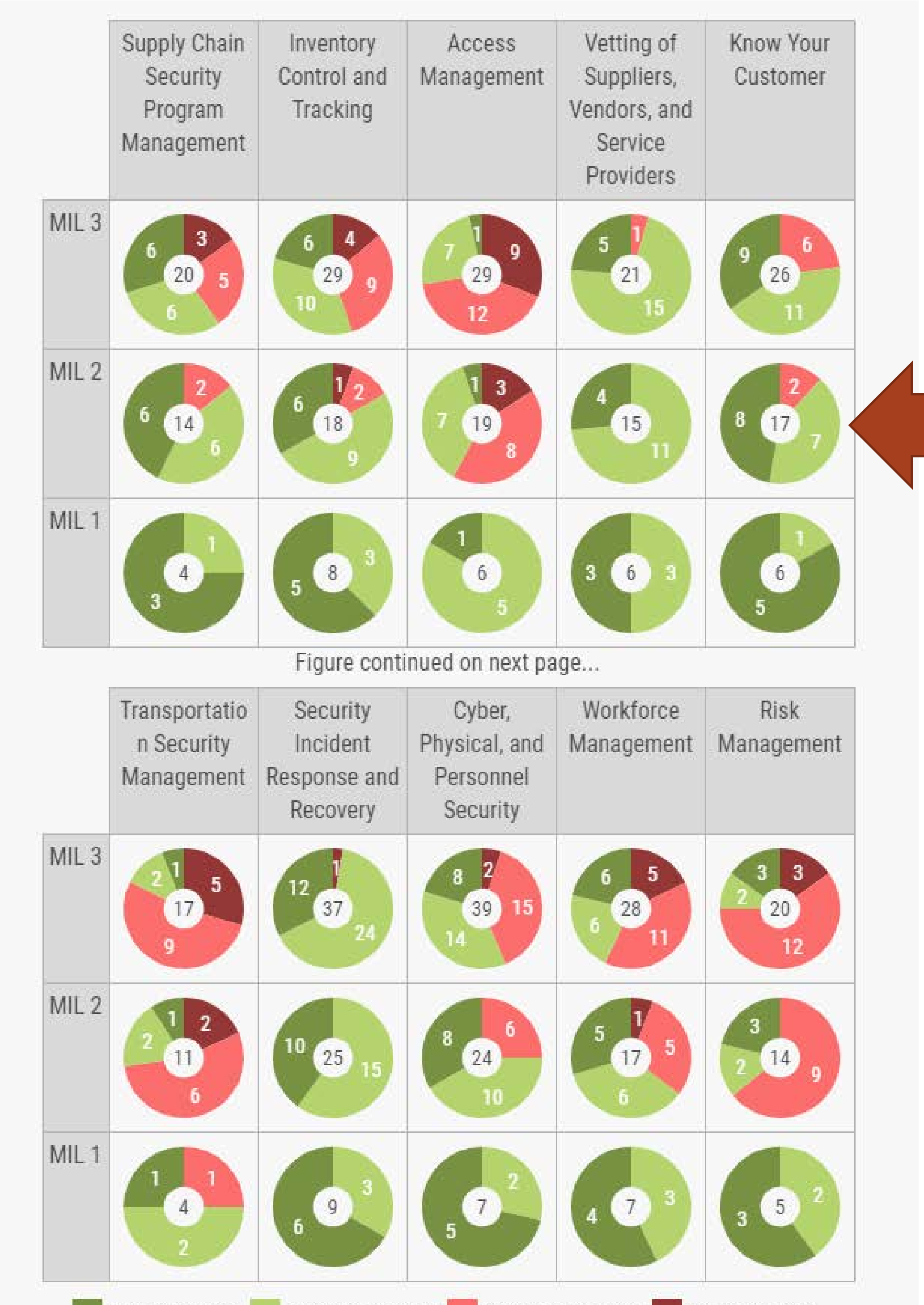
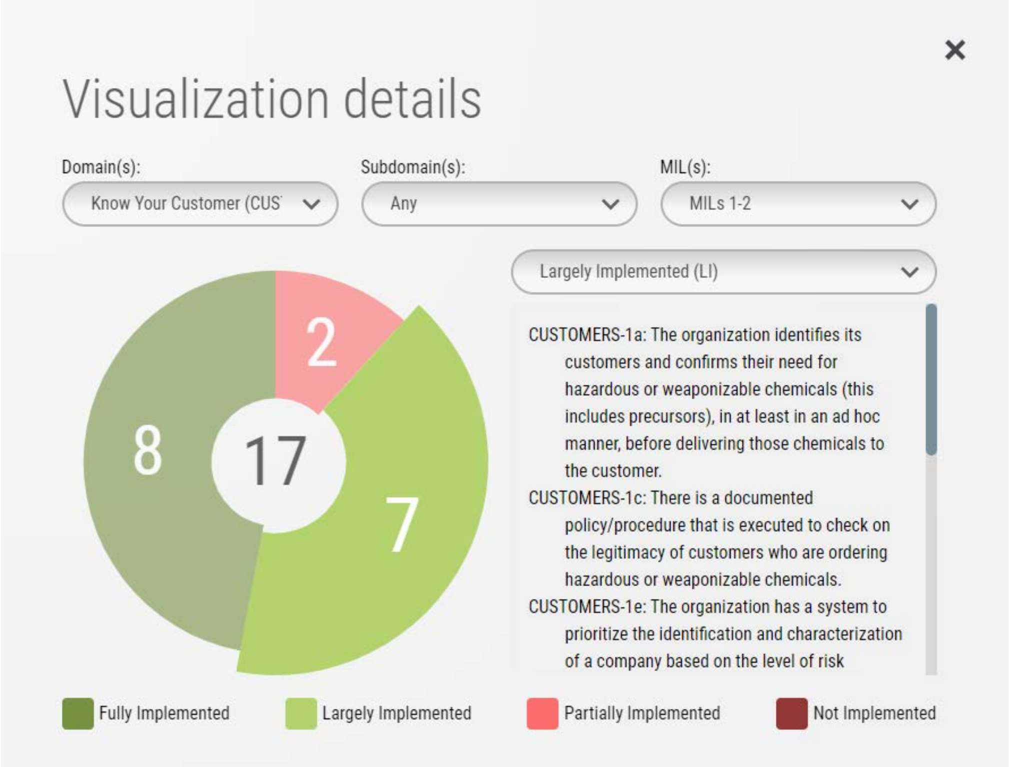


Figure 4: Pie Summary of Answer Input by MIL and Domain

MIL1 is a subset of MIL2; MIL2 is a subset of MIL3. For non-subset type independent results of MILs, refer to *Figure 6* in *Appendix C*.



