Industry Workforce Solutions

PREPARING THE OIL, GAS, AND ENERGY SUPPLY CHAIN

Advancing Diversity by Implementing Cybersecurity Standards

IWS
9800 Connecticut Drive
Crown Point, IN 46307
www.IndustryWorkforceSolutions.com

Preparing the Oil, Gas, and Energy Supply Chain

By Dr. Jan Fourman, PhD, EdD, MBA, MRA, RAC, CSSBB

In the gas, oil and energy supply chain, the number of women and minority owned suppliers and startups is lacking. For example, the following are facts about the gas, oil, and energy workforce diversity from the NASEO 2021 report.

Issues:

- **"BELOW-AVERAGE PROPORTION OF WOMEN IN THE WORKFORCE" (NASEO, 2021, P. 5)**
- **"BELOW-AVERAGE REPRESENTATION OF HISPANIC OR LATINX WORKERS AND BLACK OF AFRICAN AMERICAN WORKERS" (NASEO, 2021, P. 5)**
- **"BLACK OR AFRICAN AMERICAN WORKERS ARE UNDERREPRESENTED ACROSS ENERGY TECHNOLOGY AND ENERGY SOURCE SECTORS" (NASEO,2021, P. 5)**
- **"WOMEN REPORT LOWER AWARENESS OF CAREER NAVIGATION SUPPORT COMPARED TO MEN" (NASEO, 2021, P. 9)**
- **"HEALTHCARE COVERAGE FOR ENERGY WORKERS VARIES BY RACE AND ETHNICITY" (NASEO, 2021, P.9)**

How to Create a Solution

IWS is preparing the gas, oil, and energy industry with qualified supply chain vendors. We understand that the management operations systems for this industry is complex. Therefore, we have carefully planned a cybersecurity program tailored for the gas, oil, and energy sectors. This program is called the CyberReadyMBE program.

It has been developed by our experts to meet the management systems and cybersecurity requirements of gas, oil and energy suppliers and vendors. Benefits of the program include:

Why the Solution is Effective

- Skilling-up women and minority owned businesses to meet international best practices and credentialing important to the gas, oil, and energy.
- Providing a CyberReadyMBE badge of which requirements align with NIST CMMC Level1 and ISA/IEC 62443 cybersecurity principles.
- Ensuring cybersecurity instruction that aligns with cyber best practices in ISO 14001 Environmental Management Systems, ISO 45001 Occupational Health, ISO 50001 Energy, and Sarbanes-Oxley.
- Approaching management system solutions for a holistic viewpoint that combines the best practices of international standards, and legal requirements.
- Buy in from leadership means the CyberReadyMBE program has sustainable, comprehensive information, but also flexible enough to allow for unique skill sets.

IWS has a team of cyber experts in the three essential controls for effective cybersecurity vendor supply – managerial, operational, and technical. These controls are essential behind any organization's security process (Whitman & Mattord, 2022). Using these controls and the NIST CMMC Level 1, and ISA 62443 cyber principles as the foundation the CyberReadyMBE program.

Managerial control. IWS instructs this control with emphasis on leadership that drives performance. Especially performance directed to startup operations, and managing to adaptations that happen with construction and maintenance.

Operational control. The operational control parts of a gas, oil and energy cyber policy need to cover short-term operations and processes. This is meant to establish that the operational controls are consistent with established policy language. For the gas, oil and energy industry, IWS instructs our CyberReadyMBE participants to provide their organizations needed information on proactiveness and scheduled operational maintenance. We build on our participants' operating experiences as well, to ensure learning that can be directly applied to effective delivery of projects and compliance metrics.

Technical control. The technical control part of our program centers around security controls. These are the safeguards or countermeasures that are implemented and executed by mechanisms contained in the hardware, software, or firmware parts of the information system (NIST, 2023).

The result is a program that includes an introduction to cyber readiness, protocols of cyber readiness by industry sector, how to identify workforce needs for cybersecurity, requirements for doing business with corporations and government, and matchmaking new capabilities with corporate and federal buyers.

One important feature of the CyberReady MBE program is its emphasis on risk assessment, management, and mitigation. IWS understands that risk strategies are imperative in today's world of cyberthreats. We include tools to assess and quantify potential inherent and residual operational risks (Whitman & Mattord, 2019).

