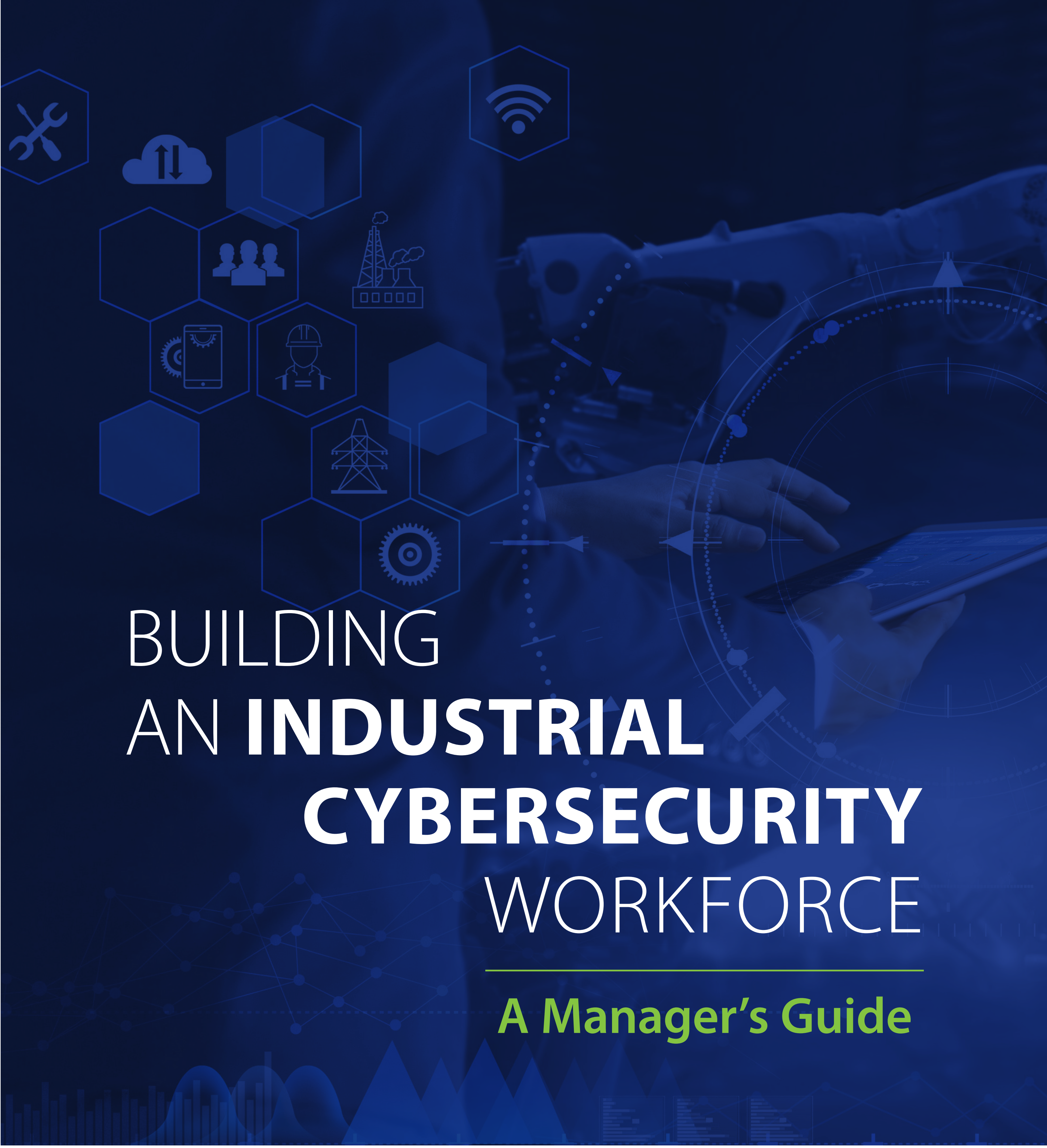


BUILDING AN **INDUSTRIAL CYBERSECURITY** WORKFORCE

A Manager's Guide

Idaho State University

INL Idaho National Laboratory

INDUSTRIAL CYBERSECURITY **AWAKENING**

As smart devices and networks push deeper into power grids, oil refineries, and water treatment plants, we must consciously prepare professionals to securely design, build, operate and maintain such infrastructures so that they are prepared to protect and defend them.

