DEFENSE-IN-DEPTH: CYBERSECURITY IN THE NATURAL GAS & OIL INDUSTRY

OIL AND NATURAL GAS SECTOR COORDINATING COUNCIL

NATURAL GAS COUNCIL

“Defense-in-Depth: Cybersecurity in the Natural Gas and Oil Industry” is a product of the Oil and Natural Gas Subsector Coordinating Council (ONG SCC) and Natural Gas Council (NGC).

MEMBER ORGANIZATIONS:

American Exploration & Production Council
American Fuel & Petrochemical Manufacturers
American Gas Association
American Petroleum Institute
American Public Gas Association
Association of Oil Pipe Lines
Energy Security Council
Gas Processors Association
Independent Petroleum Association of America
International Association of Drilling Contractors
International Liquid Terminals Association
Interstate Natural Gas Association of America
National Association of Convenience Stores
National Ocean Industries Association
National Propane Gas Association
Natural Gas Supply Association
Offshore Marine Service Association
Offshore Operators Committee
Petroleum Marketers Association of America
Society of Independent Gas Marketers Association
Texas Oil & Gas Association
U.S. Oil & Gas Association

DEFENSE-IN-DEPTH:

CYBERSECURITY IN THE NATURAL GAS & OIL INDUSTRY

OIL AND NATURAL GAS SECTOR COORDINATING COUNCIL

NATURAL GAS COUNCIL

TABLE OF CONTENTS

FOREWORD

REGARDING QUESTIONS ON PIPELINE RELIABILITY AND RESILIENCY

Various federal agencies have stated or represented that natural gas pipelines are more vulnerable to cyberattacks than other energy infrastructure. These statements are not based on evidence and have not been substantiated. Threats are shared by the Intelligence Community to cybersecurity experts from natural gas and oil companies, the Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC) and the Downstream Natural Gas Information Sharing and Analysis Center (DNG-ISAC) on an ongoing basis, and threat mitigations continue to be incorporated into the cybersecurity programs of companies in the natural gas sector.

There is a misconception between cyber threats and vulnerabilities in the calculation of risk to natural gas pipelines. Companies operating these pipelines are continuously reducing their vulnerability through work with the U.S. Government to evolve their defensive posture inside the methods and frameworks outlined in this paper. Most, if not all, of the largest industry companies – including natural gas pipeline operators – manage cybersecurity as an enterprise risk – the highest designation – with oversight from Boards of Directors and Senior Executives.

Natural gas pipeline companies account for and manage cybersecurity to protect the use of automated digital controls, or industrial control systems (ICS). ICS are not unique or new to pipelines; they are prevalent across the entire energy landscape, including at coal and nuclear power generation facilities.

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) has been widely adopted by natural gas pipeline operators. Different segments of the natural gas and oil value chain have adopted additional standards as applicable to their business model, including the ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems Security.

Furthermore, the natural gas system is highly resilient because the production, gathering, processing, transmission, distribution and storage are highly flexible and elastic – characterized by multiple fail-safes, redundancies and backups. Pipeline companies have in place layers that protect against cascading failure, which also include mechanical controls that are not capable of being overridden through any cyber compromise of ICS.

EXECUTIVE SUMMARY

Cybersecurity is a top priority for the natural gas and oil industry. As the owners and operators of some of the nation's most critical infrastructure, industry companies take seriously the protection of industrial control systems (ICS) and operational technology (OT) – the digital monitoring and/or controls of physical assets – and prevention of energy disruptions that can impact national security and public safety. While industry companies are also responsible for and prioritize the protection of information technology (IT), intellectual property (IP) and personally identifiable information (PII), this report focuses predominately on cybersecurity in the natural gas and oil industry as it relates to the protection of ICS.

Natural gas and oil companies recognize that their assets are the targets of a growing number of increasingly sophisticated cyberattacks perpetrated by a variety of attackers including nation-states and organized international criminals. Companies acknowledge that cyberattacks can present "enterprise risks" – risks that could compromise the viability of a company – and have developed comprehensive approaches to cybersecurity similar to industry's approach to managing safety: robust governance, systematic risk-based management, and multi-dimensional programs based on proven frameworks including the NIST Cybersecurity Framework (NIST CSF), best-in-class international cybersecurity standards including ISA/IEC 62443, and the Department of Energy (DOE) Cybersecurity Capability Maturity Model (C2M2).

Cybersecurity in the natural gas and oil industry applies throughout the value chain, extending from wellheads to pipelines and through to the supply of natural gas to an electric power generation facility or gas utility, or the supply of oil to a refinery and through to the manufacturing of fuels and sales at a gasoline station. Industry works closely with the government agencies responsible for cybersecurity throughout each of these segments – from Coast Guard regulatory oversight in maritime and maritime-facing facilities to Transportation Security Administration (TSA) regulatory oversight of pipelines, as well as bi-directional sharing with the U.S. intelligence community via the Department of Homeland Security (DHS)/NIST's National Cybersecurity & Communications Integration Center (NCCIC), DOE, FBI and others – ensuring collaboration and communication at every point. Furthermore, industry participates in information sharing through ISACs and peer-to-peer learning through trade associations to force multiply individual companies' threat analysis assets and defenses.

The reliance upon proven risk management-based frameworks and public-private collaboration, rather than prescriptive regulation, is the most effective and robust method of bolstering the cybersecurity of the natural gas and oil industry and the critical infrastructure they operate. With the increasing sophistication and adaptiveness of cyber adversaries, it is essential that industry be afforded the necessary flexibility and agility to respond to a constantly-changing threat landscape, and that government and industry continue to partner to share cyber threat intelligence and strengthen cyber defenses.