Visualization details

Domain(s): Know Your Customer (CUS

Subdomain(s): Any

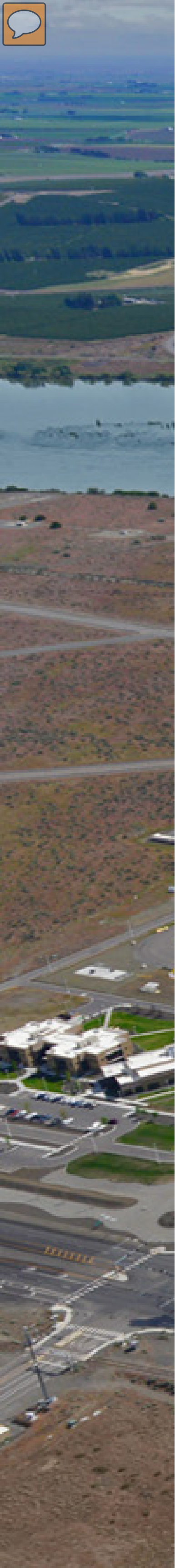
MIL(s): MILs 1-2

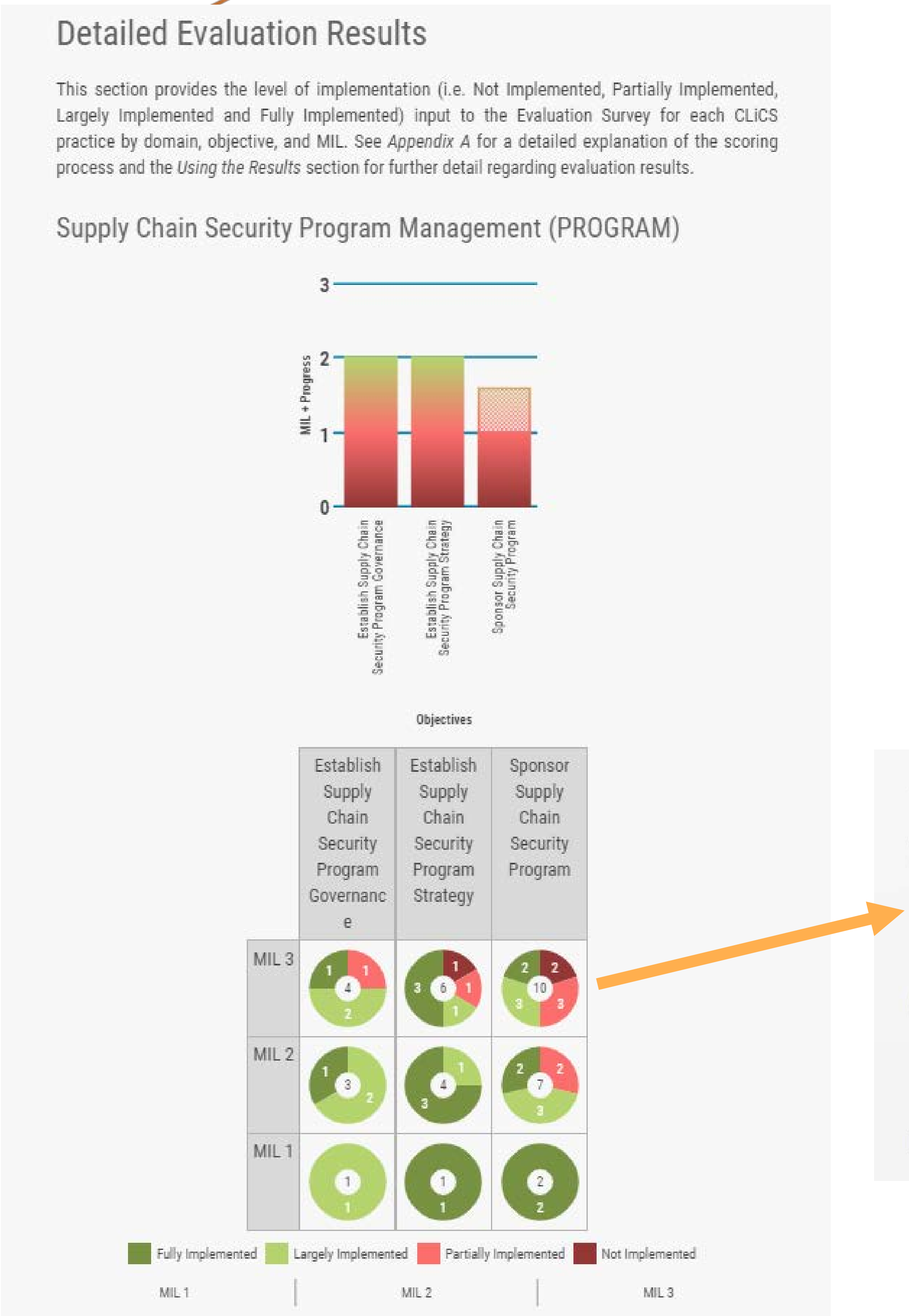
Largely Implemented (LI)

CUSTOMERS-1a: The organization identifies its customers and confirms their need for hazardous or weaponizable chemicals (this includes precursors), in at least in an ad hoc manner, before delivering those chemicals to the customer.

CUSTOMERS-1c: There is a documented policy/procedure that is executed to check on the legitimacy of customers who are ordering hazardous or weaponizable chemicals.

CUSTOMERS-1e: The organization has a system to prioritize the identification and characterization of a company based on the level of risk



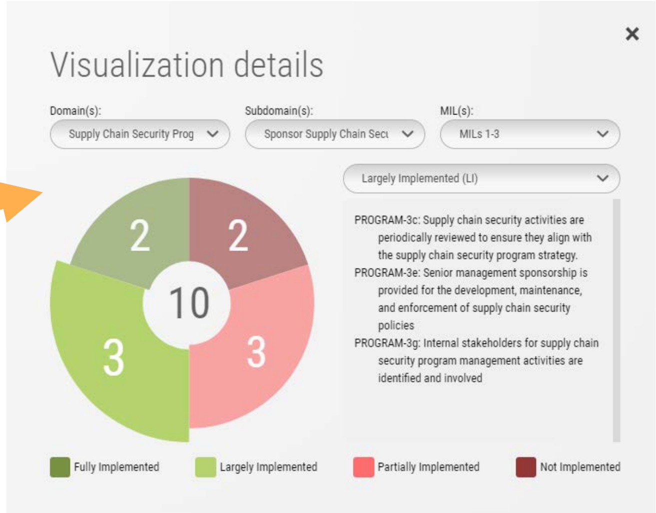


Detailed Evaluation Results

This section provides the level of implementation (i.e. Not Implemented, Partially Implemented, Largely Implemented and Fully Implemented) input to the Evaluation Survey for each CLiCS practice by domain, objective, and MIL. See *Appendix A* for a detailed explanation of the scoring process and the *Using the Results* section for further detail regarding evaluation results.