Where the Solution Works

To build the curriculum for the CyberReadyMBE program, the team has used the following foundational documentation – NIST SP 800-171 (Rev 2), NIST 800-172, NIST SP 800-161, NIST SP 800-18 (Rev 1), NIST SP 800-37 (Rev 2), NIST SP 800-53 (Rev 4), NIST SP 800-82 (Rev.2). As well as the ISO, and ISA/IEC standards, and legal financial regulations.

Upon completion of the CyberReadyMBE program, the women and minority owned businesses are ready to be preferred gas, oil and energy vendors as they have satisfied the following program objectives:

- Know what basic cyber hygiene is
- Recognize what cyber security controls are
- Identify the basics of cyber security domains and principles:
    1. Access Control
    2. Identification and Authentication
    3. Media Protection
    4. Physical Protection
    5. System and Communication Protection
    6. System and Information Integrity
    7. Know the basics of seventeen cyber security practices:
    8. Authorized Access Control
    9. Transaction and Function Control
    10. External Connection

11. Control Public Information
12. Identification
13. Authentication
14. Media Disposal
15. Limit Physical Access
16. Escort Visitors
17. Physical Access Logs
18. Manage Physical Access
19. Boundary Protection
20. Public-Access System Separation
21. Flaw Remediation
22. Malicious Code Protection
23. Update Malicious Code

- Understand Industry Sectors and Cybersecurity Responsibilities
- Knowledge to write a System Security Plan (SSP)
- Realize security risk assessment for system design
- Recognize system security requirements and security levels

Program Mapping to ISO Standards and Sarbanes-Oxley

We align with ISO 14001 Environmental Management System as shown in the mapping to the CMMC Level 1 principles and the CyberReadyMBE program content.

Section of ISO 14001	Mapping to CMMC Level 1	CyberReadyMBE Content
Section 4 – Content of Organization	• AC. L1-3.1.1 - Authorized Access Control • AC. L1-3.1.20 - External Connections • AC. L1-3.1.22 - Control Public Information • IA. L1-3.5.1 - Identification • IA. L1-3.5.2 - Authentication • SC. L1-3.13.1 - Boundary Protection • SC. L1-3.13.5 - Public-Access System Separation	• Module 1 Chapter 2 – Understanding Cyber Hygiene • Module 1 Chapter 3 – Alignment by Industry Sector • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness
Section 5 - Leadership	• AC. L1-3.1.1 - Authorized Access Control • AC. L1-3.1.2 - Transaction and Function • MP. L1-3.8.3 - Media Disposal • SC. L1-3.13.1 - Boundary Protection • SC. L1-3.13.5 - Public-Access System Separation	• Module 1 Chapter 2 – Understanding Cyber Hygiene • Module 1 Chapter 4 – Need for a Cybersecurity Gap Assessment • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness

Section 6 - Planning	• AC. L1-3.1.20 - External Connections • AC. L1-3.1.22 - Control Public Information • IA. L1-3.5.1 - Identification • IA. L1-3.5.2 - Authentication • PE. L1-3.10.1 - Limit Physical Access • PE. L1-3.10.5 - Control and Manage Physical Access	• Module 1 Chapter 2 – Understanding Cyber Hygiene • Module 1 Chapter 3 – Alignment by Industry Sector • Module 1 Chapter 4 – Need for a Cybersecurity Gap Assessment • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness • Module 4 Chapter 1 – Building your Capability Statement
Section 7 - Support	• IA. L1-3.5.1 - Identification • IA. L1-3.5.2 - Authentication • SI. L1-3.14.1 - Flaw Remediation • SI. L1-3.14.4 - Update Malicious Code • SI. L1-3.14.5 - System and File Scanning • PE. L1-3.10.5 - Manage Physical Access • SC. L1-3.13.1 - Boundary Protection • SC. L1-3.13.5 - Public-Access System Separation	• Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness • Module 5 – Being Cyber Ready and doing Business with Corporations
Section 8 - Operation	• AC. L1-3.1.1 - Authorized Access Control • AC. L1-3.1.2 - Transaction and Function • AC. L1-3.1.20 - External Connections • IA. L1-3.5.1 - Identification • IA. L1-3.5.2 - Authentication • SI. L1-3.14.4 - Update Malicious Code • PE. L1-3.10.5 - Manage Physical Access • SC. L1-3.13.1 - Boundary Protection • SC. L1-3.13.5 - Public-Access System Separation	• Module 1 Chapter 4 – Need for a Cybersecurity Gap Assessment • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness • Module 4 Chapter 1 – Building your Capability Statement • Module 5 – Being Cyber Ready and Doing Business with Corporations
Section 9 – Performance Evaluation	• SI. L1-3.14.1 - Flaw Remediation • SI. L1-3.14.4 - Update Malicious Code • SI. L1-3.14.5 - System and File Scanning • PE. L1-3.10.1 - Limit Physical Access • PE. L1-3.10.5 - Control and Manage Physical Access • SC. L1-3.13.1 - Boundary Protection	• Module 1 Chapter 2 – Understanding Cyber Hygiene • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness
Section 10 - Improvement	• SI. L1-3.14.4 - Update Malicious Code • SI. L1-3.14.5 - System and File Scanning	• Module 1 Chapter 4 – Need for a Cybersecurity Gap Assessment