CYBER THREATS AND CYBERSECURITY: SITUATIONAL ANALYSIS

Natural gas and oil companies share the concerns of policymakers and others regarding the potential implications of a cyberattack on industry assets, and take seriously the responsibility to protect critical infrastructure, provide reliable energy for society and safeguard public safety and the environment. As operators and service providers of energy critical infrastructure in the United States and globally, protecting services from cyberattacks is a top priority.

The natural gas and oil industry faces the threat of cyberattacks from a variety of malicious actors including nation states, criminal organizations and unaffiliated bad-actors seeking to steal intellectual property and/or compromise industrial control systems (ICS), among many other nefarious goals.

Industry has witnessed the evolution of such cyber criminals as well as the advancement of the techniques, tactics and procedures (TTPs) they use, moving from manual operations to more sophisticated and wider-spread machine-to-machine and artificial intelligence automated attacks. There are multiple other attack vectors including insider threats, attacks via supply chain tampering or disruption, and insertion via counterfeits. Cyber threats may be exacerbated through combination with physical attacks or execution during a natural hazard disruption.

Cyberattacks targeting U.S. energy infrastructure are on the rise. The number of reported incidents directed at critical infrastructure rose from 245 in 2014 to 295 in 2015, with a similar count (290) in 2016.[1] Of the reported incidents, roughly 20 percent (59 reported incidents) targeted the energy sector.

Industry companies recognize that they and their assets are the targets of an increasing number of cyberattacks, and protecting these assets — including critical infrastructure, people and the environment — is a significant priority. Industry infrastructure is highly automated, and pipeline operators, terminal owners and utilities alike rely on ICS for monitoring and/or remote control. ICS are not unique or new to pipelines and are prevalent across the energy system, including at coal and nuclear plants. These systems, the digital controls of industrial facilities, include supervisory control and data acquisition (SCADA), process control networks (PCN) and distributed control systems. These systems – controlled and monitored by a trained operator – keep operations up and running. Advanced cybersecurity operations are critical to ensure that ICS – particularly those operating critical infrastructure (CI) – are segmented and thus protected by limiting exposure to attack.[2]

INDUSTRY APPROACH TOWARDS CYBERSECURITY

ENTERPRISE RISK MANAGEMENT AND DEFENSE-IN-DEPTH

Throughout the course of operations, natural gas and oil companies are faced with a variety of "enterprise risks" – meaning threats that are considered to pose the highest level of risk to a company with potential firm-wide impacts that could compromise the company's viability. Examples of enterprise risks faced by industry companies include safety hazards; changes in laws, regulations or geopolitical forces that affect the fundamental license to operate; changes in market demand or competition; or other systemic financial risks. Cyberattacks can be considered to pose this level of risk and are thus managed at the same priority level on an ongoing basis.

Cyberattacks can target ICS, seeking to compromise business continuity or cause a potential health, safety or environmental incident. Attacks can also target IT — data on business or enterprise networks — including IP such as sensitive business development information and trade secrets that, if stolen, could impact new ventures and opportunities to grow.

In recognition of the sophistication and dedication of cyber attackers, and the enterprise risk presented by cyberattacks, natural gas and oil companies have developed comprehensive risk-based "defense-in-depth" approaches to cybersecurity similar to industry's approach to managing the other enterprise risks: robust governance, systematic risk-based management, and multi-dimensional programs based on best-in-class standards and proven frameworks. Industry also coordinates with government partners at all levels.

A layered defense approach provides optimal protection in the rapidly evolving cyber threat landscape, as no one layer of defense or technology will ever be completely effective. This approach creates a landscape that is much more challenging for an attacker to fully penetrate – providing necessary time to implement defensive response measures.

A layered defense approach also incorporates system redundancies and fail safes including the ability to manually operate without ICS.

In the natural gas and oil industry, Boards of Directors and senior executives establish a company's acceptable level of risk mitigation to address cybersecurity threats and regularly monitor the effectiveness of the company's cybersecurity program, allocating additional resources to enhance cybersecurity when it is determined that risks need to be lowered, and re-affirming the priority of company-wide cybersecurity practices and protocols. The natural gas and oil industry's risk-based approach to cybersecurity also accords with the NIST CSF, described in more detail below.

Industry has a long history of risk management including the development and use of internal procedures to drive continuous improvement and manage the most significant risks. These principles extend to cybersecurity through a focus on maintaining basic cybersecurity practices including ensuring antivirus applications are up to date, mitigation measures such as security patches are applied as appropriate, and the use of powerful system identifications are managed for appropriate usage. Companies routinely make difficult choices to improve security over user productivity, for example restricting the use of removable media devices such as USBs to limit possible infections to the environment introduced via these devices, restricting web use and prohibiting access to personal email from company workstations. Many companies routinely conduct drills with key personnel, such as a simulated data breach, to provide assurances that attacks can be detected, contained and remediated to avoid significant loss. These practices set a solid foundation for further enhancing security capabilities with respect to cyberattacks, allowing companies to focus on more sophisticated and challenging cyber threats.

Industry sets priorities and implements processes to protect the most critical aspects of infrastructure against likely threats; to build redundancy into the system to make it more resilient; to coordinate preparation and response efforts with the government; and to develop contingency plans for response and recovery if operations are impacted.