This document, “A Manager’s Guide” is the first in a series of guidebooks dedicated to the important topic of developing an industrial cybersecurity workforce. Other publications will include “A Human Resources Guide” for Human Resource (HR) personnel seeking to ensure the effectiveness of industrial cybersecurity personnel, and “A Career Development Guide” for individuals seeking to develop industrial cybersecurity competencies.

This guide will aid managers in answering four pivotal questions:

1. **Are you ready to build an industrial cybersecurity team?**
2. **How do you structure your industrial cybersecurity team?**
3. **What does you industrial cybersecurity team need to know?**
4. **What does your industrial cybersecurity team need to do?**

ARE YOU READY TO BUILD AN INDUSTRIAL CYBERSECURITY TEAM?

Many managers fail to fully appreciate the intense cultural, managerial, and educational differences between information technology (IT) systems and operational technology (OT) systems, which we call the IT-OT gap.

IT systems consist of desktops, laptops, web servers, communications networks, email, storage and backup systems used to help humans make better decisions.

OT systems consist of programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA), control logic, sensors and actuators that provide reliable electricity, consistent transportation, and safe drinking water. Operational technology systems are the collection of technologies used to control and monitor industrial operations used in electric power, oil & natural gas, water & wastewater, and manufacturing sectors. These systems include:

- Industrial control systems (ICS)
- Supervisory control and data acquisition (SCADA)
- Programmable logic controllers (PLCs)
- Industrial control communications protocols, control logic, sensors and actuators.

Figure: Information Technology (IT) Versus Operation Technology (OT)

The table below shows some of the differing characteristics between information technology and operational technology.

	Information Technology	Operational Technology
Being controlled	Data	Physics
Measurement	Bits and bytes	Temperature, pressure, flow
Lifecycle	System lifecycle	Facility lifecycle
Consequences	Competitive disadvantage Embarrassment Financial loss	Product damage Loss of life Environmental release
Desired system characteristics	Confidentiality Integrity Availability	Safety Reliability Functionality
Educational background	Computer Science Information Systems Cybersecurity	On the job Career & Technical Education Electrical Engineering
Reporting chain	ISO CISO CIO	Shift Supervisor Plant Manager COO
Managerial accounting	Cost center	Profit center

Corporate boards, executives and officers are awakening to the challenges securing the operational technology (OT) systems that run their factories, support local economies, and undergird modern societies.

Failure to appreciate the IT-OT gap can hamper effective and sustainable approaches to industrial cybersecurity. The Industrial Cybersecurity Awakening Model describes the stages many organizations pass through as their OT security efforts mature. The materials in this guide helps shift management mentality towards Stage 5.

Industrial Cybersecurity Awakening Model

	STAGE 1	STAGE 2	STAGE 3	STAGE 4	STAGE 5
Management mentality	**External consultants** "Get someone in here before that happens again."	**Allocated budget** "Here's some money to go make us secure."	**Appropriate technology** "Technology will help IT security staff cover OT too."	**Industrial cybersecurity program** "Let's do this right by following the guidance."	**Industrial cybersecurity team** **"Let's build a team to make this sustainable."**
	6 months	1 year	2 years	3 years	4 years

WHAT DOES YOUR INDUSTRIAL CYBERSECURITY TEAM **NEED TO KNOW**?

A group of 14 industrial cybersecurity subject matter experts representing 88 years of industrial experience, 32 years of cybersecurity experience, and 31 years of industrial cybersecurity experience convened by Idaho National Laboratory (INL) and Idaho State University (ISU) identified six industrial cybersecurity knowledge domains and associated content not normally covered in cybersecurity training and education.

Industrial and Cybersecurity Knowledge Domains

Industrial Knowledge

- Industrial operations
- Instrumentation and control
- Equipment
- Communications
- Safety
- Regulation

+

Cybersecurity Knowledge

- Data
- Software
- Component
- Connection
- System
- Human, organizational and societal

Industrial knowledge domain content:

Industrial operations and processes: industry sectors, professional roles and responsibilities in industrial environments, engineering diagrams, process types, plant lifecycle.