	• PE. L1-3.10.5 - Manage Physical Access • SC. L1-3.13.1 - Boundary Protection • SC. L1-3.13.5 - Public-Access System Separation	• Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness • Module 4 Chapter 1 – Building your Capability Statement • Module 5 – Being Cyber Ready and Doing Business with Corporations

We have mapped ISO Occupational Health and Safety to the NIST CMMC Level 1 cybersecurity principles, which are part of our instruction. The program content has also been mapped to ISO 45001 and CMMC Level1.

Section of ISO 45001	Mapping to CMMC Level 1	CyberReadyMBE Content
Section 4 – Content of Organization	• AC. L1-3.1.20 - External Connections • AC. L1-3.1.22 - Control Public Information • SC. L1-3.13.1 - Boundary Protection • SC. L1-3.13.5 - Public-Access System Separation	• Module 1 Chapter 2 – Understanding Cyber Hygiene • Module 1 Chapter 3 – Alignment by Industry Sector • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness
Section 5 - Leadership	• SI. L1-3.14.2 - Malicious Code Protection • SI. L1-3.14.4 - Update Malicious Code • SC. L1-3.13.1 - Boundary Protection • SC. L1-3.13.5 - Public-Access System Separation	• Module 1 Chapter 2 – Understanding Cyber Hygiene • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness
Section 6 - Planning	• AC. L1-3.1.1 - Authorized Access Control • AC. L1-3.1.2 - Transaction and Function • IA. L1-3.5.1 - Identification • IA. L1-3.5.2 - Authentication • SC. L1-3.13.1 - Boundary Protection • SC. L1-3.13.5 - Public-Access System Separation	• Module 1 Chapter 2 – Understanding Cyber Hygiene • Module 1 Chapter 4 – Need for a Cybersecurity Gap Assessment • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness
Section 7 - Support	• AC. L1-3.1.1 - Authorized Access Control • AC. L1-3.1.20 - External Connections	• Module 1 Chapter 2 – Understanding Cyber Hygiene

	• PE. L1-3.10.1 - Limit Physical Access • PE. L1-3.10.3 - Escort Visitors • SC. L1-3.13.1 - Boundary Protection • SC. L1-3.13.5 - Public-Access System Separation	• Module 1 Chapter 3 – Alignment by Industry Sector • Module 1 Chapter 4 – Need for a Cybersecurity Gap Assessment • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness • Module 4 Chapter 1 – Building your Capability Statement
Section 8 - Operation	• AC. L1-3.1.20 - External Connections • AC. L1-3.1.22 - Control Public Information • SI. L1-3.14.2 - Malicious Code Protection • SI. L1-3.14.4 - Update Malicious Code • SI. L1-3.14.5 - System and File Scanning • PE. L1-3.10.5 - Manage Physical Access • SC. L1-3.13.1 - Boundary Protection • SC. L1-3.13.5 - Public-Access System Separation • SC. L1-3.13.5 - Public-Access System Separation	• Module 1 Chapter 3 – Alignment by Industry Sector • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness
Section 9 – Performance Evaluations	• SI. L1-3.14.1 - Flaw Remediation • SI. L1-3.14.5 - System and File Scanning • PE. L1-3.10.4 - Physical Access Logs • PE. L1-3.10.5 - Control and Manage Physical Access	• Module 1 Chapter 2 – Understanding Cyber Hygiene • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness
Section 10 - Improvement	• SI. L1-3.14.1 - Flaw Remediation • SI. L1-3.14.5 - System and File Scanning • PE. L1-3.10.4 - Physical Access Logs • SC. L1-3.13.1 - Boundary Protection • SC. L1-3.13.5 - Public-Access System Separation	• Module 1 Chapter 4 – Need for a Cybersecurity Gap Assessment • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness • Module 4 Chapter 1 – Building your Capability Statement • Module 5 – Being Cyber Ready and Doing Business with Corporations

We have mapped ISO 50001 Energy Management System to the CMMC Level 1 practices below.