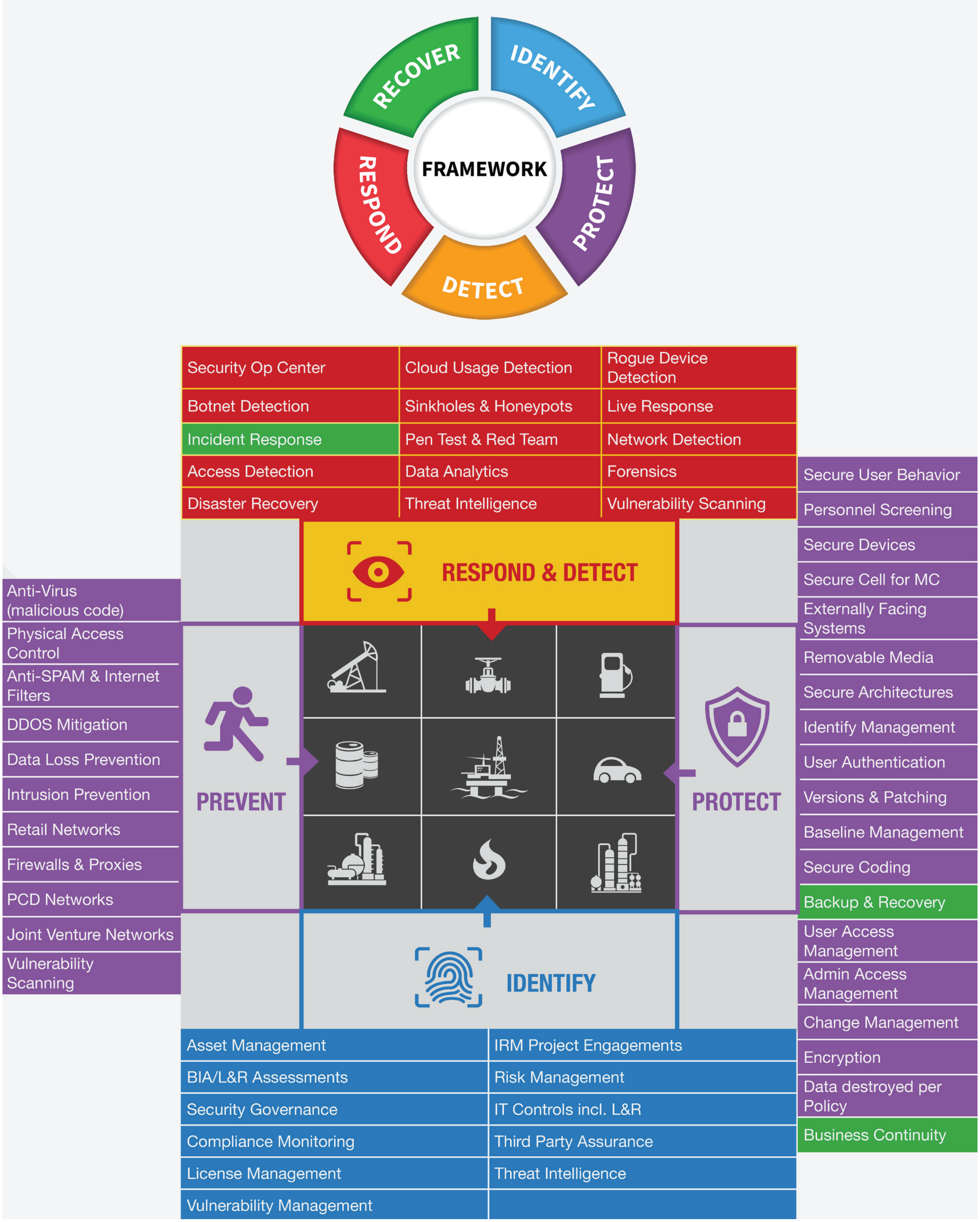
Companies typically establish cybersecurity programs that can be understood through three fundamental lenses: the critical functions as they apply to leading standards such as the NIST CSF; the components of a system as expressed through all technologies connected to company operations; and the network architecture. These lenses apply to all companies – they are overlapping ways to understand how the natural gas and oil industry implements cybersecurity.

CRITICAL CYBERSECURITY PROGRAM COMPONENTS: A NIST CYBERSECURITY FRAMEWORK LENS

Natural gas and oil companies implement cybersecurity programs that comprise many components. Companies often frame these components through the lens of the NIST Cybersecurity Framework (CSF), a voluntary framework intended to provide a common language organizations can use to assess and manage cybersecurity risk.

Developed in response to Executive Order (EO) 13636 “Improving Critical Infrastructure Cybersecurity”, the CSF recommends risk management processes that enable organizations to inform and prioritize decisions regarding cybersecurity based on business needs, without additional regulatory requirements. It enables organizations—regardless of sector, size, degree of cybersecurity risk, or cybersecurity sophistication—to apply the principles and effective practices of risk management to improve the security and resilience of critical infrastructure.[3]

FIGURE 1 displays an example of a cybersecurity program based on the NIST CSF deployed across one company. The programmatic areas correspond to the NIST Framework Functions via the color-coded legend.



Security Op Center	Cloud Usage Detection	Rogue Device Detection
Botnet Detection	Sinkholes & Honeypots	Live Response
Incident Response	Pen Test & Red Team	Network Detection
Access Detection	Data Analytics	Forensics
Disaster Recovery	Threat Intelligence	Vulnerability Scanning

- Anti-Virus (malicious code)
- Physical Access Control
- Anti-SPAM & Internet Filters
- DDOS Mitigation
- Data Loss Prevention
- Intrusion Prevention
- Retail Networks
- Firewalls & Proxies
- PCD Networks
- Joint Venture Networks
- Vulnerability Scanning

- Secure User Behavior
- Personnel Screening
- Secure Devices
- Secure Cell for MC
- Externally Facing Systems
- Removable Media
- Secure Architectures
- Identify Management
- User Authentication
- Versions & Patching
- Baseline Management
- Secure Coding
- Backup & Recovery
- User Access Management
- Admin Access Management
- Change Management
- Encryption
- Data destroyed per Policy
- Business Continuity

Asset Management	IRM Project Engagements
BIA/L&R Assessments	Risk Management
Security Governance	IT Controls incl. L&R
Compliance Monitoring	Third Party Assurance
License Management	Threat Intelligence
Vulnerability Management	

FIGURE 1. Example of cybersecurity programs deployed across one company.

