



Exceptional service in the national interest

# BIOENERGY CYBERSECURITY

## Landscape Survey

Timothy Berg

**Sandia National Laboratories**

BETO BIOENERGY CYBERSECURITY WORKSHOP

September 11, 2023 10:00 a.m. 2:00 p.m. PST (Virtual)

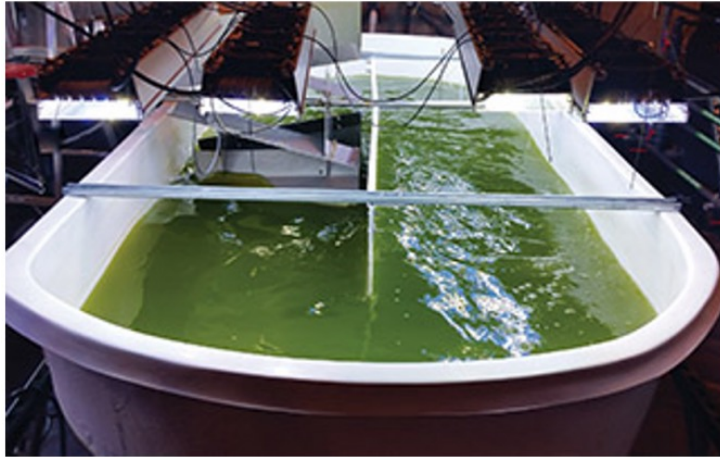
[www.sandia.gov/bioenergy-cybersecurity-workshop](http://www.sandia.gov/bioenergy-cybersecurity-workshop)

SAND2023-08983PE

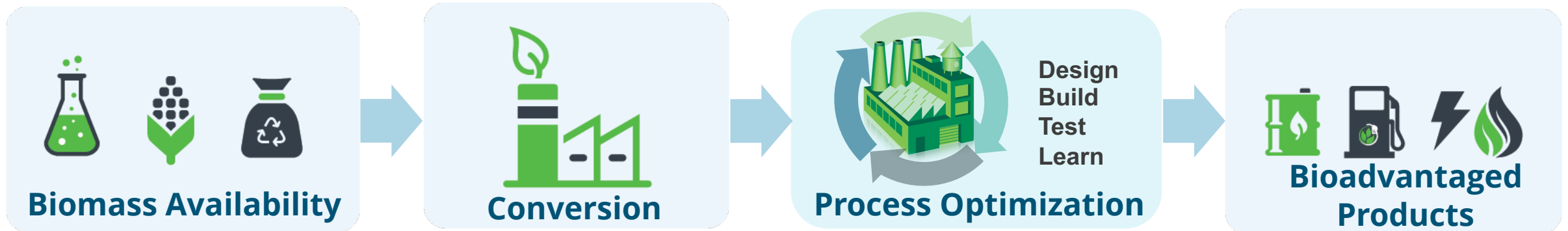
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.



# SANDIA BIOENERGY



Courtesy of ABPDU LBNL



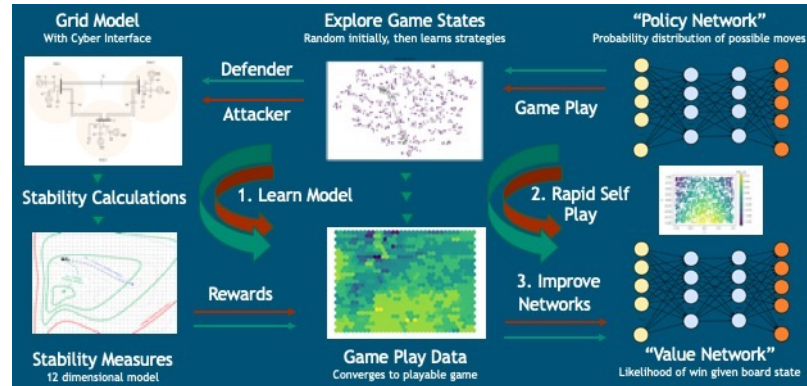
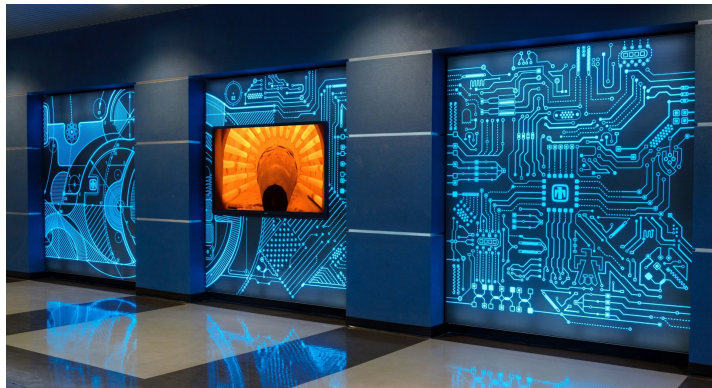
DISC  VR