Section of ISO 50001	Mapping to CMMC Level 1	CyberReadyMBE Content
Section 4 – Content of Organization	• AC. L1-3.1.1 - Authorized Access Control • AC. L1-3.1.20 - External Connections	• Module 1 Chapter 2 – Understanding Cyber Hygiene

	• AC. L1-3.1.22 - Control Public Information • SC. L1-3.13.1 - Boundary Protection • SC. L1-3.13.5 - Public-Access System Separation	• Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness
Section 5 - Leadership	• AC. L1-3.1.2 - Transaction and Function • SI. L1-3.14.1 - Flaw Remediation • SC. L1-3.13.1 - Boundary Protection • SC. L1-3.13.5 - Public-Access System Separation	• Module 1 Chapter 2 – Understanding Cyber Hygiene • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness • Module 5 – Being Cyber Ready and Doing Business with Corporations
Section 6 - Planning	• IA. L1-3.5.1 - Identification • IA. L1-3.5.2 - Authentication • PE. L1-3.10.1 - Limit Physical Access • PE. L1-3.10.4 - Physical Access Logs • PE. L1-3.10.5 - Control and Manage Physical Access	• Module 1 Chapter 4 – Need for a Cybersecurity Gap Assessment • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness • Module 5 – Being Cyber Ready and Doing Business with Corporations
Section 7 - Support	• SI. L1-3.14.1 - Flaw Remediation • SI. L1-3.14.2 - Malicious Code Protection • SI. L1-3.14.4 - Update Malicious Code • SC. L1-3.13.1 - Boundary Protection • SC. L1-3.13.5 - Public-Access System Separation	• Module 1 Chapter 4 – Need for a Cybersecurity Gap Assessment • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness • Module 4 Chapter 1 – Building your Capability Statement • Module 5 – Being Cyber Ready and Doing Business with Corporations
Section 8 - Operation	• AC. L1-3.1.20 - External Connections • AC. L1-3.1.22 - Control Public Information • SI. L1-3.14.5 - System and File Scanning • PE. L1-3.10.5 - Manage Physical Access • SC. L1-3.13.1 - Boundary Protection	• Module 1 Chapter 2 – Understanding Cyber Hygiene • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness

	• SC. L1-3.13.5 - Public-Access System Separation	• Module 4 Chapter 1 – Building your Capability Statement • Module 5 – Being Cyber Ready and Doing Business with Corporations
Section 9 – Performance Evaluation	• SI. L1-3.14.1 - Flaw Remediation • SI. L1-3.14.4 - Update Malicious Code • SI. L1-3.14.5 - System and File Scanning	• Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness • Module 5 – Being Cyber Ready and doing Business with Corporations
Section 10 - Improvement	• SI. L1-3.14.1 - Flaw Remediation • SI. L1-3.14.5 - System and File Scanning • PE. L1-3.10.4 - Physical Access Logs • SC. L1-3.13.1 - Boundary Protection • SC. L1-3.13.5 - Public-Access System Separation	• Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness • Module 5 – Being Cyber Ready and doing Business with Corporations

We align Sarbanes-Oxley with CMMC Level 1 principles and the CyberReadyMBE program content (SEC, 2020).

Titles of Sarbanes-Oxley	Key Points of Title	Mapping to CMMC Level 1	CyberReadyMBE Content
Public Company Accounting Oversight Board	• Intended to provide independent oversight of public accounting firms, and to provide audit services • Created a central oversight board tasked with registering auditors, defining the specific processes and procedures for compliance audits, inspecting and policing conduct and quality control, and enforcing compliance with the specific mandates of SOX	• AC. L1-3.1.22 - Control Public Information • PE. L1-3.10.4 - Physical Access Logs • SC. L1-3.13.1 - Boundary Protection • SC. L1-3.13.5 - Public-Access System Separation	• Module 1 Chapter 2 – Understanding Cyber Hygiene • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness • Module 5 – Being Cyber Ready and Doing Business with Corporations
Auditor Independence	• Stresses auditor independence so there is no conflict of interest • Auditors cannot do business other than auditing with their clients	• PE. L1-3.10.1 - Limit Physical Access • PE. L1-3.10.3 - Escort Visitors	• Module 1 Chapter 2 – Understanding Cyber Hygiene • Modules 2 – Fundamentals of Cybersecurity Readiness