The CSF is designed to complement, and not replace or limit, an organization's risk management process and cybersecurity program. Each individual organization can use the CSF in a tailored manner to address its cybersecurity objectives.

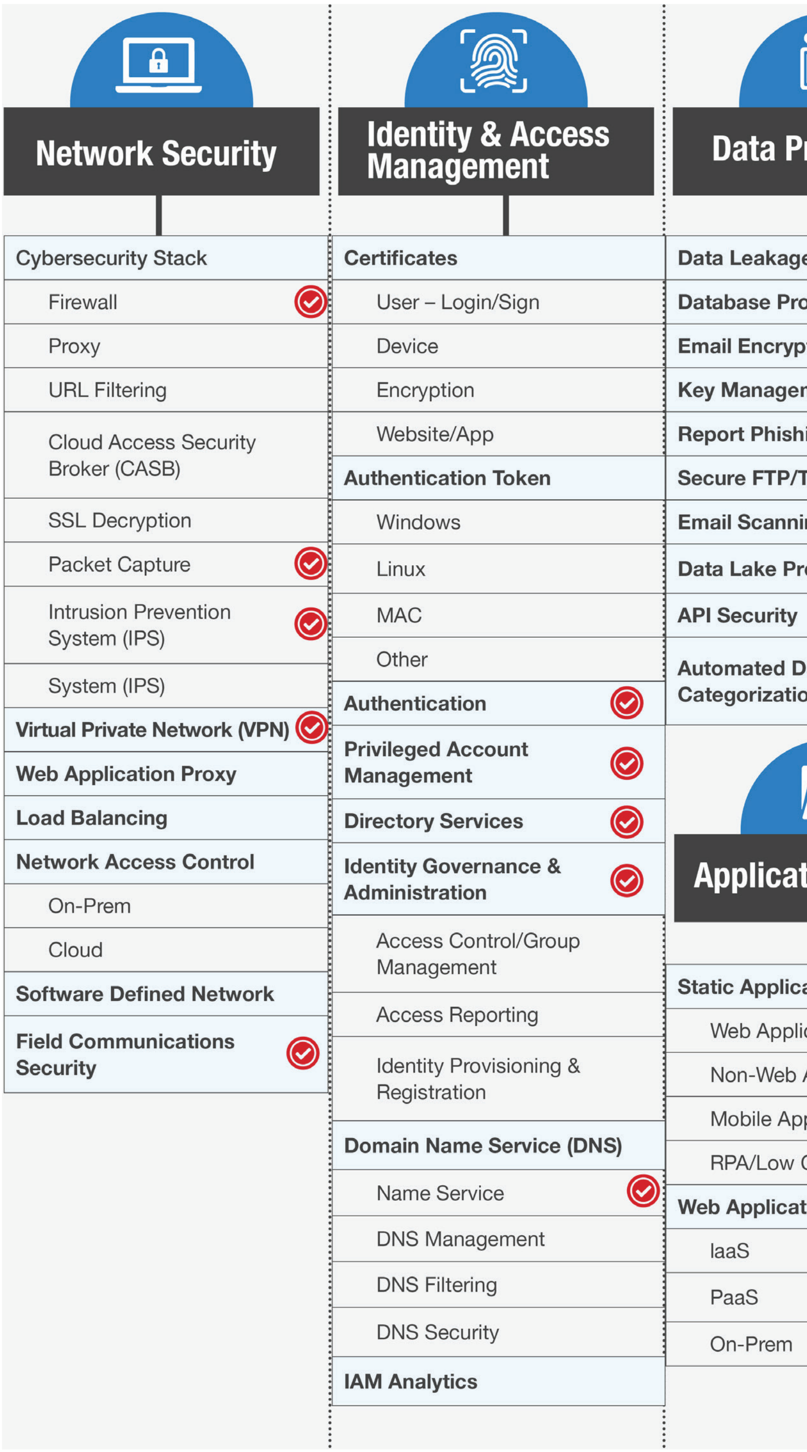
The framework was developed with a focus on industries vital to national and economic security including energy, banking, communications and the defense industrial base. Representatives from these industries – including natural gas and oil companies – participated in the development. It has since proven flexible enough to be adopted voluntarily by large and small companies and organizations across all industry sectors, as well as by federal, state and local governments.[4]

Through widespread industry adoption of the NIST CSF, natural gas and oil companies are able to effectively communicate cybersecurity issues for internal evaluations of capabilities and programs, internal program prioritization, external benchmarking against peers' performance and external evaluation of suppliers and contractors.[5]

As shown in **FIGURE 1**, the five core functions of the NIST CSF provide a base by which natural gas and oil companies – and companies of all sizes in sectors from healthcare to banking to telecommunications and others – can structure comprehensive cybersecurity programs.[6] A more detailed explanation of the five programmatic areas can be found in **APPENDIX A**.

CRITICAL CYBERSECURITY PROGRAM COMPONENTS: A TECHNOLOGY LENS

Natural gas and oil companies take into account technologies connected to company operations when developing a comprehensive cybersecurity program.