Supply Chain Security Program Management (PROGRAM)

3
2
1
0
MIL + Progress
Establish Supply Chain Security Program Governance
Establish Supply Chain Security Program Strategy
Sponsor Supply Chain Security Program
Objectives
Establish Supply Chain Security Program Governance
Establish Supply Chain Security Program Strategy
Sponsor Supply Chain Security Program
MIL 3
MIL 2
MIL 1
Fully Implemented
Largely Implemented
Partially Implemented
Not Implemented
MIL 1
MIL 2
MIL 3



Visualization details

Domain(s): Supply Chain Security Prog

Subdomain(s): Sponsor Supply Chain Secu

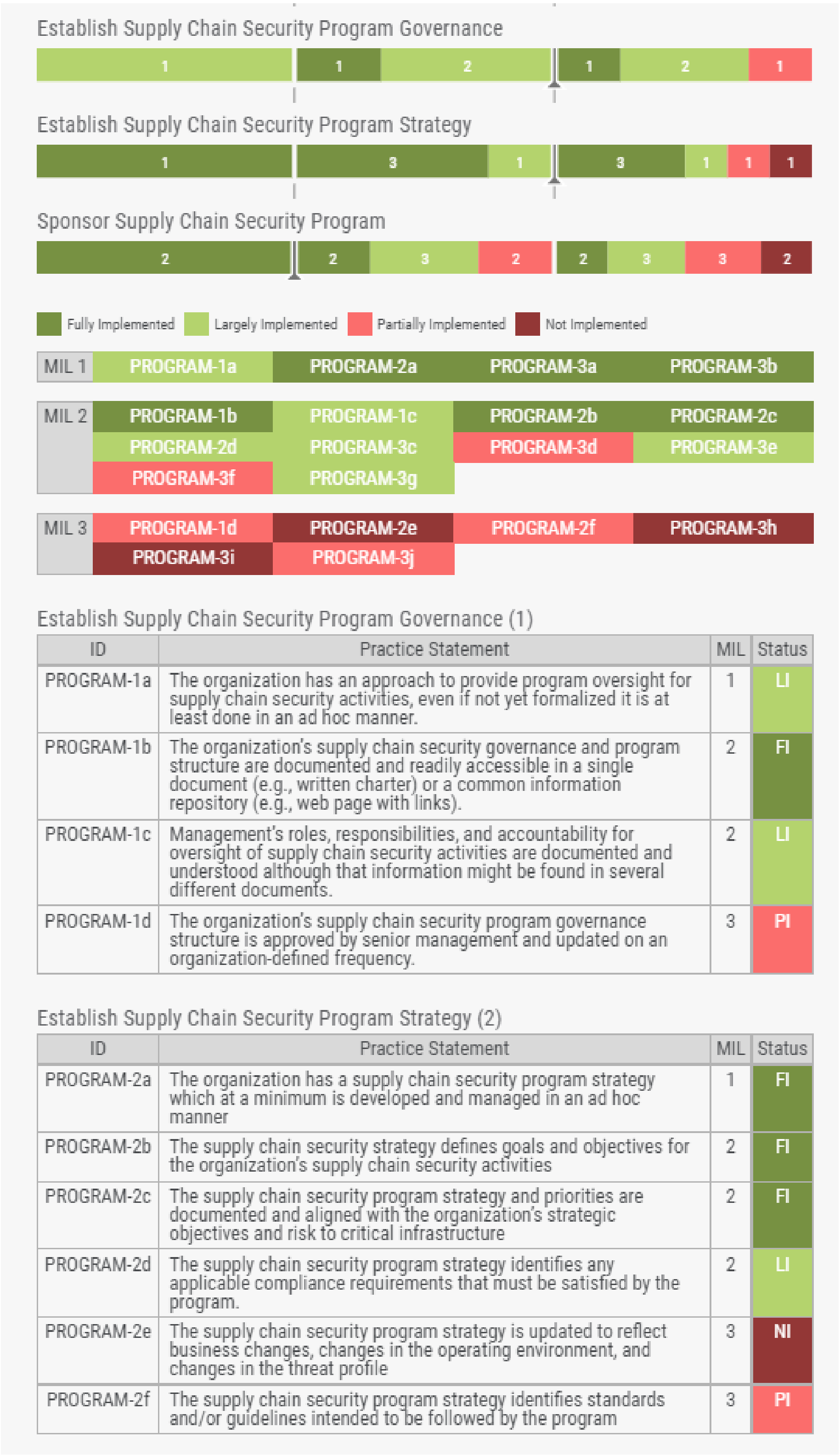
MIL(s): MILs 1-3

Largely Implemented (LI)

PROGRAM-3c: Supply chain security activities are periodically reviewed to ensure they align with the supply chain security program strategy.

PROGRAM-3e: Senior management sponsorship is provided for the development, maintenance, and enforcement of supply chain security policies

PROGRAM-3g: Internal stakeholders for supply chain security program management activities are identified and involved



Establish Supply Chain Security Program Governance
1
1
2
1
2
1
Establish Supply Chain Security Program Strategy
1
3
1
3
1
1
1
Sponsor Supply Chain Security Program
2
2
3
2
2
3
3
2
Fully Implemented
Largely Implemented
Partially Implemented
Not Implemented