**JBEI**  
Joint BioEnergy Institute

 **Agile  
BioFoundry**

 **USDA  
CERTIFIED  
BIOBASED**  
**bio**diesel****

# SANDIA CYBERSECURITY





# BIOENERGY CYBERSECURITY LANDSCAPE SURVEY OVERVIEW



**What risks do cyber events pose to BETO's mission?**

**Open Source Review**

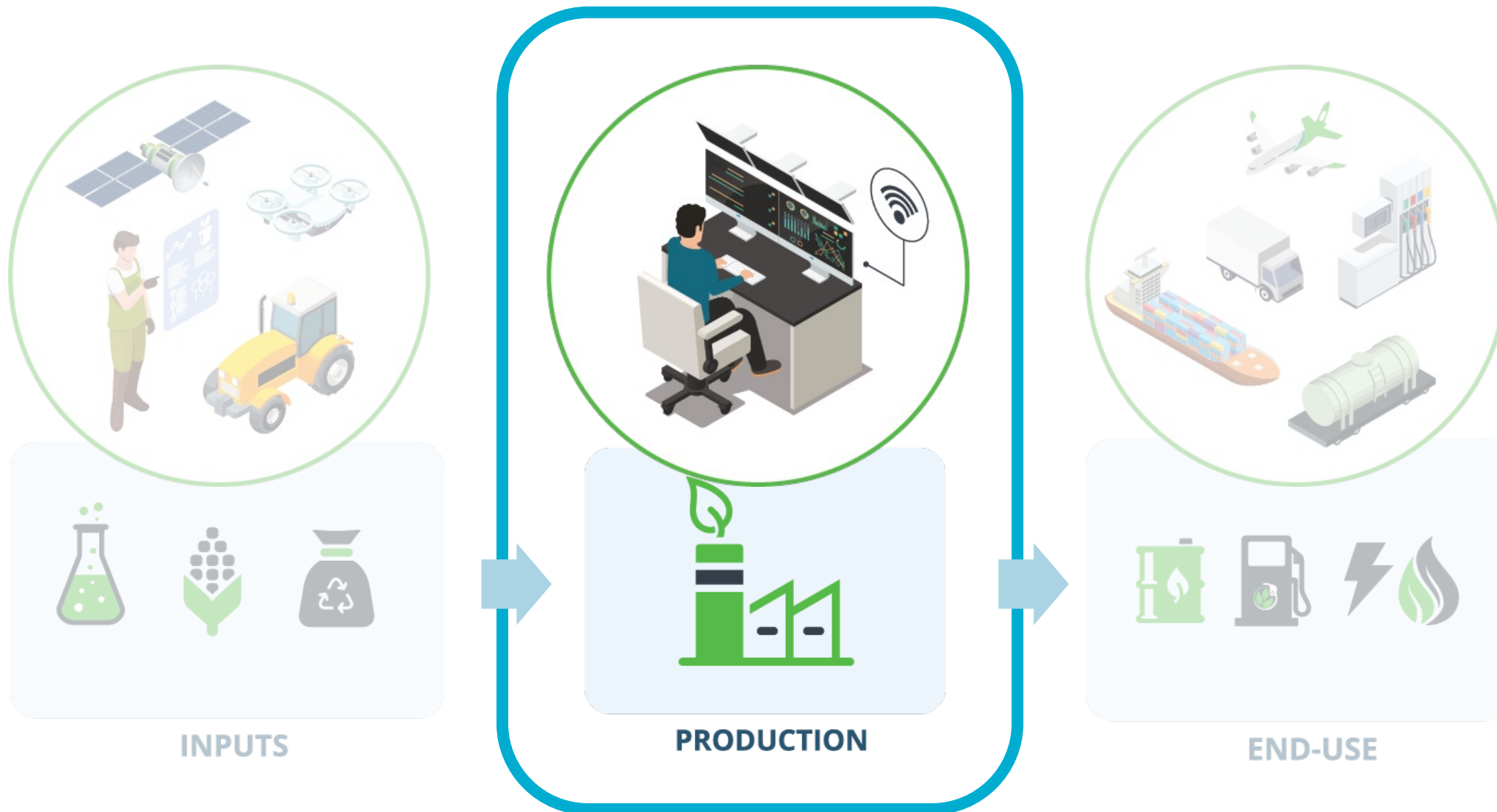
**What are the state of practice and challenges?**

