Introduction Block

This survey will take approximately 20 minutes to complete

Dear Participant:

The International Society of Automation Global Cybersecurity Alliance (ISA GCA), Idaho State University (ISU), and Idaho National Laboratory (INL) request your help to determine a reasonable foundational set of knowledge needed to secure control systems -- *to which traditional IT, computer science, or cybersecurity students/professionals are not normally exposed*.

The results of this survey will inform and improve global efforts to educate and train professionals in this critical field.

Your responses to the survey will be anonymous (names and contact information are not requested, and IP addresses are not collected). All survey information will be retained and hosted on a third party Qualtrics server and not on an Idaho State University server.

Participation is completely voluntary and you may withdraw at any time. There is no reward for participating or consequence for not participating.

For further information regarding this research please contact Sean McBride at 208.282.2800, email:

participant you may contact the Idaho State University Human Subjects Committee Coordinator Tom Bailey, at 1-208-282-2179 or humsubj@isu.edu.

By choosing "I consent" below, you certify that you are 18 years or older, have read and understood this consent form, and agree to participate.

- ○ I consent
- ○ I do not consent

Section I - Respondent Background

Section I

In this section you will be asked about your professional background.

Highest degree obtained

- ○ High School Diploma/GED
- ○ Associate
- ○ Bachelor
- ○ Master
- ○ Doctorate

Major field of study of highest degree

Do you have professional engineering (PE) license/charter?

- ○ Yes
- ○ No

Professional specialty

- [ ] Electrical
- [ ] Chemical
- [ ] Civil
- [ ] Mechanical
- [ ] Control Systems
- [ ] Industrial
- [ ] Other

Professional experience in the following industries (select all that apply)

- [ ] Aerospace
- [ ] Chemical & Petroleum
- [ ] Construction & Design
- [ ] Food & Pharmaceuticals
- [ ] Mining & Metals
- [ ] Power
- [ ] Pulp & Paper
- [ ] Water & Wastewater
- [ ] Building Automation
- [ ] Manufacturing

Years experience in industrial automation / control systems

Percent experience in industrial automation / control systems in each organization type/role (must equal 100)

ICS product supplier	0
ICS integration service provider	0
ICS maintenance service provider	0
ICS asset owner	0
Total	0

Total years in cybersecurity

Percent cybersecurity experience (from Q8) in internal vs external role (must equal 100)

Securing your organization (internal role)	0
Securing other's organizations (external consultant/service provider)	0
Total	0

Percent cybersecurity experience in employer type (must equal 100)

Corporation/For Profit	0
Non-profit	0
Government	0
Academia	0
Total	0

Percent cybersecurity experience dealing with industrial automation / control systems (Input a number between 1-100)

Professional cybersecurity certifications held

ISA

- [ ] CAP
- [ ] CCST Level I
- [ ] CCST Level II
- [ ] CCST Level III
- [ ] 62443 Fundamentals Specialist
- [ ] 62443 Maintenance Specialist
- [ ] 62443 Design Specialist
- [ ] 62443 Risk Assessment Specialist

CompTIA

- [ ] Security+
- [ ] CySA+

(ISC)2

- [ ] CISSP
- [ ] SSCP
- [ ] CCSP
- [ ] CAP
- [ ] HCISPP

SANS GIAC

- [ ] GICSP
- [ ] GCIP
- [ ] GRID
- [ ] Offensive Operations Focus Certification
- [ ] Cyber Defense Focus Certification
- [ ] Cloud Security Focus Certification
- [ ] Digital Forensics Focus Certification

Have you worked as an educator?

- Yes
- No

How many years of experience do you have as an educator?
(Please input a number)

Percent experience providing education to student type (must equal 100)

secondary (high school)	0
post-secondary (college/university)	0
graduate	0
working professionals	0
Total	0

Percent of experience providing education by your role (must total 100)

Content author	0
Teacher	0
Total	0

Percent experience as educator that you have taught cybersecurity (input a number between 1-100)

Percent of experience as an educator covering cybersecurity by discipline (must total 100)

Enterprise/business IT	0
Industrial Automation / Control Systems	0
Other	0
Total	0

Section II - Foundational ICS Knowledge

Overview of Section II of III -- Foundational ICS Knowledge

In this section of the survey you will examine content to help determine a reasonable foundational set of knowledge needed to secure control systems -- *to which traditional IT, computer science, or cybersecurity students/professionals are not normally exposed.*

The content is currently composed of five categories (shown in bold) and associated topics. Please take a moment to preview the categories and topics below before proceeding to the survey questions. You may wish to Foundational ICS Knowledge text for reference as you proceed. This information will also be available as hover-over text for reference as you answer the questions.