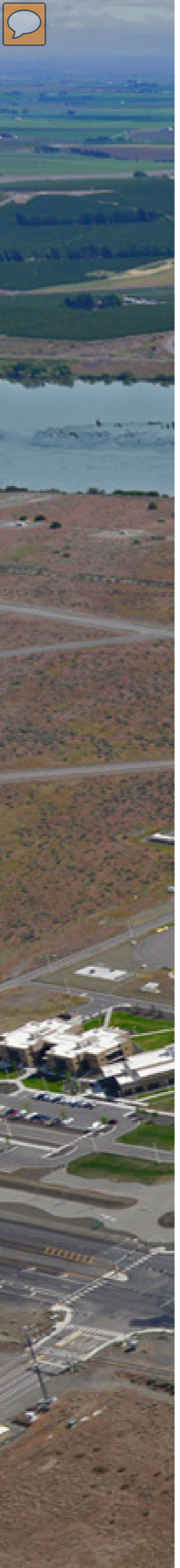
MIL 1	PROGRAM-1a	PROGRAM-2a	PROGRAM-3a	PROGRAM-3b
MIL 2	PROGRAM-1b	PROGRAM-1c	PROGRAM-2b	PROGRAM-2c
	PROGRAM-2d	PROGRAM-3c	PROGRAM-3d	PROGRAM-3e
	PROGRAM-3f	PROGRAM-3g		
MIL 3	PROGRAM-1d	PROGRAM-2e	PROGRAM-2f	PROGRAM-3h
	PROGRAM-3i	PROGRAM-3j		

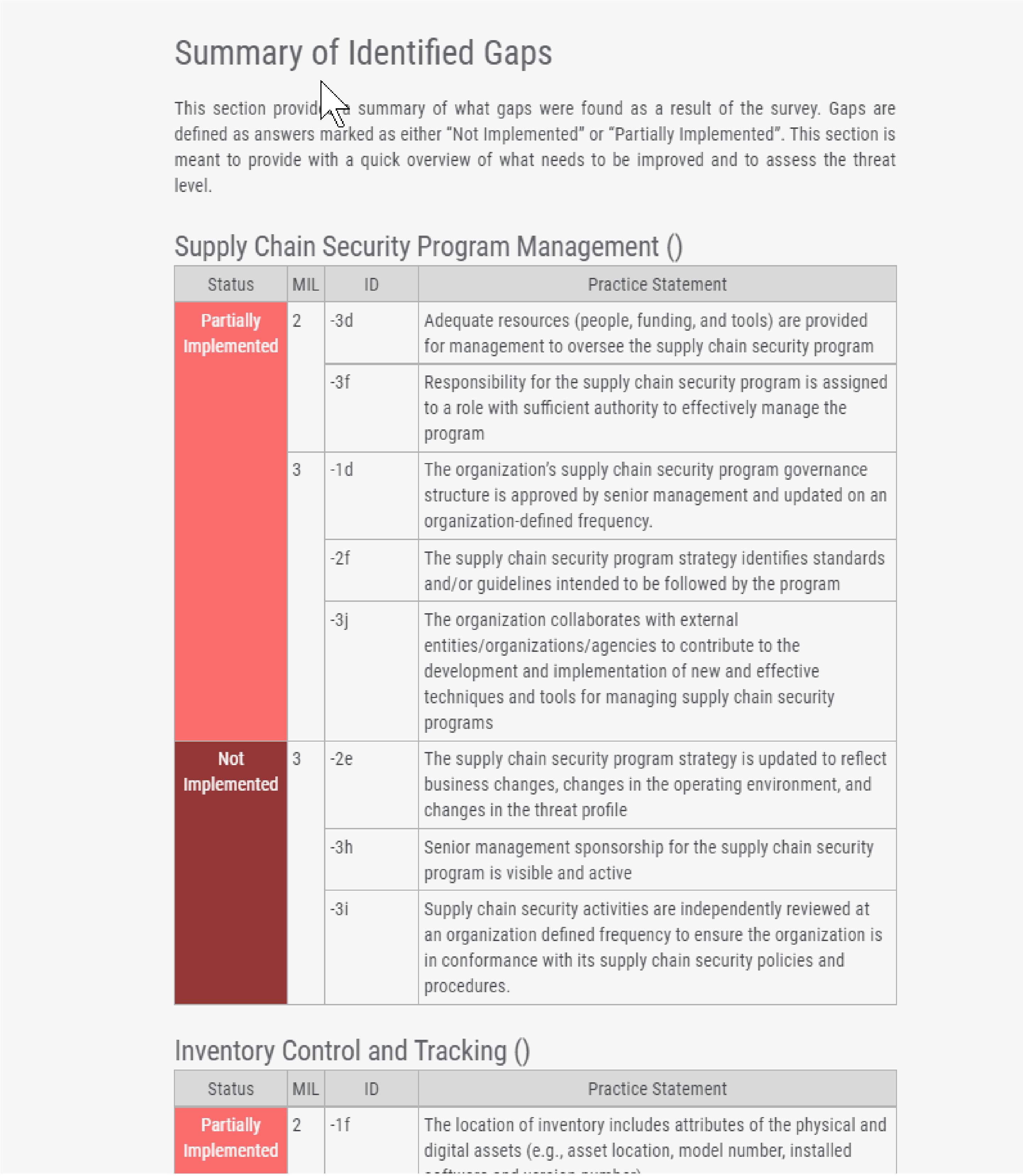
Establish Supply Chain Security Program Governance (1)

ID	Practice Statement	MIL	Status
PROGRAM-1a	The organization has an approach to provide program oversight for supply chain security activities, even if not yet formalized it is at least done in an ad hoc manner.	1	LI
PROGRAM-1b	The organization's supply chain security governance and program structure are documented and readily accessible in a single document (e.g., written charter) or a common information repository (e.g., web page with links).	2	FI
PROGRAM-1c	Management's roles, responsibilities, and accountability for oversight of supply chain security activities are documented and understood although that information might be found in several different documents.	2	LI
PROGRAM-1d	The organization's supply chain security program governance structure is approved by senior management and updated on an organization-defined frequency.	3	PI

Establish Supply Chain Security Program Strategy (2)

ID	Practice Statement	MIL	Status
PROGRAM-2a	The organization has a supply chain security program strategy which at a minimum is developed and managed in an ad hoc manner	1	FI
PROGRAM-2b	The supply chain security strategy defines goals and objectives for the organization's supply chain security activities	2	FI
PROGRAM-2c	The supply chain security program strategy and priorities are documented and aligned with the organization's strategic objectives and risk to critical infrastructure	2	FI
PROGRAM-2d	The supply chain security program strategy identifies any applicable compliance requirements that must be satisfied by the program.	2	LI
PROGRAM-2e	The supply chain security program strategy is updated to reflect business changes, changes in the operating environment, and changes in the threat profile	3	NI
PROGRAM-2f	The supply chain security program strategy identifies standards and/or guidelines intended to be followed by the program	3	PI





Summary of Identified Gaps

This section provides a summary of what gaps were found as a result of the survey. Gaps are defined as answers marked as either "Not Implemented" or "Partially Implemented". This section is meant to provide with a quick overview of what needs to be improved and to assess the threat level.