		• PE. L1-3.10.5 - Manage Physical Access • SC. L1-3.13.1 - Boundary Protection • SC. L1-3.13.5 - Public-Access System Separation	• Modules 3 – Workforce Capabilities and Readiness • Module 5 – Being Cyber Ready and Doing Business with Corporations
Corporate Responsibility	• Senior executives take responsibilities for the accuracy and completeness of financial records • If there is a problem, the CFO could face forfeitures of benefits and civil penalties	• AC. L1-3.1.1 - Authorized Access Control • AC. L1 – 3.1.2 - Transaction and Function • AC. L1 – 3.1.20 - External Connections • AC. L1 – 3.1.22 - Control Public Information • IA. L1-3.5.1 - Identification • IA. L1-3.5.2 - Authentication	• Module 1 Chapter 2 – Understanding Cyber Hygiene • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness
Enhanced Financial Disclosures	• Requires internal controls for assuring the accuracy of financial reports and disclosures • Requires audits and reports on those controls • Requires these reports to be available in a timely manner	• IA. L1-3.5.1 - Identification • IA. L1-3.5.2 - Authentication • SI. L1-3.14.1 - Flaw Remediation • SI. L1-3.14.5 - System and File Scanning • PE. L1-3.10.4 - Physical Access Logs	• Module 1 Chapter 4 – Need for a Cybersecurity Gap Assessment • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness • Module 4 Chapter 1 – Building your Capability Statement • Module 5 – Being Cyber Ready and Doing Business with Corporations
Analysts Conflict of Interest	• Intended to restore investor confidence in the reporting of securities analysis • Defines the codes of conduct for securities analysts and requires disclosure of knowledgeable conflicts of interest	• AC. L1-3.1.1 - Authorized Access Control • AC. L1 – 3.1.2 - Transaction and Function • AC. L1 – 3.1.20 - External Connections • AC. L1 – 3.1.22 - Control Public Information • IA. L1-3.5.1 - Identification	• Module 1 Chapter 2 – Understanding Cyber Hygiene • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness

		• IA. L1-3.5.2 - Authentication	
Commission Resources and Authority	• Defines practices to restore investor confidence in securities analysts • Defines the conditions under which a person can be barred from practicing as a broker, advisor or dealer	• AC. L1 – 3.1.22 - Control Public Information • IA. L1-3.5.1 - Identification • IA. L1-3.5.2 - Authentication • SC. L1-3.13.1 - Boundary Protection • SC. L1-3.13.5 - Public-Access System Separation	• Module 1 Chapter 4 – Need for a Cybersecurity Gap Assessment • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness • Module 4 Chapter 1 – Building your Capability Statement • Module 5 – Being Cyber Ready and Doing Business with Corporations
Studies and Reports	• Controller General and the SEC to perform various studies and report their findings • These reports include: ○ Effects of consolidation of public accounting firms ○ The role of credit rating agencies in the operation of securities markets ○ Securities violations ○ Enforcement actions ○ Whether investment banks assist others to manipulate earnings and obfuscate true financial conditions	• IA. L1-3.5.1 - Identification • IA. L1-3.5.2 - Authentication	• Module 1 Chapter 2 – Understanding Cyber Hygiene • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness • Module 5 – Being Cyber Ready and Doing Business with Corporations
Corporate and Criminal Fraud Accountability	• Describes criminal penalties for manipulation, destruction or adulteration of financial records • No interference for investigations	• IA. L1-3.5.1 - Identification • IA. L1-3.5.2 - Authentication • SI. L1-3.14.1 - Flaw Remediation • SI. L1-3.14.2 - Malicious Code Protection • SI. L1-3.14.4 - Update Malicious Code • SI. L1-3.14.5 - System and File Scanning	• Module 1 Chapter 2 – Understanding Cyber Hygiene • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness • Module 5 – Being Cyber Ready and Doing Business with Corporations
White Collar Crime Penalty Enhancement	• Increases the criminal penalties associated	• IA. L1-3.5.1 - Identification	• Module 1 Chapter 2 – Understanding Cyber Hygiene