Industrial operations ecosystem: industry sectors, professional roles and responsibilities in industrial environments, organizational roles, facilities, engineering diagrams, process types, industrial life-cycles

Instrumentation and control: sensing elements, control devices, programmable control devices, control paradigms, programming methods, process variables, data acquisition, supervisory control, alarms, engineering laptops/workstations, data historians, operator interfaces, control system software

Equipment under control: motors/generators, pumps, valves, relays, generators, transformers, breakers, variable frequency drives

Industrial communications: reference architectures,

industrial communications protocols, transmitter signals, fieldbuses

Safety: electrical safety, personal protective equipment, safety/hazards assessment, safety instrumented functions, lock-out tag-out, safe work procedures, common failure modes for equipment under control

Categories

First you will review the titles of the categories in this section.

Later you will be asked to provide input about the contents of each category.

On a scale of 1-10, Where 1 is irrelevant and 10 is extremely relevant, How relevant is each category to the field of industrial cybersecurity/ICS security?

Industrial Operations Ecosystem

Instrumentation and control

Equipment under control

Industrial communications

Safety

For each category title, recommend whether to: keep as is, change, or remove entirely.

If you recommend to change the title, you will be asked to suggest a new title in a follow-up question.

If you recommend to remove the title, you will be asked to enter a brief explanation.

	Keep as is	Change title	Remove category
Industrial Operations Ecosystem	○	○	○
Instrumentation and control	○	○	○
Equipment under control	○	○	○
Industrial Communications	○	○	○
Safety	○	○	○

What category title would you suggest over "Industrial operations ecosystem"?

Briefly explain why you would remove the category title "Industrial operations ecosystem"?

"What category title would you suggest over Instrumentation and control"?

Briefly explain why you would remove the category title "Instrumentation and control"?

What category title would you suggest over “Equipment under control"?

Briefly explain why you would remove the category title “Equipment under control"?

What category title would you suggest over “Industrial communications"?

Briefly explain why you would remove the category title “Industrial communications"

What category title would you suggest over "Safety"?

Briefly explain why you would remove the category title "Safety"?

Would you recommend adding additional categories of Foundational ICS knowledge to which traditional IT, computer science, or cybersecurity students/professionals are not normally exposed?

- Yes
- No

In the box below, please write the category names you recommend adding, separating them by commas.

Topics within Categories

Now you will review the contents of each category.

In this section you will review contents of the **Industrial operations ecosystem** category, which are:

Industry sectors, professional roles and responsibilities in industrial environments, organizational roles, facilities, engineering diagrams, process types, industrial life-cycles

On a scale of 1-10, Where 1 is irrelevant and 10 is extremely relevant, how relevant is each topic to the field of industrial cybersecurity/ICS security?

Industry sectors	
Professional roles and responsibilities in industrial environments	
Organizational roles	
Facilities	
Engineering diagrams	
Process types	
Industrial life-cycles	

For each topic, recommend whether to: keep as is, change, or remove entirely.

If you recommend to change the topic, you will be asked to suggest a new topic in a follow-up question.

If you recommend to remove the topic, you will be asked to enter a brief explanation.

	Keep as is	Change topic name	Remove topic
Industry sectors	○	○	○
Professional roles and responsibilities in industrial environments	○	○	○
Organizational roles	○	○	○
Facilities	○	○	○
Engineering diagrams	○	○	○
Process types	○	○	○
Industrial life-cycles	○	○	○

What topic would you suggest over "industry sectors"?

Briefly explain why you would remove the topic "Industry sectors".

What topic would you suggest over "Professional roles and responsibilities in industrial environments"?

Briefly explain why you would remove the topic "Professional roles and responsibilities in industrial environments".

What topic would you suggest over "Organizational

roles"?

Briefly explain why you would remove the topic "Organizational roles".

What topic would you suggest over "Facilities"?

Briefly explain why you would remove the topic "Facilities".