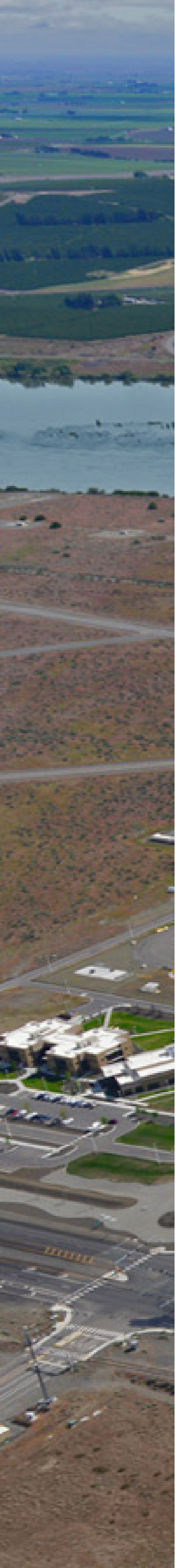
Supply Chain Security Program Management ()

Status	MIL	ID	Practice Statement
Partially Implemented	2	-3d	Adequate resources (people, funding, and tools) are provided for management to oversee the supply chain security program
		-3f	Responsibility for the supply chain security program is assigned to a role with sufficient authority to effectively manage the program
	3	-1d	The organization's supply chain security program governance structure is approved by senior management and updated on an organization-defined frequency.
		-2f	The supply chain security program strategy identifies standards and/or guidelines intended to be followed by the program
		-3j	The organization collaborates with external entities/organizations/agencies to contribute to the development and implementation of new and effective techniques and tools for managing supply chain security programs
Not Implemented	3	-2e	The supply chain security program strategy is updated to reflect business changes, changes in the operating environment, and changes in the threat profile
		-3h	Senior management sponsorship for the supply chain security program is visible and active
		-3i	Supply chain security activities are independently reviewed at an organization defined frequency to ensure the organization is in conformance with its supply chain security policies and procedures.

Inventory Control and Tracking ()

Status	MIL	ID	Practice Statement
Partially Implemented	2	-1f	The location of inventory includes attributes of the physical and digital assets (e.g., asset location, model number, installed software and version number)

Pacific Northwest
NATIONAL LABORATORY

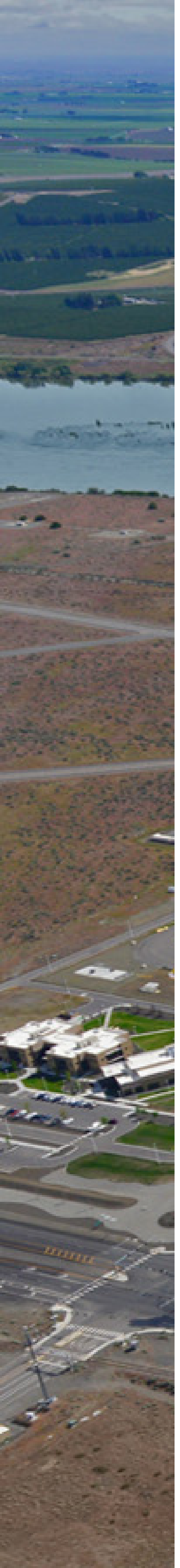


Thank you

Exercise F – Apply the Chemical Life Cycle and Supply Chain Security (CLiCS) Maturity Model

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

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



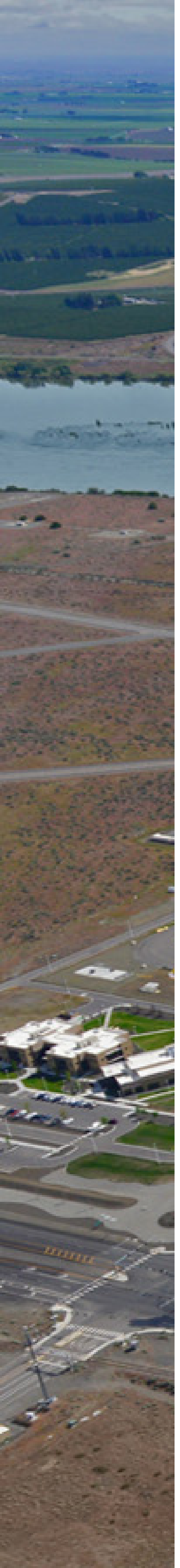
Part 1: Customer Vetting Domain – Identify Customers Objective

You will apply the Chemical Life Cycle and Supply Chain Security Maturity Model to evaluate your facility or an imaginary facility (your choice).

- Security Policies, Roles, and Responsibilities
- Inventory and Information Control and Tracking
- Access Management
- Vetting of Suppliers and Vendors
- **Know Your Customer**
- Transportation Management
- Security Awareness and Incident Response and Reporting
- Cyber, Physical, and Personnel Security
- Workforce Management Risk Management

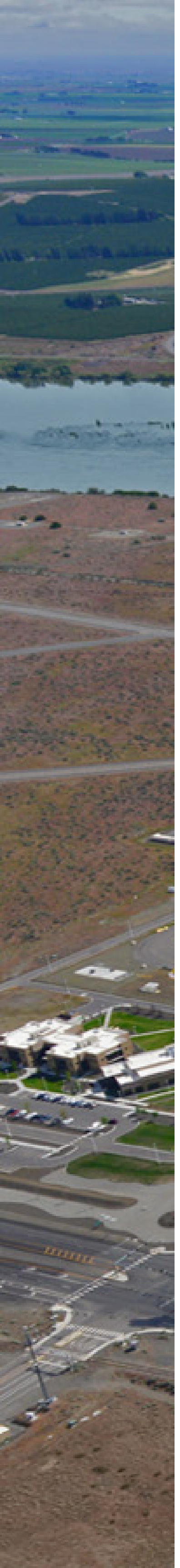
Objectives

1. **Identify Customers**
2. Know Your Customer
3. Management Support



Each Domain Characterized by a Series of Practices.

