July 21, 2020

EMERGING ISSUES COMMITTEE CASE STUDIES

SUMMER 2020

copas
Council of Petroleum Accountants Societies

This Emerging Issues session is an interactive and collaborative seminar session that will take place on Adobe Connect. You will have received a link to the meeting in the email. Please follow the instructions in the email carefully to enter the session and arrive early.

This handout contains a copy of the meeting agenda, system and setup requirements, Break Out Room instructions and Case study details.

You may want to print the handout for use during the session, but for your best experience of this meeting please read the handout thoroughly prior to the meeting.

System and Session Requirement for Optimal Experience

Adobe connect requires a Bandwidth of 512Kbps for participants, meeting attendees, and end users of Adobe Connect applications. Please maximize the bandwidth available to you during the session for the best user experience.

This platform will require you to download the Adobe Connect application or use a flash enabled browser for access. The optimal experience is with the application, which you can access here: https://helpx.adobe.com/adobe-connect/connect-downloads-updates.html . It is recommended that you prepare for the meeting by downloading the application ahead of time.

This meeting is set up to use VOIP (Voice Over internet Protocol), so you will need to have active speakers or a headset to hear the presentation, there is no dial in access for the meeting. COPAS recommends the use of a USB headset, or other earbud/microphone combination for optimal audio. You should ensure that your computer/device audio settings have been selected prior to launching the application – headsets and ear buds plugged in after the application has launched many not be recognized.

For the best interactive experience, you should have access to a microphone to participate in discussion. Small Breakout rooms used during the EI meeting for topic one will also allow the use of webcams for participation. You may use a

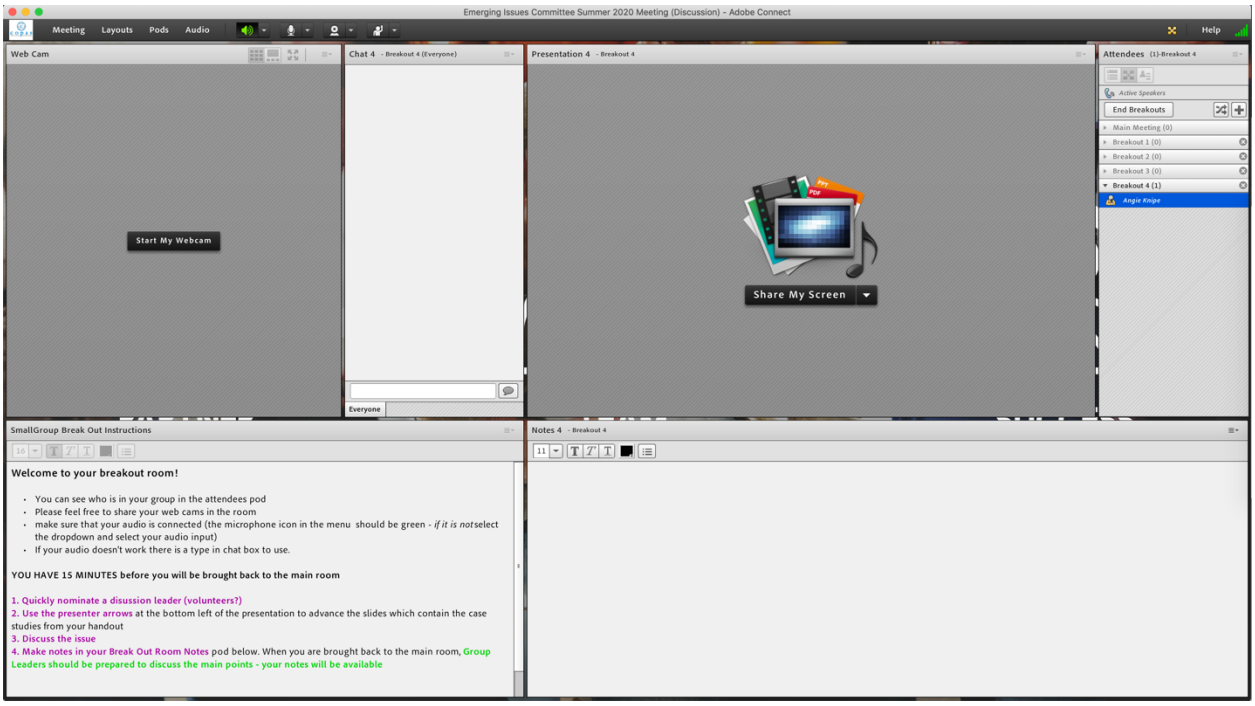
built-in microphone on your computer/laptop/device during the meeting as long as you keep the microphone muted when not speaking to avoid speaker echo over the system.