What topic would you suggest over "Engineering diagrams"?

Briefly explain why you would remove the topic "Engineering diagrams".

What topic would you suggest over "Process types"?

Briefly explain why you would remove the topic "Process types".

What category title would you suggest over "Industrial life-cycles"?

Briefly explain why you would remove the category title "Industrial life-cycles"

Would you recommend adding additional topics to this category (Industrial operations ecosystem) that are relevant to the field of industrial cybersecurity/ICS security?

- Yes
- No

In the box below, please write the topics you recommend adding to this category (Industrial operations ecosystem), separating them by commas.

In this section you will review contents of the **Instrumentation and Control** category, which are:

Sensing elements, Control devices, Programmable control devices, Control paradigms, Programming methods, Process variables, Data acquisition, Supervisory control, Alarms, Engineering laptops/workstations, Process data historians, Operator interfaces, Control systems software

On a scale of 1-10, Where 1 is irrelevant and 10 is extremely relevant, how relevant is each topic to the field of industrial cybersecurity/ICS security?

Sensing elements

Control devices

Programmable control devices

Control paradigms

Programming methods

Process variables

Data acquisition

Supervisory control

Alarms

Engineering laptops/workstations

Operator interfaces

Control systems software

For each topic, recommend whether to: keep as is, change, or remove entirely.

If you recommend to change the topic, you will be asked to suggest a new topic in a follow-up question.

If you recommend to remove the topic, you will be asked to enter a brief explanation.

	Keep as is	Change topic name	Remove topic
Sensing elements	○	○	○
Control devices	○	○	○
Programmable control devices	○	○	○
Control paradigms	○	○	○
Programming	○	○	○

Supervisory control	○	○	○
Alarms	○	○	○
Engineering laptops/workstations	○	○	○
Process data historians	○	○	○
[illegible]	○	○	○
[illegible] software	○	○	○

What topic would you suggest over "Sensing elements"?

Briefly explain why you would remove the topic "Sensing elements".

What topic would you suggest over "Control devices"?

Briefly explain why you would remove the topic "Control devices".

What topic would you suggest over "Programmable control devices"?

Briefly explain why you would remove the topic "Programmable control devices".

What topic would you suggest over "Control paradigms"?

Briefly explain why you would remove the topic "Control paradigms".

What topic would you suggest over "Programming methods"?

Briefly explain why you would remove the topic "Programming methods".

What topic would you suggest over "Process variables"?

Briefly explain why you would remove the topic "Process variables".

What topic would you suggest over "Data acquisition"?

Briefly explain why you would remove the topic "Data acquisition".

What topic would you suggest over "Supervisory control"?

Briefly explain why you would remove the topic "Supervisory control".

What topic would you suggest over "Alarms"?

Briefly explain why you would remove the topic "Alarms".

What topic would you suggest over "Engineering laptops/workstations"?

Briefly explain why you would remove the topic "Engineering laptops/workstations".

What topic would you suggest over "Process data historians"?

Briefly explain why you would remove the topic "Process data historians".

What topic would you suggest over "Operator interfaces"?

Briefly explain why you would remove the topic "Operator interfaces".

What topicwould you suggest over "Control system software"?

Briefly explain why you would remove the topic "Control systems software".

Would you recommend adding additional topics to this category (Instrumentation and control) that are relevant to the field of industrial cybersecurity/ICS security?

- Yes
- No

In the box below, please write the topics you recommend

adding to this category (Instrumentation and control), separating them by commas.

In this section you will review contents of the **Equipment under control** category, which are:

Motors, Pumps, Valves, Relays, Generators, Transformers, Breakers, Variable frequency drives

On a scale of 1-10, Where 1 is irrelevant and 10 is extremely relevant, how relevant is each topic to the field of industrial cybersecurity/ICS security?

Motors	
Pumps	
Valves	
Relays	
Generators	
Transformers	
Breakers	
Variable frequency drives	

For each topic, recommend whether to: keep as is, change, or remove entirely.

If you recommend to change the topic, you will be asked to suggest a new topic in a follow-up question.

If you recommend to remove the topic, you will be asked to enter a brief explanation.