4-point answer scale	The organization’s performance of the practice described in the model is …
Fully Implemented (FI)	Complete
Largely Implemented (LI)	Complete, but with a recognized opportunity for improvement
Partially Implemented (PI)	Incomplete; there are multiple opportunities for improvement
Not Implemented (NI)	Absent; the practice is not performed in the organization

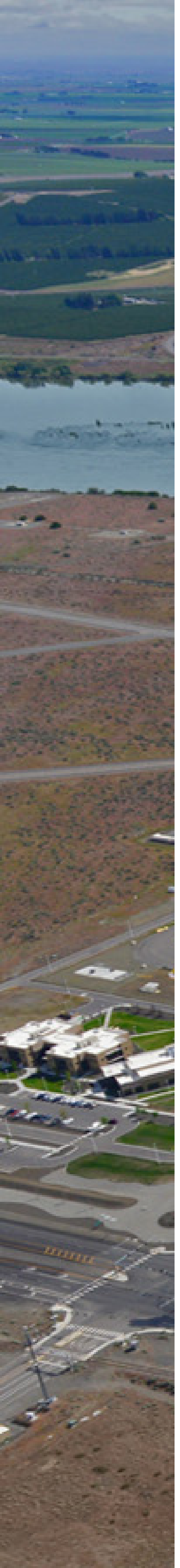


Instructions

- We will examine 10 “Identify Customer” practices one-at-a-time.
- Evaluate each practice for your facility (or an imaginary facility)
- Select one of four implementation scores for each practice:

○	◒	◒	◉
Not Implemented	Partially Implemented	Largely Implemented	Fully Implemented
1	2	3	4

- Provide your answer when each poll question appears on your screen.



Supply Chain and External Dependencies: Manage Dependency Risk

1. The organization identifies its customers and confirms their need for hazardous or weaponizable chemicals, in at least in an ad hoc manner, before delivering those chemicals to the customer.

   ○ Not Implemented ◔ Partially Implemented ◑ Largely Implemented ● Fully Implemented

2. The organization keeps a record of valid delivery addresses, at least in an ad hoc manner, for those companies that are permitted to order hazardous or weaponizable chemicals.

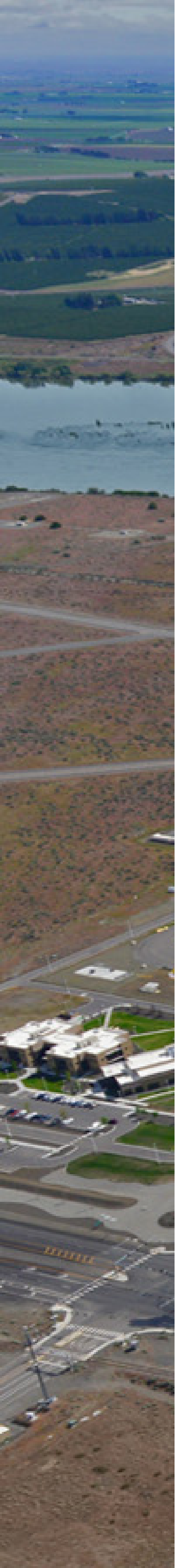
   ○ Not Implemented ◔ Partially Implemented ◑ Largely Implemented ● Fully Implemented

3. There is a document policy or procedure that is executed to check on the legitimacy of customers who are ordering involving hazardous or weaponizable chemicals.

   ○ Not Implemented ◔ Partially Implemented ◑ Largely Implemented ● Fully Implemented

4. The organization documents its compliance with laws and regulations on the identification of customers prior to completing a sale of hazardous and weaponizable chemicals.

   ○ Not Implemented ◔ Partially Implemented ◑ Largely Implemented ● Fully Implemented



Manage Dependency Risk (cont)

5. The organization has a system to prioritize the identification and characterization of a company based on the level of risk associated with that companies order of hazardous or weaponizable chemicals.

○ Not Implemented ◔ Partially Implemented ◑ Largely Implemented ● Fully Implemented

6. The organization has a system for identifying and addresses orders that could be suspicious.

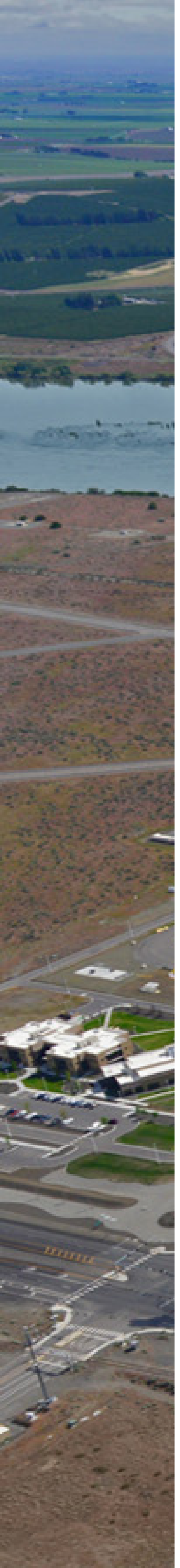
○ Not Implemented ◔ Partially Implemented ◑ Largely Implemented ● Fully Implemented

7. The organization maintains an up-to-date database of customers information that is updated at an organization-defined frequency.

○ Not Implemented ◔ Partially Implemented ◑ Largely Implemented ● Fully Implemented

8. The customer database is protected using an array of cybersecurity controls and the database is periodically backed up and stored in a safe location.

○ Not Implemented ◔ Partially Implemented ◑ Largely Implemented ● Fully Implemented



Pacific Northwest
NATIONAL LABORATORY

Manage Dependency Risk (cont)

9. The organization checks to verify that legitimate customers have the capability to securely store and process any hazardous or weaponizable chemical ordered from the organization.