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.

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

Industrial communications: reference architectures, industrial communications protocols, fieldbuses.

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

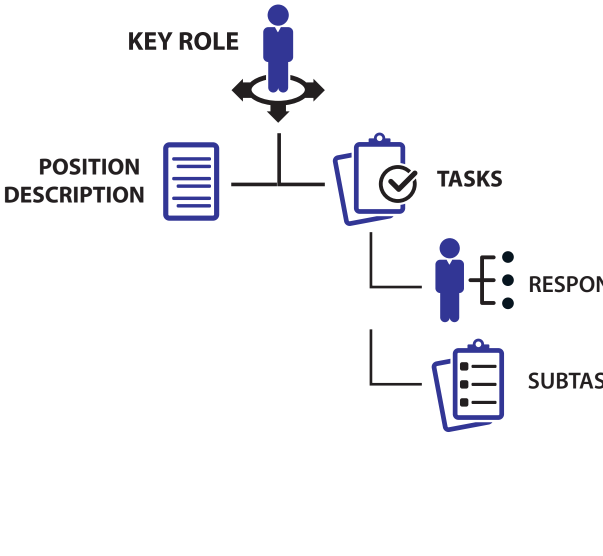
Regulation and guidance: presidential/executive orders, NIST SP 800-82 R2, IEC 62443, NERC CIP.

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

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

HOW DO YOU STRUCTURE AN INDUSTRIAL CYBERSECURITY TEAM?

Managers seeking to build an industrial cybersecurity team may rely on human resource development models (as exampled below) to plan to meet organizational needs. This guide was developed to adhere to the following role-based workforce development structure. It presents the key role, position description, and tasks.



The **job role** should be the primary component to organizing your workforce.

KEY ROLES OF THE TEAM

ENGINEER
Design safe and secure industrial systems.

ANALYST
Synthesize threat and vulnerability information.

MANAGER
Direct and oversee industrial cybersecurity program.

TECHNICIAN
Assure security and safety of ICS operations.

RESEARCHER
Identify new vulnerabilities to achieve kinetic consequences.

WHAT DOES YOUR INDUSTRIAL CYBERSECURITY TEAM **NEED TO DO**?

MANAGER

An Industrial Cybersecurity manager is responsible to direct and oversee the work of industrial cybersecurity for all phases of the plant, product and system lifecycles. The manager interfaces continuously with operations, IT, and cybersecurity personnel.

MANAGER PRIMARY TASKS

- Prioritize efforts
- Understand requirements per effort
- Obtain and manage budget
- Build the team
- Run and improve the program.

Qualifications and Certifications

- Master of Business Administration
- Project Management
- Information systems security
- Licensed Professional Engineer
- Industrial cybersecurity.

HIRING GUIDANCE

☐ Ideal candidate has project management experience in cybersecurity AND engineering.

☐ One senior manager per strategic business unit.

☐ Intimately familiar with industrial cybersecurity good practice guidance.

☐ Comfortable in both corporate offices and industrial environments.

☐ Compliance and audit experience desired.

☐ Capable of keeping the big picture in mind while not afraid of technical details.

ENGINEER

The Industrial Cybersecurity engineer works within the engineering department to design and create systems, processes and procedures that maintain the safety, reliability, controllability and security of industrial systems in the face of intentional and incidental cyber events. Interfaces with Chief Information Security Officer, plant managers and industrial cybersecurity technicians.

ENGINEER PRIMARY TASKS

- Direct creation of industrial systems inventory and model for cybersecurity purposes
- Design physical failsafes to counteract potential cybersabotage
- Advise development and operation of security operations center relative to the industrial environment
- Recommend security techniques, technologies, and approaches for adoption in industrial environment
- Create cybersecurity inspection and test procedures for industrial systems
- Review industrial system engineering plans and documentation for cybersecurity concerns
- Review proposed cybersecurity policies and procedures related to industrial environments; and equipment and software based on cybersecurity criteria
- Optimize industrial system designs for security effectiveness and efficiency.

Qualifications and Certifications

- Master of Science in Electrical, Mechanical, or Computer Engineering
- Licensed Professional Engineer
- Industrial automation
- Information systems security.