**Subject Matter Expert Survey**

**What helpful actions do experts recommend BETO take?**



# BIOENERGY RELIES UPON MANY ADVANCED TECHNOLOGIES



# OPEN SOURCE SURVEY (CONDUCTED 2021)

## Open source survey

- Publications, articles, patents, press releases, industry literature, social media

## “Bioenergy cybersecurity” sparsely represented in the literature

- Katie Schroeder. *Digital Defenses*. Ethanol Producer Magazine. (8/2022).

## Biosecurity, biodefense, broader bioeconomy cybersecurity

- Cybersecurity of synthetic biology, genomic tools, datasets, biomanufacturing
- Examples: SARS-CoV-2 during survey, biology as code example

## Office of Energy Efficiency & Renewable Energy (EERE)

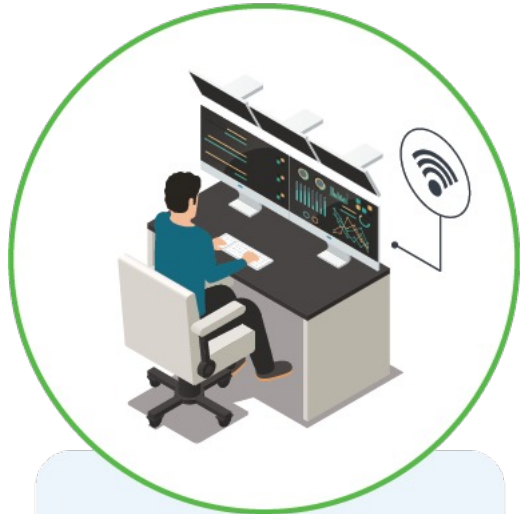
- EVs@Scale, H<sub>2</sub>@Scale cyber efforts: charging, fueling, grid infrastructure



# OPEN SOURCE SURVEY OF PRODUCTION CYBER IN RELATED SECTORS

## Operational technology (OT) security in related sectors

Oil & gas, food & beverage, pharmaceuticals, chemical, manufacturing



PRODUCTION

Colonial Pipeline (CP) (during survey, Summary from *CEO Senate testimony via Reuters*)

- Fuel shortages, panic buying, price spikes; long recovery for CP
- Started by theft of a single strong password of legacy remote access
- CP quickly paid \$5M ransom to regain access to their systems

Molson Coors (during survey, Summary from *SEC Form 8-K*)

- Short term production impacts, \$120-140M shift; cyber recovery costs
- Coincident with winter storms in Texas, Covid lockdowns
- Activated incident response plan, communication plan, law enforcement

Merck (began 2017, battled insurer during survey. Summary from *Reuters, NYFed, WSJ*)

- Worldwide operations disrupted: manufacturing, research, sales
- Started with corrupted software update from small, non-US firm
- Borrowed vaccines from CDC stockpile; \$1.4B insurance claim

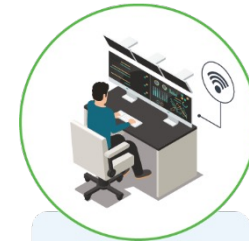
What is happening in bioenergy?