For the best viewing experience of all the information included in the session it is recommended that you use a computer for this session.

Breakout Rooms

As mentioned, breakout rooms for small group participation will be used for Topic One discussion in the Case Studies. Participants will be randomly distributed into a breakout room of approximately 10 participants in size. You will have access to microphone and web cam while in the breakout room. Cameras are not mandatory, and *type in chat* is available but not recommended as time is limited.

The following is a screenshot of a breakout room set up:



You will be able to see the name of the attendee in your breakout room in the Attendees pod.

1. Please decide on a group leader quickly as you will only have 15 minutes in the room.
2. Discuss the issue using the case study guide.
3. Make notes in the notes pod.
4. Discussion will continue after the breakout session in the main meeting room and your group leader will have the opportunity to participate and present your group's thoughts. The notes pods from your breakout room will be available and visible to all participants.

Summer 2020 Meeting
Tuesday, July 21, 2020 at 9:30 AM CST
Adobe Connect Online Meeting
Emerging Issues Committee Agenda

TIME (CDT)	AGENDA ITEM	DISCUSSSION LEADERS
9:30	Welcome and Introductions Antitrust Statement EI Disclaimer Meeting Overview & Format	Lucas Vaughn/Todd Smith
9:35	**Emerging Issues in the Oil and Gas Industry**	

This is a seminar session, consisting of guided case studies and small group discussion and review on issues affecting the oil & gas industry. Discussion will focus on how to account for costs related to these emerging issues.

Learning Objectives:

By the end of this session you will be able to:

1. Identify COVID Related Impacts in the Energy Industry
2. Describe an Operator's ability to charge ransom payments made to resolve a cyberattack on one of its facilities
3. Determine other major issues affecting the energy industry that may require additional discussion and analysis by COPAS

Program Level:	Intermediate
Pre-requisites:	Some familiarity with the COPAS documents, their purpose and use, as well as some familiarity with general accounting standards
Advance Preparation:	Read the EI Case Studies handout
Delivery Method:	Group Internet Based
Field of Study:	Specialized Knowledge
CPE Credits:	2.0

TOPIC ONE: COVID Related Impacts in the Energy Industry

	Topic Introduction and Overview	Lucas Vaughn/Todd Smith
9:50	Breakout Rooms – small group discussions	
10:10	Return to main meeting room – Group Leaders Share	
10:35	Break	
10:45	**TOPIC TWO: Cyber Attacks on the Energy Industry**	
	Topic Introduction and Overview	Lucas Vaughn/Todd Smith

11:10 Open discussion in the main meeting room

11:30 Adjourn

COPAS National Summer 2020: Emerging Issues Sub-Committee Meeting
Adobe Connect Online Meeting, July 21, 2020

DISCLAIMER FOR EMERGING ISSUES CASE STUDIES:

The COPAS Emerging Issues Sub-Committee is an open communications forum for expressing opinions and ideas relating to industry joint interest accounting and audit issues. These discussions, including any expression of ideas and results of straw polls, do not represent individual company positions, industry consensus or COPAS endorsement or policy. These discussions should not be represented as being industry policy or as being endorsed by COPAS in any forum or writing.