Network Security

- **Cybersecurity Stack**
  - Firewall ✓
  - Proxy
  - URL Filtering
  - Cloud Access Security Broker (CASB)
  - SSL Decryption
  - Packet Capture ✓
  - Intrusion Prevention System (IPS) ✓
  - System (IPS)
- **Virtual Private Network (VPN)** ✓
- **Web Application Proxy**
- **Load Balancing**
- **Network Access Control**
  - On-Prem
  - Cloud
- **Software Defined Network**
- **Field Communications Security** ✓

Identity & Access Management

- **Certificates**
  - User – Login/Sign
  - Device
  - Encryption
  - Website/App
- **Authentication Token**
  - Windows
  - Linux
  - MAC
  - Other
- **Authentication** ✓
- **Privileged Account Management** ✓
- **Directory Services** ✓
- **Identity Governance & Administration** ✓
  - Access Control/Group Management
  - Access Reporting
  - Identity Provisioning & Registration
- **Domain Name Service (DNS)**
  - Name Service ✓
  - DNS Management
  - DNS Filtering
  - DNS Security
- **IAM Analytics**

Data Pr

- **Data Leakage**
- **Database Pro**
- **Email Encryp**
- **Key Manager**
- **Report Phishi**
- **Secure FTP/T**
- **Email Scanni**
- **Data Lake Pr**
- **API Security**
- **Automated D Categorizatio**

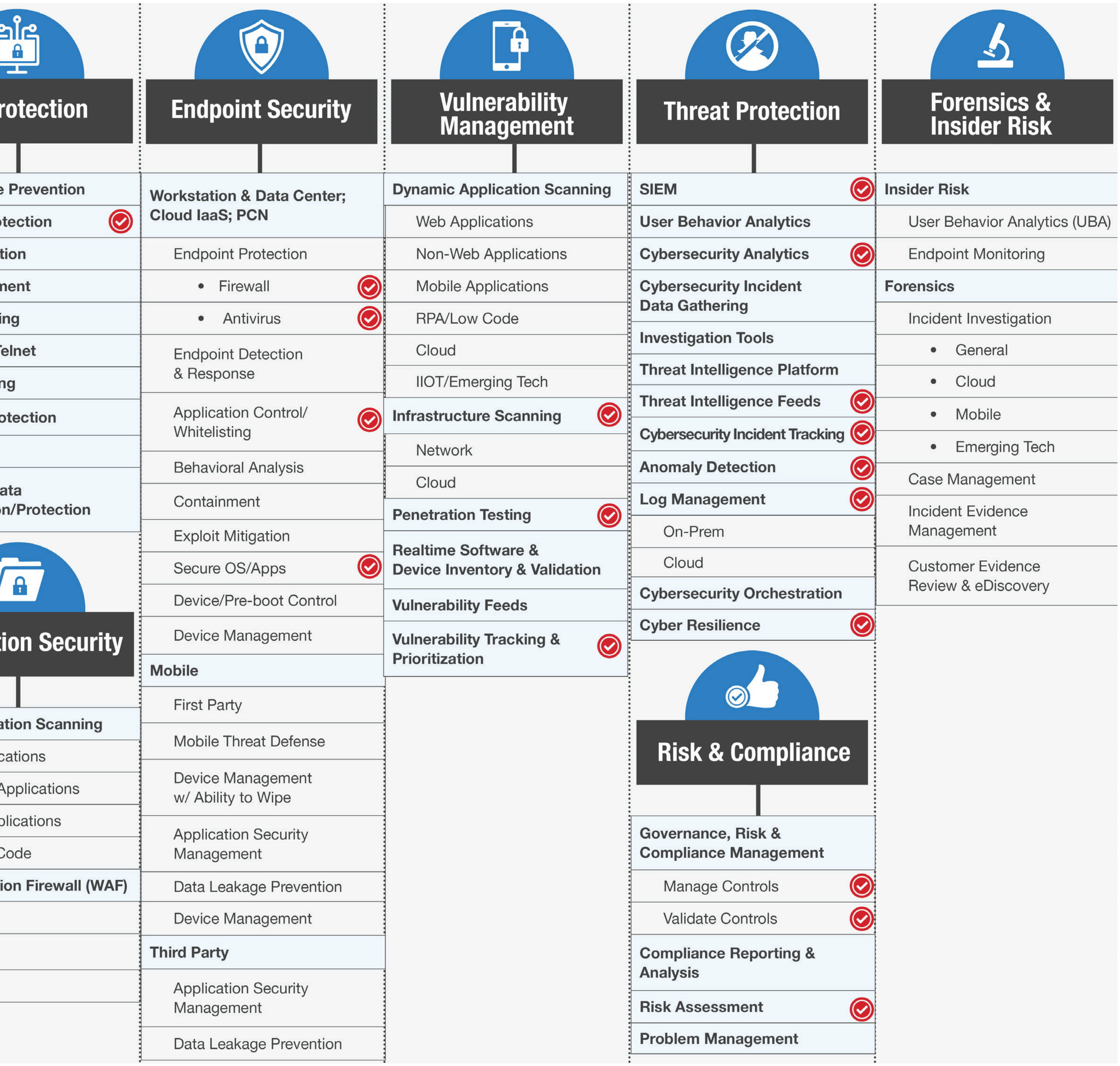
Applicat

- **Static Applica**
  - Web Applic
  - Non-Web A
  - Mobile App
  - RPA/Low C
- **Web Applicat**
  - IaaS
  - PaaS
  - On-Prem

FIGURE 2. Example of technologies deployed across one company.

By determining all critical system components and identifying which components apply to the company's ICS, companies are able to segment technologies and implement firewalls where needed.