	Keep as is	Change topic name	Remove topic
Motors	○	○	○
Pumps	○	○	○
Valves	○	○	○
Relays	○	○	○
Generators	○	○	○
Transformers	○	○	○
Breakers	○	○	○
Variable frequency drives	○	○	○

What topic would you suggest over "Motors"?

Briefly explain why you would remove the topic "Motors".

What topic would you suggest over "Pumps"?

Briefly explain why you would remove the topic "Pumps".

What topic would you suggest over "Valves"?

Briefly explain why you would remove the topic "Valves".

What topic would you suggest over "Relays"?

Briefly explain why you would remove the topic "Relays".

What topic would you suggest over "Generators"?

Briefly explain why you would remove the topic "Generators".

What category title would you suggest over "Transformers"?

Briefly explain why you would remove the category title "Transformers".

What category title would you suggest over "Breakers"?

Briefly explain why you would remove the category title "Breakers".

What category title would you suggest over "Variable frequency drives"?

Briefly explain why you would remove the category title "Variable frequency drives".

Would you recommend adding additional topics to this category (Equipment under control) that are relevant to the field of industrial cybersecurity/ICS security?

- ○ Yes
- ○ No

In the box below, please write the topcs you recommend adding to this category (Equipment under control), separating them by commas.

In this section you will review contents of the **Industrial communications** category, which are:

reference architectures, industrial communications protocols, transmitter signals, fieldbuses

On a scale of 1-10, Where 1 is irrelevant and 10 is extremely relevant, how relevant is each topic to the field of industrial cybersecurity/ICS security?

Reference Architectures	
Industrial communications protocols	
Transmitter signals	
Fieldbuses	

For each topic, recommend whether to: keep as is, change, or remove entirely.

If you recommend to change the topic, you will be asked to suggest a new topic in a follow-up question.

If you recommend to remove the topic, you will be asked to enter a brief explanation.

	Keep as is	Change topic name	Remove topic
Reference architectures	○	○	○
Industrial communications protocols	○	○	○
Transmitter signals	○	○	○
Fieldbuses	○	○	○

What topic would you suggest over "Reference architectures"?

Briefly explain why you would remove the topic "Reference architetctures".

What topic would you suggest over "Industrial communications protocols"?

Briefly explain why you would remove the topic "Industrial communications protocols".

What topic would you suggest over "Transmitter signals"?

Briefly explain why you would remove the topic "Transmitter signals".

What topic would you suggest over "Fieldbuses"?

Briefly explain why you would remove the topic "Fieldbuses".

Would you recommend adding additional topics to this category (Industrial communications) that are relevant to the field of industrial cybersecurity/ICS security?

- ○ Yes
- ○ No

In the box below, please write the topics you recommend adding to this category (Industrial communications), separating them by commas.

In this section you will review contents of the **Safety** category, which are:

Electrical safety, personal protective equipment, safety/hazards assessment, safety instrumented functions, lock-out tag-out, safe work procedures, common failure modes for equipment under control

On a scale of 1-10, Where 1 is irrelevant and 10 is extremely relevant, how relevant is each topic to the field of industrial cybersecurity/ICS security?

Electrical safety	
Personal protective equipment	
Safety/hazards assessment	
Safety instrumented functions	
Lock-out, tag out	
Safe work procedures	
Common failure modes for equipment under control	

For each topic, recommend whether to: keep as is, change, or remove entirely.

If you recommend to change the topic, you will be asked to suggest a new topic in a follow-up question.

If you recommend to remove the topic, you will be asked to enter a brief explanation.

	Keep as is	Change topic name	Remove topic
Electrical safety	○	○	○
Personal protective equipment	○	○	○
Safety/hazards assessment	○	○	○
Safety instrumented functions	○	○	○
lock-out, tag-out	○	○	○
Safe work procedures	○	○	○
Common failure modes for equipment under control	○	○	○

What topic would you suggest over "Electrical safety"?

Briefly explain why you would remove the topic "Electrical safety".

What topic would you suggest over "Personal protective equipment"?

Briefly explain why you would remove the topic "Personal protective equipment".

What topic would you suggest over "Safety/hazards assessment"?

Briefly explain why you would remove the topic "Safety/hazards assessment".

What topic would you suggest over "Safety instrumented functions"?

Briefly explain why you would remove the topic "Safety instrumented functions".

What topic would you suggest over "Lock-out, tag-out"?