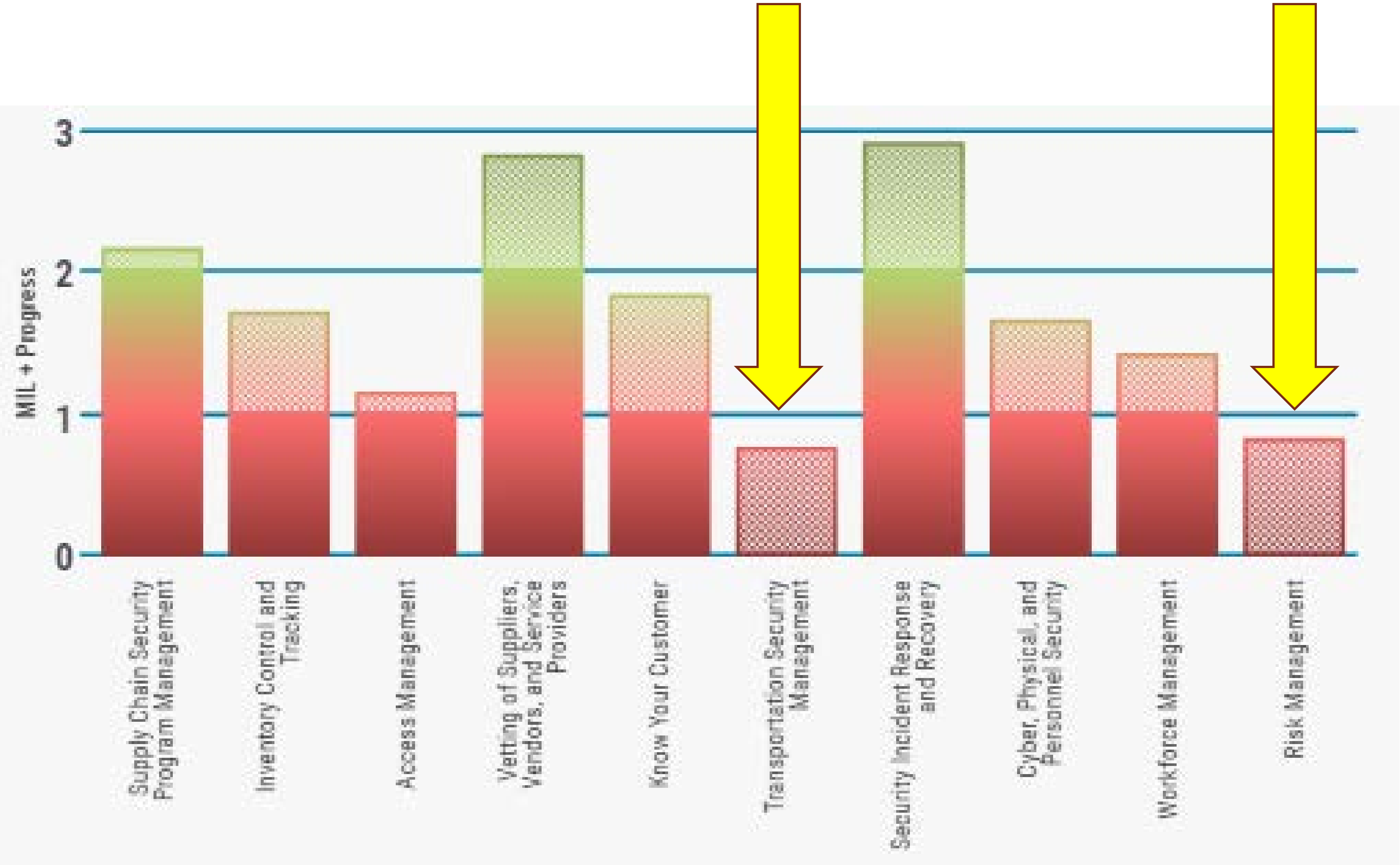
10. The identification and characterization of customers is conducted in a manner that fully meets industry standards for best practice.

Present Results

Pacific Northwest
NATIONAL LABORATORY

Overall Results

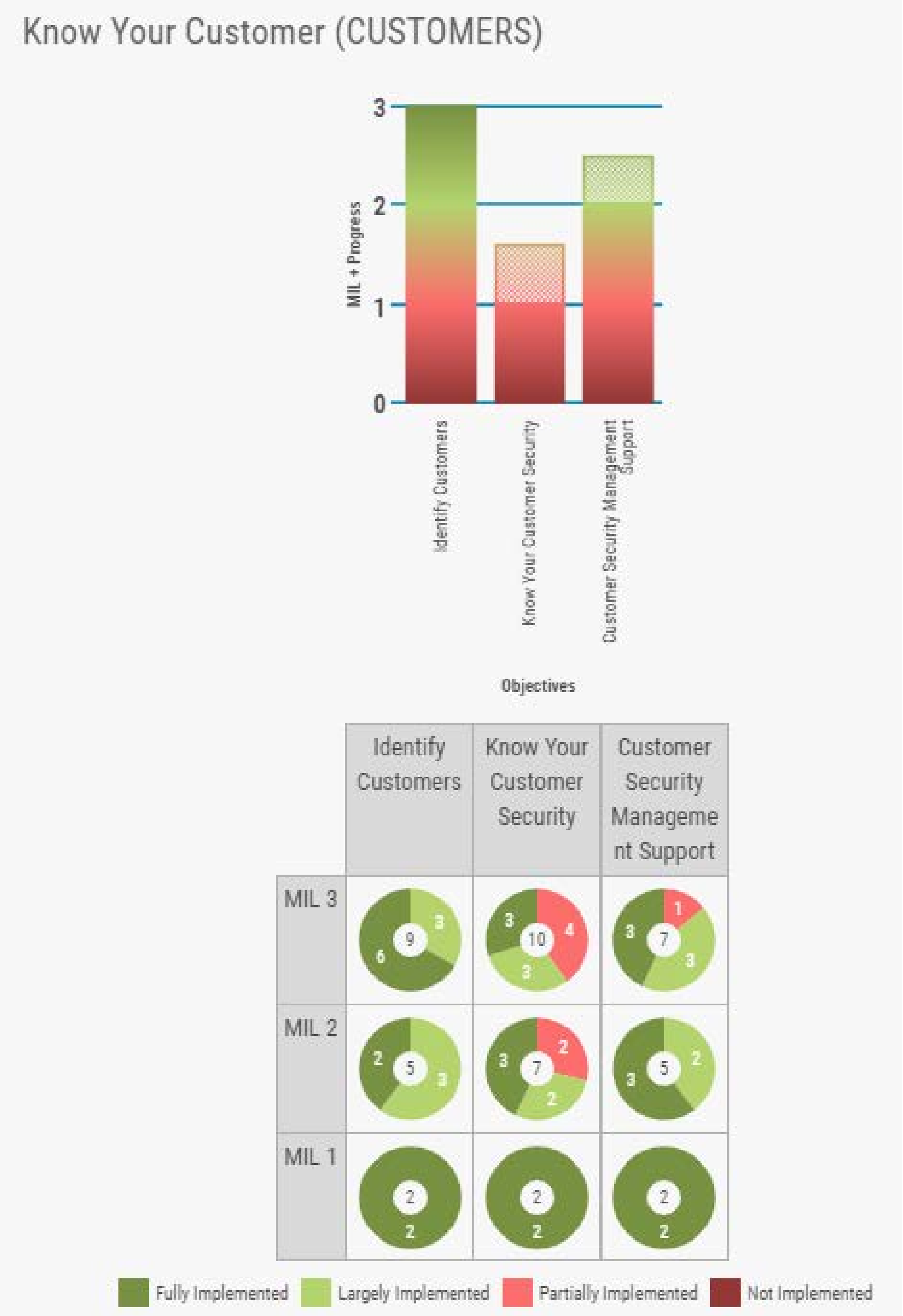
- Two domains, “Transportation Security” and “Risk Management” do not achieve MIL1
- Five domains achieve MIL1.
- Three domains achieve MIL2.
- Decision makers must decide if this profile for the chemical security program is acceptable.
- One option is to accept this distribution.