An example of these processes implemented across a natural gas and oil company is displayed in **FIGURE 2**. In this example, technologies that may apply to the production ICS are designated by a red check. A more detailed explanation of the nine critical system areas can be found in **APPENDIX B**.



rotection

- e Prevention
- tection ✓
- tion
- nent
- ing
- elnet
- ng
- otection
- ata n/Protection

tion Security

- ation Scanning
- cations
- Applications
- plications
- Code
- ion Firewall (WAF)

Endpoint Security

- **Workstation & Data Center; Cloud IaaS; PCN**
  - Endpoint Protection
    - Firewall ✓
    - Antivirus ✓
  - Endpoint Detection & Response
  - Application Control/ Whitelisting ✓
  - Behavioral Analysis
  - Containment
  - Exploit Mitigation
  - Secure OS/Apps ✓
  - Device/Pre-boot Control
  - Device Management
- **Mobile**
  - First Party
  - Mobile Threat Defense
  - Device Management w/ Ability to Wipe
  - Application Security Management
  - Data Leakage Prevention
  - Device Management
- **Third Party**
  - Application Security Management
  - Data Leakage Prevention

Vulnerability Management

- **Dynamic Application Scanning**
  - Web Applications
  - Non-Web Applications
  - Mobile Applications
  - RPA/Low Code
  - Cloud
  - IIOT/Emerging Tech
- **Infrastructure Scanning** ✓
  - Network
  - Cloud
- **Penetration Testing** ✓
- **Realtime Software & Device Inventory & Validation**
- **Vulnerability Feeds**
- **Vulnerability Tracking & Prioritization** ✓

Threat Protection

- **SIEM** ✓
- **User Behavior Analytics**
- **Cybersecurity Analytics** ✓
- **Cybersecurity Incident Data Gathering**
- **Investigation Tools**
- **Threat Intelligence Platform**
- **Threat Intelligence Feeds** ✓
- **Cybersecurity Incident Tracking** ✓
- **Anomaly Detection** ✓
- **Log Management** ✓
  - On-Prem
  - Cloud
- **Cybersecurity Orchestration**
- **Cyber Resilience** ✓

Risk & Compliance

- **Governance, Risk & Compliance Management**
  - Manage Controls ✓
  - Validate Controls ✓
- **Compliance Reporting & Analysis**
- **Risk Assessment** ✓
- **Problem Management**

Forensics & Insider Risk

- **Insider Risk**
  - User Behavior Analytics (UBA)
  - Endpoint Monitoring
- **Forensics**
  - Incident Investigation
    - General
    - Cloud
    - Mobile
    - Emerging Tech
  - Case Management
  - Incident Evidence Management
  - Customer Evidence Review & eDiscovery

NETWORK ARCHITECTURE AND SEGMENTATION

Regardless of the structure used for cybersecurity program development, natural gas and oil companies typically buffer ICS from cyberattacks through the use of "defense-in-depth" network architecture.

Natural gas and oil companies segment their systems and implement "demilitarized zones" (DMZ) between industrial controls and internet-facing business networks.[7] **FIGURE 3** illustrates an example network architecture utilizing the ISA/IEC 62443 series of standards on industrial automation and control systems (IACS) security and a modified "Purdue Model."

As seen in this example, the ISA/IEC standards provide ICS operators with:

- **CONCEPTS AND MODELS:** a framework for network architecture, including segmentation through zones and conduits.
- **POLICIES AND PROCEDURES:** prompts for companies to put into place a security management system, conduct patch management, and establish internal cybersecurity requirements for suppliers.
- **CYBERSECURITY OF OPERATION OF INTERNAL ICS SYSTEM:** guidance to companies for deployment of cybersecurity technologies, ICS security risk assessment and system design, and internal requirements for ICS security and cybersecurity levels.
- **CYBERSECURITY OF INSTALLED ICS COMPONENTS:** guidance to companies for internal requirements for product development and technical security of ICS components.

Most natural gas and oil companies operate in a cybersecurity landscape consisting of three critical areas: the ICS, internet-facing components and internal networks. Companies architect and manage cybersecurity across these networks to reduce the risk of compromise to ICS from attacks that could flow from the outside-in across these networks.

The computer systems that compose the ICS run the most critical components of operations. These are represented in Levels 0-3 of **FIGURE 3**. Today's ICS environments in the natural gas and oil industry rely on computing technologies for advanced monitoring and/or control of unit processes, such as adjusting valves to regulate pressure or controlling pumps to regulate product flow, located in refineries, petrochemical plants and pipeline/terminal distribution sites. These technologies in turn make operations vulnerable to cyber threats. A widely accepted practice is to ensure ICS remain logically isolated from systems providing control of the unit.

Organizations mitigate the risk of a cyber threat to internal networks from exposure to the public internet by creating a security zone between the ICS and business network that is frequently referred to as the DMZ, represented between Level 3 and Level 4 of **FIGURE 3**. Firewalls within the DMZ serve as "data diodes" allowing specific information to travel from ICS to IT environments while limiting or eliminating information flow from IT environments to ICS.

Level 4 of **FIGURE 3** represents a company's business network or enterprise zone, the environment where users perform functions such as email, collaboration and analytics. It is here that companies hold most intellectual property assets and conduct other internal business transactions. For the natural gas and oil industry, the most valuable intellectual property includes information regarding proprietary technology, breakthrough research, bid proposals and acquisitions and mergers. Industry's cybersecurity focus in this area relies on early detection and a layered approach to defenses. User awareness training is also a critical focus area as it is highly recognized that no amount of technology will protect against every threat – the end-user plays a large role as a layer in defense.

The natural gas and oil industry relies on internet-facing components such as e-commerce for product purchases along with areas that allow collaboration with business partners. These components, represented in Level 5 of **FIGURE 3,** above, are contained within an area of a company network that is outwardly facing to the public and separated from the internal business network by another DMZ.