Briefly explain why you would remove the topic "Lock-out, tag-out".

What category title would you suggest over "Safe work procedures"?

Briefly explain why you would remove the category title "Safe work procedures".

What category title would you suggest over "Common failure modes for equipment under control"?

Briefly explain why you would remove the category title "Common failure modes for equipment under control".

Would you recommend adding additional topics to this category (Safety) that are relevant to the field of industrial cybersecurity/ICS security?

- Yes
- No

In the box below, please write the topics you recommend adding to this category (Safety), separating them by commas.

Please list the topics that you recommend should be in the new Foundational ICS Knowledge category (or categories) you suggested. Provide the list in the format of Category1: topic1, topic2, topic3, ...

Section III - ICS Security Knowledge

Overview of Section III -- ICS Security Knowledge

In this section of the survey you will examine content to help determine a reasonable foundational set of knowledge needed to secure control systems -- *to which traditional IT, computer science, or cybersecurity students/professionals are not normally exposed.*

The content is currently composed of four categories (shown in bold) and associated topics. Please take a moment to preview the categories and topics below

before proceeding to the survey questions.

Regulation and guidance: Presidential/executive orders, ISA/IEC 62443, NIST SP 800-82 R2, NERC CIP, EU Cybersecurity Act

Common weaknesses: indefensible network architectures, unauthenticated protocols, unpatched and outdated hardware/firmware/software, lack of training and awareness among ICS-related personnel, transient devices, third-party access, unverified supply chain

Events and incidents: DHS Aurora, Stuxnet, Ukraine 2015, Ukraine 2016, Triton, Taum Sauk Dam, DC Metro Red Line, San Bruno, Colonial pipeline

Defensive technologies and approaches: firewalls, data diodes, process data analysis, ICS network monitoring, cyber-informed engineering, process hazards assessment-based approaches, cyber-physical fail-safes, awareness and training for ICS-related personnel

Categories

First you will review the titles of the categories in this section.

Later you will be asked to provide input about the contents of each category.

On a scale of 1-10, Where 1 is irrelevant and 10 is extremely relevant, How relevant is each category to the field of industrial cybersecurity/ICS security?

Regulation and guidance	
Common weaknesses	
Events and incidents	
Defensive technologies and approaches	

For each category title, recommend whether to: keep as is, change, or remove entirely.

If you recommend to change the title, you will be asked to suggest a new title in a follow-up question.

If you recommend to remove the title, you will be asked to enter a brief explanation.

	Keep as is	Change title	Remove category
Regulation and guidance	○	○	○
Common weaknesses	○	○	○
Events and incidents	○	○	○
Defensive technologies and approaches	○	○	○

What category title would you suggest over "Regulation and Guidance"?

Briefly explain why you would remove the category title "Regulation and guidance"?

What category title would you suggest over "Common weaknesses"?

Briefly explain why you would remove the category title "Common weaknesses".

What category title would you suggest over "Events and incidents"?

Briefly explain why you would remove the category title "Events and incidents".

What category title would you suggest over "Defensive technologies and approaches"?

Briefly explain why you would remove the category title "Defensive technologies and approaches".

Would you recommend adding additional categories of ICS security knowledge to which traditional IT, computer science, or cybersecurity students/professionals are not normally exposed?

- ○ Yes
- ○ No

In the box below, please write the category names you recommend adding, separating them by commas.

Topics within Categories

Now you will review the contents of each category.

In this section you will review contents of the **Regulation and guidance** category, which are:

ISA/IEC 62443, Presidential/executive orders, NIST SP

800-82 R2, NERC CIP, EU Cybersecurity Act

On a scale of 1-10, Where 1 is irrelevant and 10 is extremely relevant, how relevant is each topic to the field of industrial cybersecurity/ICS security?

ISA/IEC 62443

Presidential/executive orders

NIST SP 800-82

NERC CIP

EU Cybersecurity Act

For each topic, recommend whether to: keep as is, change, or remove entirely.

If you recommend to change the topic, you will be asked to suggest a new topic in a follow-up question.

If you recommend to remove the topic, you will be asked to enter a brief explanation.

	Keep as is	Change topic name	Remove topic
ISA/IEC 62443	○	○	○
Presidential/Executive orders	○	○	○
NIST SP 800-82 R2	○	○	○
NERC CIP	○	○	○
EU Cybersecurity Act	○	○	○

What topic would you suggest over "ISA/IEC 62443"?