HIRING GUIDANCE

☐ **Most important role on the industrial cybersecurity team and may require skilled recruitment.**

☐ Requires 5 or more years of engineering experience in each of industrial automation, information technology, and cybersecurity.

☐ Demonstrates expert level familiarity with industrial safety and cybersecurity events including detailed root-cause analysis.

☐ Deep engineering experience and expertise and is capable of considering the mindset of a well-resourced adversary.

☐ Demonstrates proficiency in systems thinking and systems design, including production of policies, diagrams, drawings, and specifications.

☐ *For Team: One or two per facility or per type of facility.*

TECHNICIAN

The Industrial Cybersecurity Technician works among plant operations personnel to assure safety, reliability, functionality and cybersecurity of industrial control systems during installation, monitoring, troubleshooting, and restoration of industrial process operations.

TECHNICIAN PRIMARY TASKS

- Maintains ICS device asset inventory for security purposes
- Reviews architecture of ICS networks
- Updates ICS software and firmware during stoppages
- Maintains backups of control software
- Maintains awareness of evolving threat environment
- Securely implements process control equipment.

HIRING GUIDANCE

□ Demonstrates fascination and enthusiasm for knowing how things work.

□ Demonstrates hands-on experience with industrial automation equipment.

□ Demonstrates proficiency in safe work procedures.

□ Provides technical experience and builds relationships that provide a fantastic foundation for all the other cybersecurity roles.

□ Possess proficient IT and OT terminology and cultures to enable communications across the IT-OT gap.

□ Understands common security weaknesses in OT environments.

□ *For Team: At least one per facility.*

Qualifications and Certifications

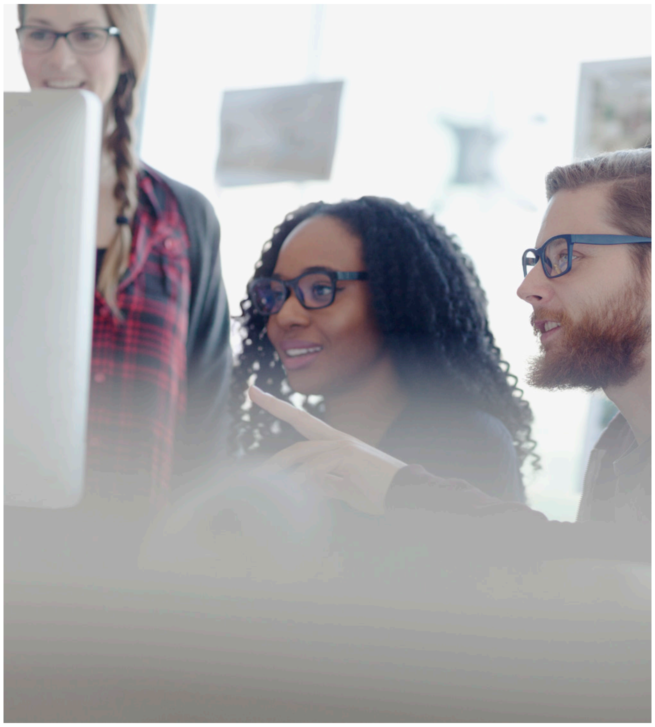
- Associate or Bachelor of Applied Science in Engineering Technology
- Control Systems Technician
- Industrial cybersecurity
- Basic networking
- Basic security.

ANALYST

The Industrial Cybersecurity Analyst works among enterprise cybersecurity personnel to contextualize and synthesize threats, vulnerabilities and consequences relevant to industrial environments to provide strategic, tactical, and operational decision makers with perspective, options, and recommendations. The analyst works with industrial operations personnel to gain perspective and vet practicality of possible courses of action.

ANALYST PRIMARY TASKS

- Stays abreast emerging developments relevant to industrial cybersecurity
- Dissects analytical requests
- Collects information
- Synthesizes information
- Analyzes threats, vulnerabilities and consequences pertinent to industrial environments
- Produces analytical products
- Proposes new work.



HIRING GUIDANCE

□ Enjoys the professional writing process.

□ Reads insatiably.