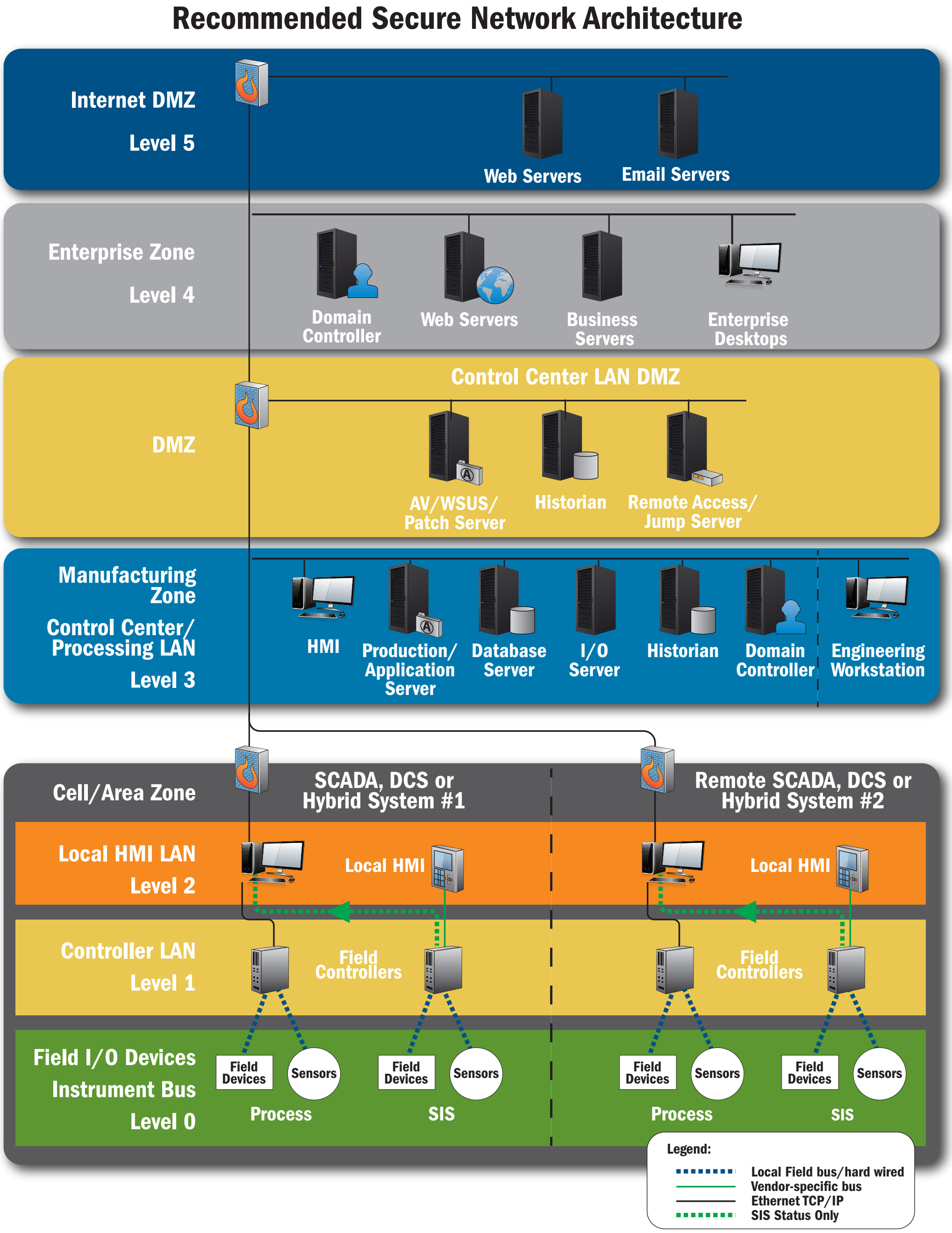


FIGURE 3. Diagram illustrating "defense-in-depth" network architecture.[8]

INCORPORATING LEADING EXTERNAL FRAMEWORK AND STANDARDS

In partnership with the Department of Commerce's National Institute of Standards and Technology (NIST), Department of Energy (DOE) and other U.S. and international standards-setting bodies, the industry orients its cybersecurity programs to the NIST CSF and additional programs such as the ISA/IEC 62443 Series of Standards on IACS Security and the DOE Cybersecurity Capability Maturity Model (C2M2). These tools are complementary and compatible, often cross-referencing from one to the other to guide the industry cybersecurity efforts for protecting ICS and IT.

The ISO/IEC 27000 family of ISO/IEC Information Security Management Systems (ISMS) standards widely used in the production segment of the natural gas and oil industry. The ISO/IEC 27000 standards are IT-focused and provide detailed guidance to the industry for protecting IT and IP from cyberattacks. Similar standards are used in other segments of the natural gas and oil value chain.

Another standard that has been produced by the natural gas and oil industry, API Standard 1164, is specific to pipeline cybersecurity. Subject matter experts from natural gas and oil companies and from cybersecurity vendors are currently working to update API 1164 to make it complementary to the NIST CSF and other applicable cybersecurity standards, such as ISA/IEC 62443 while still providing pipeline-specific cybersecurity guidance.

NATURAL GAS AND OIL COMPANIES OPERATE TO LEADING CYBERSECURITY STANDARDS AND FRAMEWORKS

API STANDARD 1164

Content unique to pipelines not covered by NIST CSF and IEC 62443; Currently being updated with expected completion in 2019.

NIST CYBERSECURITY FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (NIST CSF)

Pre-eminent Framework adopted by companies in all industry sectors; Natural gas and oil companies increasingly orient enterprise-wide programs around NIST CSF.