Briefly explain why you would remove the topic "ISA/IEC

62443".

What topic would you suggest over "Presidential/executive orders"?

Briefly explain why you would remove the topic "Presidential/executive orders".

What topic would you suggest over "NIST SP 800-82 R2"?

Briefly explain why you would remove the topic "NIST SP 800-82 R2".

What topic would you suggest over "NERC CIP"?

Briefly explain why you would remove the topic "NERC CIP".

What topic would you suggest over "EU Cybersecurity Act"?

Briefly explain why you would remove the topic "EU

Cybersecurity Act".

Would you recommend adding additional topics to this category (Regulation and guidance) that are relevant to the field of industrial cybersecurity/ICS security?

- Yes
- No

In the box below, please write the category names you recommend adding to this category (Regulation and guidance), separating them by commas.

In this section you will review contents of the **Common weaknesses** category, which are:

indefensible network architectures, unauthenticated protocols, unpatched and outdated hardware/firmware

/software, lack of training and awareness among ICS-related personnel, transient devices, third-party access, unverified supply chain

On a scale of 1-10, Where 1 is irrelevant and 10 is extremely relevant, how relevant is each topic to the field of industrial cybersecurity/ICS security?

Indefensible network architectures	
Unauthenticated protocols	
Unpatched and outdated hardware/firmware/software	
Lack of training and awareness among ICS-related personnel	
Transient devices	
Third-party access	
Unverified supply chain	

For each topic, recommend whether to: keep as is, change, or remove entirely.

If you recommend to change the topic, you will be asked to suggest a new topic in a follow-up question.

If you recommend to remove the topic, you will be asked to enter a brief explanation.

	Keep as is	Change topic name	Remove topic
Indefensible network architectures	○	○	○
Unauthenticated protocols	○	○	○
Unpatched and outdated hardware/firmware /software	○	○	○
Lack of training and awareness among ICS-related personnel	○	○	○
Transient devices	○	○	○
Third-party access	○	○	○
Unverified supply chain	○	○	○

What topic would you suggest over "Indefensible network architectures"?

Briefly explain why you would remove the topic "Indefensible network architectures".

What topic would you suggest over "Unauthenticated protocols"?

Briefly explain why you would remove the topic "Unauthenticated protocols".

What topic would you suggest over "Unpatched and outdated hardware/firmware/software"?

Briefly explain why you would remove the topic "Unpatched and outdated hardware/firmware/software".

What topic would you suggest over "Lack of training and awareness among ICS-related personnel"?

Briefly explain why you would remove the topic "Lack of training and awareness among ICS-related personnel".

What topic would you suggest over "Transient devices"?

Briefly explain why you would remove the topic "Transient devices".

What topic would you suggest over "Third-party access"?

Briefly explain why you would remove the topic "Third-party access".

What topic would you suggest over "Unverified supply

chain"?

Briefly explain why you would remove the topic "Unverified supply chain".

Would you recommend adding additional topics to this category (Common weaknesses) that are relevant to the field of industrial cybersecurity/ICS security?

- Yes
- No

In the box below, please write the category names you recommend adding to this category (Common weaknesses), separating them by commas.

In this section you will review contents of the **Events and incidents** category, which are:

DHS Aurora, Stuxnet Ukraine 2015, Ukraine 2016, Triton, Taum Sauk Dam, DC Metro Red Line, San Bruno, Colonial Pipeline

On a scale of 1-10, Where 1 is irrelevant and 10 is extremely relevant, how relevant is each topic to the field of industrial cybersecurity/ICS security?

DHS Aurora

Stuxnet

Ukraine 2015

Ukraine 2016

Triton

Taum Sauk Dam

DC Metro Red Line

San Bruno

Colonial Pipeline

For each topic, recommend whether to: keep as is, change, or remove entirely.

If you recommend to change the topic, you will be asked to suggest a new topic in a follow-up question.

If you recommend to remove the topic, you will be asked to enter a brief explanation.

	Keep as is	Change topic name	Remove topic
DHS Aurora	○	○	○
Stuxnet	○	○	○
Ukraine 2015	○	○	○
Ukraine 2016	○	○	○
Triton	○	○	○
Taum Sauk Dam	○	○	○
DC Metro Red Line	○	○	○
San Bruno	○	○	○
Colonial pipeline	○	○	○

What topic would you suggest over "DHS Aurora"?