Submit a comment or question by text: 713-702-8957

COPAS National Summer 2020: Emerging Issues Sub-Committee Meeting
Adobe Connect Online Meeting, July 21, 2020

Case Study 1: COVID-19 Impacts Discussion

Oil and gas operators are incurring unplanned, onerous costs as they work to respond to the effects of the COVID-19 pandemic, including restrictions and requirements implemented by governmental authorities, and its subsequent effects on the supply-demand imbalance. Some of these costs affect Joint Property or Joint Operations, and today's discussion will focus on the reasons why such costs are either directly chargeable to a Joint Account or indirectly chargeable and recovered through the overhead rates (which type of overhead?) under existing Accounting Procedure language. Additionally, some experts predict a possible "second wave" of the COVID-19 pandemic in the fall, and there is a need to determine when costs are pandemic related.

The potential COVID-19 related costs are grouped into the five categories listed below. We will split into Adobe Connect breakout rooms for 20 minutes in order to collaborate on these topics. Please be sure to take notes on the breakout room discussion, even if a consensus is not reached. Following 20 minutes of breakout room discussion, we will reassemble in the main Adobe Connect meeting room to share the results of the topics discussed. Each breakout room should select a representative to share the highlights of the discussions when we reconvene.

<u>Potential COVID-19 Impacts to the Oil & Gas Industry to Consider</u>

1. Operator costs
    a. Deep cleaning of field offices, rigs, facilities
    b. Idle field labor, rig crews, frac crews, or other labor
    c. Standby for rigs, marine vessels, and other equipment during quarantine
    d. Medical screening as a preventative measure and for those that are sick
    e. Personal Protection Equipment requirements
    f. Paycheck Protection Program (PPP) loan forgiveness credits (should they be passed to Joint Account?)

2. Allocations (many are based on well count; many wells have been temporarily shut-in due to demand decreases)
    a. Are changes in allocation processes appropriate in these circumstances?
    b. If so, what kind of allocation changes would be acceptable or necessary?
    c. Should well count allocations of costs (including labor, vehicles, supplies, etc.) be based on active well count, or should the temporarily shut-in wells be included?
    d. What determines if a well was shut-in due to COVID-19 (certain date, how the shut-in was decided or implemented, etc.)?

e. If allocation methods are changed, should an operator apply the changes to all areas of operations, or is it acceptable to change a specific area only? Does it matter?
f. If allocation methods are changed, is an operator required to revert back to the original method at some point? And if so, when should that happen and what factors should be considered in determining the appropriate time to revert?

3. Project Cancellation
    a. As projects are cancelled, are the cancellation and related fees paid to project vendors directly chargeable?
    b. Are the costs of previously purchased long-lead assets directly chargeable? And if so, how should the costs be allocated across an operator's operation?
    c. Are the costs incurred for pre-drill services already performed directly chargeable (environmental assessments, etc.)? Are there any that would not be directly chargeable?
    d. Is an operator required to get non-operator approval for any of this?

4. Overhead
    a. If operator suspends drilling operations for 15-days while a rig crew is quarantined, does the force majeure provisions allow the operator to charge drilling overhead even though the suspension exceeded 14 days?
    b. Under what conditions, if any, is an operator allowed to charge overhead for wells that are shut-in due to curtailment?
    c. Is the COVID-19 pandemic considered a Catastrophe as defined in the APs, and if so, what timelines should be used to define the event duration?
    d. According to the 2005 AP, Catastrophe overhead is applied to costs necessary to restore the Joint Property to the equivalent condition that existed prior to the event. Has the "condition" of joint properties changed during the COVID-19 pandemic and if so, when would a joint property be considered "restored?"
    e. Which COVID-19 related costs, if any, attract Catastrophe overhead?

5. Audits
    a. If an operator closes their office and is not able or not willing to host remote audits:
        i. Is an operator expected to grant an extension of audit rights?
        ii. If so, under what circumstances and for how long is the extension granted?
        iii. Is either party able to make the decision to postpone the audit?

b. Is there a minimum standard of COVID-19 related protocols that should be in place at an Operator's office, and if so, how are they determined?
c. Does an operator have the right to refuse access to its offices if the non-operator refuses to abide by its COVID-19 safety protocols? If so, should the non-operator be granted an extension of audit rights, and for how long?
d. Does a non-operator have the right to refuse to work in an operator's office that does not have any COVID-19 related protocols in place (masks, distancing, etc.)? If so, should the non-operator be granted an extension of audit rights, and for how long?
e. Is there ever a point where an Operator must provide audit support electronically and remotely? If so, how is that point determined?