□ Does not shy away from potentially controversial topics.

□ Presents compelling arguments in written and verbal form.

□ Has developed deep expertise in various subject areas.

□ Works well with other analytical thinkers, and appreciates constructive critique.

□ Never completely satisfied with work product.

□ Quickly and accurately describes the threat environment pertinent to a given organization.

Qualifications and Certifications

- Bachelor of Science or Arts in various fields
- Coursework in intelligence and analysis
- Cybersecurity certifications
- Military intelligence training
- Data visualization.

RESEARCHER

The Industrial Cybersecurity Researcher works to increase detailed knowledge about ways an industrial cyber-physical system may be compromised, and advance novel ways they may be protected. The researcher employs specific tools and techniques suited to their assignment, and often works alone, but engages expert-level resources as necessary. Reports must meet standards for clarity of technical content.

RESEARCHER PRIMARY TASKS

- Describes and characterizes systems
- Designs and conducts tests
- Discovers vulnerabilities
- Develops adversarial perspective
- Recommends mitigations
- Documents and reports findings.

HIRING GUIDANCE

□ Thrives when working with technology.

□ Must be capable of explaining and defending their findings.

□ May enjoy technology interaction outside of work hours.

□ Shares findings and techniques with other researchers.

Qualifications and Certifications

- Bachelor or Master of Science in computer science
- Technical track presentations at security conferences
- Publicly referenced vulnerability disclosures
- Authored security-related tools.

INDUSTRIAL CYBERSECURITY WORKFORCE **METHODOLOGY**

To create this document, INL collaborated with ISU and La Trobe University in a two-phase project.

In **Phase I**, INL sent 14 subject matter experts to Idaho State University's Simplot Decision Support Center (SDSC) with the objective of creating a framework for developing industrial cybersecurity training and education standards. The SDSC is an in-person electronic meeting room designed to implement the nominal group technique for decision making – the same facility and technique that the federal government used repeatedly between 1987 and 2005 to create the first federal cybersecurity training and education standards (NSTISS/CNSS Instructions 4011-4016).

For **Phase II**, INL identified 10 additional collaborators (two per role) with significant experience in each role. The collaborators described tasks each role performs relevant to industrial cybersecurity. The task statements were then consolidated into the primary task lists provided in this document.

LIMITATIONS

In applying the archetype roles and tasks describd herein, orgainzations should consider them notionally prescriptive rather than specifically prescriptive.

FUTURE WORK

Identifying the unique knowledge and job roles required of industrial cybersecurity professionals represents a significant step towards developing a capable workforce. The subject collaborators have noted that there is an ongoing need to establish a repository of knowledge, skills, attitudes, and behaviors on which diverse groups can rely to create training and education standards, personalized training plans, intervention methods, and training content. Their intentions are to use surveys, interviews, and field observations to expand, further validate, and refine the results.

Future deliverables include an Human Resources Guide and a Career Development Guide for Industrial Cybersecurity.

REFERENCES

S. McBride, J. Slay "Towards Standards-Based Industrial Control Systems Security Education in The United States" (2020). https://industrialcyberforce.org/wp-content/uploads/2020/07/Towards-Standards-based-ICS-Security-Education-in-the-United-States.pdf

S. McBride, J. Slay "Criteria for International ICS Security Education Standards" (2020). https://industrialcyberforce.org/wp-content/uploads/2020/07/Criteria-for-International-ICS-Security-Education-Standards.pdf

S. McBride, C. Schou, J. Frost, J. Slay "An Initial Industrial Cybersecurity Workforce Development Framework" (2020). https://industrialcyberforce.org/wp-content/uploads/2020/08/An-Initial-Industrial-Cybersecurity-Workforce-Development-Framework.pdf

S. McBride, J. Slay, C. Schou "A Security Workforce to Bridge the IT-OT Gap" (2020). https://industrialcyberforce.org/wp-content/uploads/2020/08/A-Security-Workforce-to-Bridge-the-IT-OT-Gap.pdf.

For more information, visit:

INL's National and Homeland Security's Training and Workforce Development Center at https://inl.gov/critical-infrastructure-protection-training/

Idaho State University College of Technology at https://www.isu.edu/industrialcybersecurity/