Briefly explain why you would remove the topic "DHS Aurora".

What topic would you suggest over "Stuxnet"?

Briefly explain why you would remove the topic "Stuxnet".

What topic would you suggest over "Ukraine 2015"?

Briefly explain why you would remove the topic "Ukraine 2015".

What topic would you suggest over "Ukraine 2016"?

Briefly explain why you would remove the topic "Ukraine 2016".

What topic would you suggest over "Triton"?

Briefly explain why you would remove the topic "Triton".

What category title would you suggest over "Taum Sauk Dam"?

Briefly explain why you would remove the category title "Taum Sauk Dam".

What category title would you suggest over "DC Metro

Red Line"?

Briefly explain why you would remove the category title "DC Metro Red Line".

What category title would you suggest over "San Bruno"?

Briefly explain why you would remove the category title "San Bruno".

What category title would you suggest over "Colonial pipeline"?

Briefly explain why you would remove the category title "Colonial pipeline".

Would you recommend adding additional topics to this category (Events and incidents) that are relevant to the field of industrial cybersecurity/ICS security?

- Yes
- No

In the box below, please write the category names you recommend adding to this category (Events and incidents), separating them by commas.

In this section you will review contents of the **Defensive technologies and approaches** category, which are:

Industrial network firewalls, data diodes, process data correlation, ICS network monitoring, cyber-informed engineering, process hazards assessment-based approaches, cyber-physical fail-safes, awareness and training for ICS-related personnel

On a scale of 1-10, Where 1 is irrelevant and 10 is extremely relevant, how relevant is each topic to the field of industrial cybersecurity/ICS security?

Industrial network firewalls	
Data diodes	
Process data analysis	
ICS network monitoring	
Cyber-informed engineering	
Process hazards assessment-based approaches	
Cyber-physical fail-safes	
Awareness and training for ICS-related personnel	

For each topic, recommend whether to: keep as is, change, or remove entirely.

If you recommend to change the topic, you will be asked to suggest a new topic in a follow-up question.

If you recommend to remove the topic, you will be asked to enter a brief explanation.

	Keep as is	Change topic name	Remove topic
Industrial network firewalls	○	○	○
Data diodes	○	○	○
Process data analysis	○	○	○
ICS network monitoring	○	○	○
Cyber-informed engineering	○	○	○
Process hazards assessment-based approaches	○	○	○
Cyber-physical fail-safes	○	○	○
Awareness and training for ICS-related personnel	○	○	○

What topic would you suggest over "Industrial network firewalls"?

Briefly explain why you would remove the topic "Industrial network firewalls".

What topic would you suggest over "Data diodes"?

Briefly explain why you would remove the topic "Data diodes".

What topic would you suggest over "Process data analysis"?

Briefly explain why you would remove the topic "Process data analysis".

What topic would you suggest over "ICS network monitoring"?

Briefly explain why you would remove the topic "ICS network monitoring".

What topic would you suggest over "Cyber-informed engineering"?

Briefly explain why you would remove the topic "Cyber-informed engineering".

What topic would you suggest over "Process hazards assessment-based approaches"?

Briefly explain why you would remove the topic "Process hazards assessment-based approaches".

What topic would you suggest over "Cyber-physical fail-safes"?

Briefly explain why you would remove the topic "Cyber-physical fail-safes".

What topic would you suggest over "Awareness and training for ICS-related personnel"?

Briefly explain why you would remove the topic "Awareness and training for ICS-related personnel".

Would you recommend adding additional topics to this category (Defensive technologies and approaches) that are relevant to the field of industrial cybersecurity/ICS security?

- Yes
- No

In the box below, please write the topics you recommend adding to this category (Defensive technologies and approaches), separating them by commas.

Please list the topics that you recommend should be in the new Industrial Cybersecurity Knowledge category (or categories) you suggested. Please provide the list in the format of Category1: topic1, topic2, topic3, ...

Closure block

Thank you for your time spent taking this survey.

To learn more about and participate in efforts to improve industrial cybersecurity education, training, and workforce development, please visit the community of practice web site: https://inl.gov/icscop