# SUBJECT MATTER EXPERT (SME) SURVEY

## SMEs represented broad range of bioenergy cybersecurity

**Bio:** Bioenergy, biotech, agriculture, policy, small to multinational corporations

**Cyber:** Industrial controls, design, penetration testers, red teamers, response & recovery



## Initial experts identified from open source survey, they recommended others

- Broad list of 464 considered; prioritized to 188 attempted contacts
- 120 of 184 replied (65% response rate) and scheduled interview or recommended another
- 107 interviews completed (>57% completion rate)
- Of 81 not interviewed:
  - 13 recommended another and provided valid contact information
  - 60 either did not respond or complete the scheduling process
  - 4 declined or required NDA or fee
  - 4 emails bounced





# DIVERSE INPUT FROM 107 BIO AND/OR CYBER EXPERTS

## Subject Matter Experts by Organization Type and Expertise



Included research, operations, maintenance, investors, legal, law enforcement, and international participants. Interviews were conducted January - May 2021.

# SUBJECT MATTER EXPERT (SME) SURVEY: CONCERNS

- 1) Elicit SME concerns and scenarios
- 2) Explore cyber relevance and impacts
- 3) Consider risks in BETO mission context



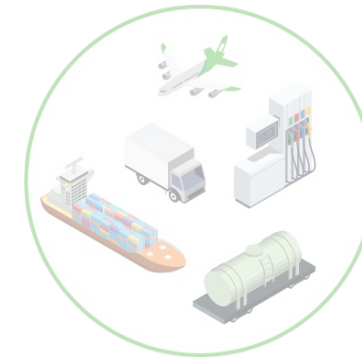
**Biology**  
**Business**  
**Computing**  
**Acceptance**  
**Supply chain**

**Competitiveness**



**Safety**  
**Environment**  
**Financial losses**  
**Public perception**  
**Equipment damage**

**Physical**



**Demand**  
**Adoption**  
**Regulation**  
**Distribution**  
**Infrastructure**

**Competitiveness**



# SUBJECT MATTER EXPERT (SME) SURVEY: CHALLENGES

## **Coordinating cybersecurity operations**

- Gathering data on incidents and needs
- Sharing of threat information, incidents, lessons learned
- Sharing operational cybersecurity expectations, standards
- Integrating IT and OT cyber operations with biological research
- Finding vetted guides, better practices, resilience and recovery plans

## **Balancing security priorities**

- Vetting partners, suppliers, visitors
- Addressing research mindset vs. security mindset
- Providing remote access for research, monitoring, control
- Balancing security needs with collaboration and trust barriers



# SUBJECT MATTER EXPERT (SME) SURVEY: DISTINCTIONS

## **OT security is not IT cybersecurity**

- Safety: humans, equipment, product
- Continuity of industrial operations
- Predictive, preventative maintenance
- Segmentation per facility owner

## **Similar but different from IT cybersecurity**

- Rigid change control
- Asset discovery, patching different
- Industrial controls and protocols

## **Bioenergy is its own business**

- Strong biology safety culture, ethics
- Feedstocks, bio-agents variable, perishable
- Research-driven, innovation-driven industry
- Segmentation per remote facilities

## **Similar but different from related sectors**

- Biologists think differently
- Biological failure modes different
- Biochemistry and bioprocesses





# SME RECOMMENDATIONS

## **DOE can play a helpful initial role with industry taking leadership**

- Gather incident and other cybersecurity data
- Help define the cyber problems, solutions, priorities
- Build a trusted bioenergy cybersecurity community
- Convene a workshop on the top priority

## **Flesh out a voluntary, appropriate baseline to support bioenergy stakeholders**

- Suggest ISA 62443 with bioenergy profile accommodating bioenergy specifics
- Use successive refinement with mature and well established security principles
- Borrow from templates of related sectors: oil & gas, chemical, pharmaceuticals, etc.
- Leverage the strong culture of safety in biology
- ISA/IEC/ANSI 62443 integrates well with ISO/IEC 27000 for IT/OT integration