	with white collar crimes and conspiracies	• IA. L1-3.5.2 - Authentication • PE. L1-3.10.3 - Escort Visitors • SI. L1-3.14.2 - Malicious Code Protection • SI. L1-3.14.4 - Update Malicious Code • SI. L1-3.14.5 - System and File Scanning	• Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness • Module 5 – Being Cyber Ready and Doing Business with Corporations
Corporate Tax Returns	• Chief executive officer should sign the company tax return	• IA. L1-3.5.1 - Identification • IA. L1-3.5.2 - Authentication • SI. L1-3.14.2 - Malicious Code Protection • SI. L1-3.14.4 - Update Malicious Code • SI. L1-3.14.5 - System and File Scanning	• Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness • Module 4 Chapter 1 – Building your Capability Statement • Module 5 – Being Cyber Ready and Doing Business with Corporations
Corporate Fraud Accountability	• Creates the crime of obstructing an official proceeding • Identifies corporate fraud and records tampering as criminal offenses	• IA. L1-3.5.1 - Identification • IA. L1-3.5.2 - Authentication • PE. L1-3.10.3 - Escort Visitors • SI. L1-3.14.2 - Malicious Code Protection • SI. L1-3.14.4 - Update Malicious Code • SI. L1-3.14.5 - System and File Scanning	• Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness • Module 4 Chapter 1 – Building your Capability Statement • Module 5 – Being Cyber Ready and Doing Business with Corporations
Obstructing an Official Proceeding	• Evidence tampering is a crime • Obstructing justice is a crime	• IA. L1-3.5.1 - Identification • IA. L1-3.5.2 - Authentication • PE. L1-3.10.3 - Escort Visitors • SC. L1-3.13.1 - Boundary Protection • SC. L1-3.13.5 - Public-Access System Separation	• Module 1 Chapter 2 – Understanding Cyber Hygiene • Modules 2 – Fundamentals of Cybersecurity Readiness • Modules 3 – Workforce Capabilities and Readiness • Module 5 – Being Cyber Ready and

			Doing Business with Corporations

In Conclusion

This document provides an overview of the CyberReadyMBE program and how it prepares women and minority owned businesses to be preferred vendors and participants of the gas, oil, and energy sector supply chain. The program is built on cybersecurity principles taken from NIST, ISO and ISA/IEC62443 standards and legal requirements like Sarbanes-Oxley. This program is fostering cyber flexible organization for the gas, oil, and energy future.

For information about the CyberReadyMBE program, contact D. Gonzalez-Gaboyan at dgaboyan@industryworkforcesolutions.com

About the Author

Dr. Jan Fourman serves as the chief advisor in workforce, risk assessment and curriculum development for Industry Workforce Solutions.

She is an expert in program development for quality compliance, risk mitigation assessment, and Six Sigma strategies for pharmaceutical, medical device and other manufacturing organizations.

To name a few, she has consulted for the Food and Drug Association (FDA), International Standards Organization (ISO), Environmental Protection Authority (EPA), National Institute of Standards and Technology (NIST), National Institute for Occupational Safety and Health (NIOSH), and the National Institute of Health (HIH).

Jan has worked in the pharmaceutical and medical device industry in therapeutics, manufacturing, quality, and cybersecurity. She also has experience in project management, metric collection, and data analysis, and is a Six Sigma Black Belt.

In the pharmaceutical industry, there are strict statutory and regulatory standards that must be met to ensure quality of drugs and medical devices. To remain compliant with those standards, the industry relies upon experts like Jan, who consult with organizations the methods to mitigate risk and remain compliant. In addition, she is a certified auditor in ISO 9001 and ISO 13485.

References

CMMC. (2021). Cybersecurity maturity model certification (CMMC) model overview (Version 2). Carnegie

NASEO. (2021). Diversity in the US energy workforce: Data findings to inform state energy, climate, and workforce development policies and programs. Retrieved from www.naseo.org/

NIST. (2023). Technical controls. CSRC. Retrieved from www.csrc.gov/glossary/term/technical.controls/

SEC. (2020). The laws that govern the securities industry. Retrieved from www.sec.gov/
Whitman, M.E., & Mattord, H.J. (2019). Management of information security (6th Ed.). Boston, MA: Cengage.