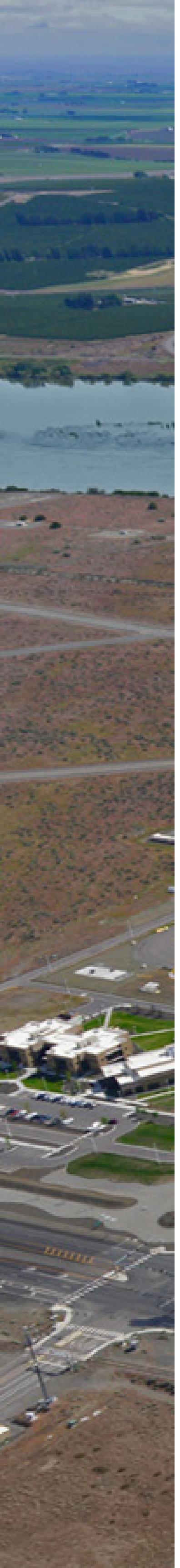


- Another option is to provide additional resources, or divert existing resources, to improve the “Transportation Security” and “Risk Management” performance program and bring them to MIL1 and in line with the five domains that achieve MIL1 and are part way towards MIL2.

Know Your Customer Domain

- Our exercise answers are provided for the *Identify Customer* objective in the “Know Your Customer” domain.
- This objective achieves MIL3!
- However, one of the other objectives for this domain only achieves MIL1 and the other achieves MIL2.
- Is the current distribution of sores acceptable to management?
- If improvements are warranted, determine which practices should be addressed.





Pacific Northwest
NATIONAL LABORATORY

Thank you

The Workshop Organizers

The U.S. partners at the workshop are Pacific Northwest National Laboratory (PNNL), CRDF Global, and their work is sponsored by the U.S. Department of State's Chemical Security Program (CSP). The Indian workshop partners include the CSIR-North East Institute of Science and Technology (CSIR-NEIST) and CSIR-Centre for Leather Research Institute (CSIR-CLRI). This workshop is a follow-up to the chemical security vulnerability assessment workshops conducted 2016 in Hyderabad; 2017 in New Delhi, Ahmedabad, and Hyderabad; 2018 in Chandigarh and Visakhapatnam and 2019 in Ahmedabad and Hyderabad.

Patrons and Advisory Committees

Patrons

Dr. Shekar Mande
Director General, CSIR, New Delhi, India

Dr. G. Narahari Sastry
Director, CSIR-NEIST, Jorhat, India

Dr. K.J. Sreeram
Director, CSIR-CLRI, Chennai, India

Mr. Jack Dishner
Chemical Security Program, Depart 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. R. L. Goswamee
Senior Principal Scientist, CSIR-NEIST, Jorhat, India

Dr. M. Surianarayanan
Senior Principal Scientist, CSIR-CLRI, Chennai, India

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

India

Dr. G. Narahari Sastry
Director, CSIR NEIST
Jorhat, Assam, India
Tel: +91 99635 82996
director@neist.res.in
gnsastry@gmail.com

Dr. Lakshi Saikia
Senior Scientist,
CSIR NEIST, Jorhat, Assam, India
Tel: +91-9957031635
lsaikia@neist.res.in
l.saikia@gmail.com

Dr. Manas Ranjan Das
Senior Scientist
CSIR NEIST
Tel: +91-9957178399
mrdas@neist.res.in

Dr. K.J. Sreeram
Director,
CSIR-Central Leather Research Institute
Adyar, Chennai, Tamil Nadu, India - 600 020
Phone: +91 - 44 - 24910897
Email:director@clri.res.in,

Dr. M. Surianarayanan
Senior Principal Scientist,
CSIR-Central Leather Research Institute
Adyar, Chennai, Tamil Nadu, India - 600 020
Tel: +1 509-375-2166
E-mail: clrimsn@gmail.com

USA

Dr. Clifford Glantz
Chief Scientist, PNNL
Tel: +1 509-375-2166
cliff.glantz@PNNL.gov

Dr. Radha Kishan Motkuri
Senior Principal Scientist, PNNL
Tel: +1 509-371-6484
radhakishan.motkuri@pnnl.gov

Dr. John Cort
Senior Principal Scientist, PNNL
Tel: +1 509-371-6334
john.cort@pnnl.gov

India (Proposed NACS)*

Prof. V.K. Jain
Gujarat University
Tel: +91-7926300969
drvkjain@hotmail.com

Prof. S. K. Mehta
Panjab University, Chandigarh
Tel:+91 944 080 2808
surinder.sk1961@gmail.com

Dr. G. V. M. Sharma
Yajushi Labs., Hyderabad
Tel: +91-944 080 2785
sharmagvm@gmail.com

Mr. 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

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

***NACS: National Association for Chemical Security (NACS)**

During the Indo-US workshop in 2018/2019, the organizers from both the USA and India, planned to establish an Association for Chemical Security at the National level, to popularize the concept on Chemical Security amongst all the Academia and Industry, along with all other stake-holders. In 2020, the above team has formed a General Body and went ahead for the registration of NACS, National Association for Chemical Security. The details will be released by the time of the proposed 5th Indo-US workshop (Virtual).

Indo-US

Workshops on

Strengthening Supply Chain Security in the Pharmaceutical Industry

2020

VIRTUAL WORKSHOP

November 30, 2020 to December 2, 2020

9h00 to 12h30 (3h30)

by

CSIR-North East Institute of Science and Technology, Jorhat, Assam, India

and

CSIR-Central Leather Research Institute, Chennai, Tamilnadu, India

In association with

Pacific Northwest National Laboratory (PNNL), Richland, WA, USA

U.S. Department of State's Chemical Security Program (CSP), Washington DC, USA

CRDF Global, Arlington, VA, USA

Pacific Northwest NATIONAL LABORATORY

CSP CHEMICAL SECURITY PROGRAM

CRDFGLOBAL INSPIRED BY PEOPLE | DRIVEN BY SCIENCE

CSIR-INDIA

CONNECTING SCIENCE & TECHNOLOGY NEIST FOR A BRIGHT TOMORROW

CSIR-CLRI