## **Models/Resources**

- DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER), National Laboratories, others
- ISA99.02.01/IEC 62443, SANS ICS 410 Reference Model, NIST 800-82, NIST CSF, CISA Guidance, industry
- Partner models: BIO-ISAC (isac.bio), BioMADE, NIIMBL (biopharma), Manufacturing USA / CymanII
- Professional society track on cybersecurity



## CYBERSECURITY SUPPORTS BETO PRIORITIES



Enhance bioenergy  
value proposition



Cultivate end use  
markets and  
customers



Expand stakeholder  
engagement and  
collaboration



Develop,  
demonstrate,  
reduce costs and  
risks



***Cybersecurity increases plant value, reduces risks to bioenergy adoption.***



## **Contact Information:**

### **Anthe George**

Laboratory Relationship Manager for Bioenergy Technologies  
Office

Email: [angeorg@sandia.gov](mailto:angeorg@sandia.gov)

Phone: (925) 294-2723

### **Timothy Berg**

Email: [tberg@sandia.gov](mailto:tberg@sandia.gov)

Phone: (925) 294-2577



QUESTIONS?





## SMES INTERVIEWED BROKEN DOWN BY ORG TYPE, EXPERTISE

SME Organization	Area of Expertise	Number of SMEs
<b>Industry</b>		45
	Biotechnology	29
	<b>Bioenergy- Algae, Biomass, Waste, etc.</b>	17
	Biosecurity	9
	Other- Biotech Tools, Investment	3
	Cybersecurity	11
	Other: Energy Operations, Financial Risk	5
<b>Government</b>		39
	DOE National Laboratory	27
	Federal / International Law Enforcement	8
	Other: Federal Agencies	4
<b>Academia</b>		23
<b>Total</b>	Includes 8 non-US SMEs from all three areas	<b>107</b>

Over 100 subject matter experts (SMEs) provided input



## KEY BIOENERGY DEFINITIONS

**<sup>1</sup>Bioeconomy:** The share of the economy based on products, services, and processes derived from biological resources (e.g., plants and microorganisms).

**<sup>2</sup>Bioenergy:** Power and fuels produced from biomass.

**Biofuels:** Biomass-derived liquid or gaseous fuels such as ethanol, methanol, methane, and hydrocarbons.

**Biorefinery:** A facility that processes and converts biomass into value-added products is called a biorefinery...based on a number of processing platforms using mechanical, thermal, chemical, and biochemical processes.

**Technology Development Stages:** Process Development Unit, Pilot Plant, Demonstration Plant, Pioneer Plant, Commercial Plant

**De-risk:** Making bio-industrial processes and products safer and more appealing by reducing the risk of negative outcomes and financial loss.



# CYBER RISK AND OPERATIONAL TECHNOLOGY DEFINITIONS

## **CYBER RISK**

Risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system. (NISTIR 8183)

## **OPERATIONAL TECHNOLOGY**

The hardware, software, and firmware components of a system used to detect or cause changes in physical processes through the direct control and monitoring of physical devices. (NIST SP 800-172)

## **SECURITY SEGMENTATION**

A cost-effective and efficient security design approach for protecting cyber assets by grouping them based on both their communication and security requirements... a six-step process (NIST CSWP 28)



# SME SURVEY QUESTIONS

Introduction: Please summarize your background and areas of expertise.

1. Please share opportunities you have had to address cybersecurity in bioenergy.
2. How might a negative cyber security event hamper the adoption of bioenergy?
3. What specific scenarios or processes unique to bioenergy are most concerning?
4. Could any of the above scenarios be induced through cyber means?
5. Is bioenergy cybersecurity a solved issue? What solutions already exist?
6. What helpful role might BETO play improving cybersecurity of bioenergy systems?
7. Who else would be a good person to contact regarding bioenergy cybersecurity?

Conclusion: Do you have any questions, concerns, or anything else to add?





END