Case Study 2: Cyberattacks on Energy Infrastructure

Cyberattacks against government entities, corporations, and other groups and individuals are becoming increasingly common as a tool for creating chaos and disorder in our society. According to Wikipedia, a cyberattack:

- **Is defined as any type of offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices**.
- Can be part of cyberwarfare or cyberterrorism.
- Can be employed by sovereign states, individuals, groups, society or organizations, and may originate from an anonymous source.
- Includes a cyberweapon(s), which is a product used to facilitate a cyberattack.
- May steal, alter, or destroy a specified target by hacking into a susceptible system.
- Ranges from installing spyware on a personal computer to attempting to destroy the infrastructure of entire nations.
- Is an incident causing physical damage, which is different from the "routine" data breaches and broader hacking activities.

As facility automation and connectivity between networks grows, the use of cloud services increases, and decisions rely more and more on real time data analytics, oil and gas companies are becoming more and more exposed to cybersecurity-related threats and cyberattacks.

Some recent examples of cyberattacks in the oil & gas industry are below, followed by some related discussion questions:

- In March 2019, Norwegian aluminum producer Norsk Hydro was hit by ransomware, forcing parts of the industrial giant to operate via pen and paper. The company refused to pay the ransom, and said it incurred between USD $60 - $70 million in damages from the incident, of which only USD $3.6 million so far had been paid by insurance.

- In November 2019, a ransomware attack hit computer services and administrative work at the Mexican national oil company, Pemex. The hackers demanded about USD $5 million in bitcoin.

- In February 2020, the Department of Homeland Security reported a U.S. natural gas compressor facility was shut down for two days because of a cyberattack. Though the hackers did not gain control of the gas compression facility, the operator decided to perform a controlled shutdown after being unable to read and aggregate real-time

operational data. While ransomware is usually designed to block access to a computer system until money is paid, no information was provided publicly as to what the hackers were demanding.

Discussion Questions:

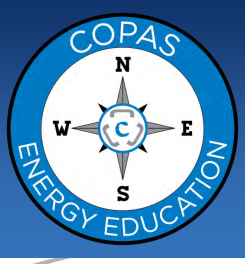
1. If a ransomware attack was deployed and an operator made a ransom payment in order to stop the attack, is the ransom payment directly chargeable to the Joint Account, and if so, under what provisions of Section II Direct Charges of the Accounting Procedure and/or Operating Agreement apply, when:
    a. Joint Property was directly impacted (e.g., well shut in and unable to sell product)?
    b. The operator's facility/equipment used in conducting Joint Operations was directly impacted in some way (e.g., equipment turned off or pipelines closed)?
    c. Operator's daily operations attacked (e.g. RTC shut off or accountants unable to log in to computers), but there was no obvious direct impact to the Joint Property?
    d. The attacker makes a general threat to an operator, but takes no action since the operator paid the ransom (so no obvious direct impact to the Joint Property)?
    e. The attacker makes a specific threat against Joint Property, but takes no action since the operator paid the ransom (so no obvious direct impact to the Joint Property)?

2. If ransom payments are billable, how do you assign a Joint Account value to cryptocurrency, such as bitcoin?

3. Are malicious acts – e.g., cyberattacks, activist attacks – on energy facilities considered a Catastrophe as defined in the various Accounting Procedures? Is the Catastrophe definition inclusive enough to cover such attacks?

4. If an operator upgrades its detection and recovery controls and/or systems for use in preventing and fighting against cyberattacks, are those costs directly chargeable to Joint Accounts? Why or why not?

Submit a comment or question by text: 713-702-8957


COPAS
N
W
E
S
ENERGY EDUCATION