DEPARTMENT OF ENERGY CYBERSECURITY CAPABILITY MATURITY MODEL: Voluntary process using industry-accepted best practices to measure the maturity of an organization's cybersecurity capabilities and strengthen operations.[9]

INTERNATIONAL ELECTROTECHNICAL COMMISSION'S IEC 62443

Pre-eminent family of standards for industrial control systems (ICS) security; Widely-adopted by production segment of natural gas and oil industry; applicable to any type of natural gas and oil ICS.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION ISO 27000

Leading standard in the family providing requirements for an information security management system (ISMS).

CYBERSECURITY PARTNERSHIP WITH GOVERNMENT

Cybersecurity in the natural gas and oil industry applies throughout the value chain, extending from wellheads to pipelines and through to the supply of natural gas to an electric power generation facility or gas utility, or the supply of oil to a refinery and through to a gasoline station.

FIGURE 4 illustrates the full natural gas and oil value chain.

Industry works closely with the government agencies responsible for cybersecurity throughout each of these segments – from Coast Guard regulatory oversight in maritime and maritime-facing facilities to TSA regulatory oversight of pipelines, as well as bi-directional sharing with the U.S. intelligence community via DHS/NCCIC, DOE, FBI and others – ensuring collaboration and communication at every point.

Industry-government collaboration on cybersecurity fits within the experience we have working together through an all-hazards approach to prepare for, respond to and recover from a wide array of threats and hazards ranging from natural disasters to cyberattacks. Initiatives and activities undertaken by industry, government or through joint partnerships on cybersecurity, just as for other hazards, include classified briefings to share threat and risk information; organizing structures to improve information sharing; availability of trained emergency responders; threat-specific and function-specific drills and exercise programs; ongoing information exchanges; and situational awareness reports.

A list of the regulatory bodies covering the natural gas and oil industry, and the relationship between those bodies and industry, can be found in **APPENDIX C**.

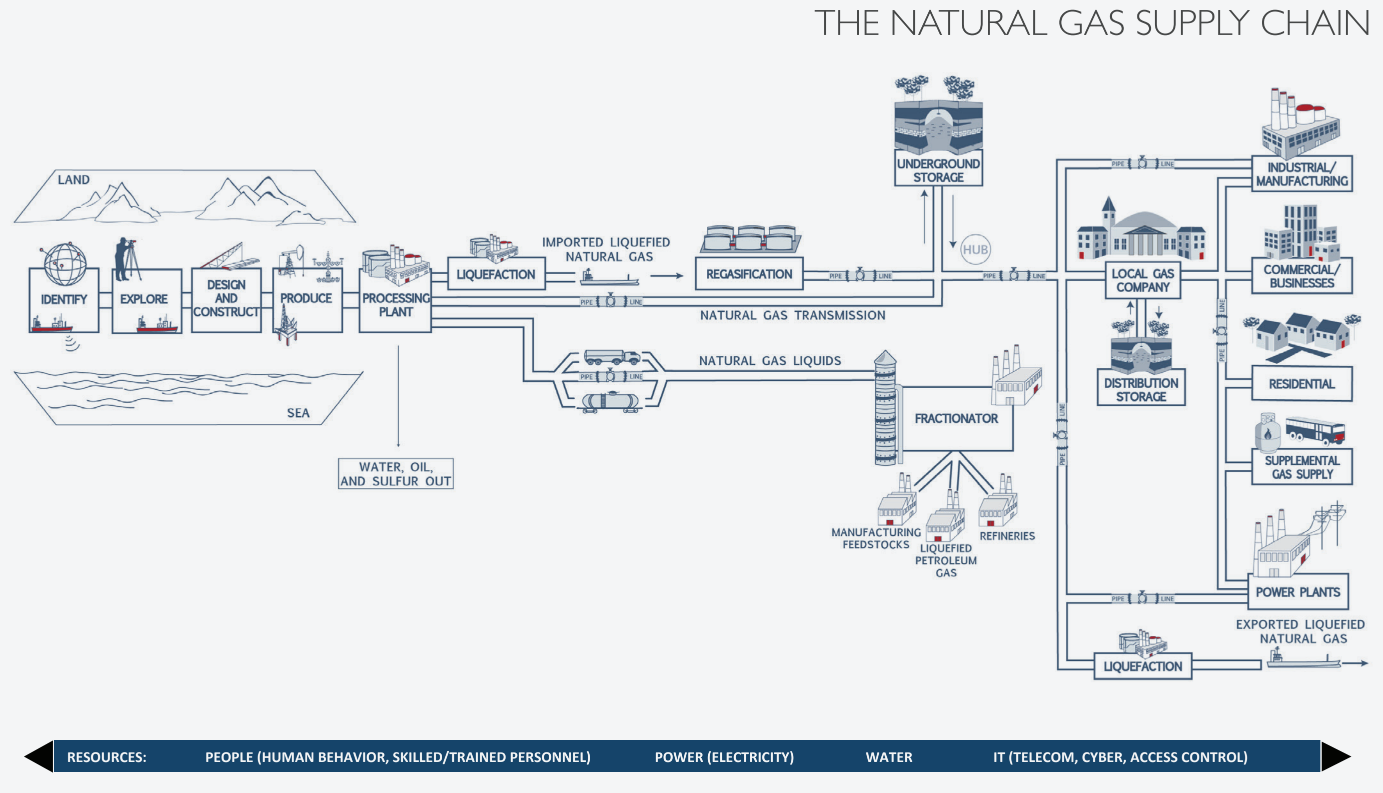


FIGURE 4. Supply Chain Model. Source: API, Oil and Natural Gas Industry Preparedness Handbook, 2013.

INFORMATION SHARING AS CRITICAL CYBERSECURITY DEFENSE

Beyond industry's work with government, companies participate in information sharing through Information Sharing and Analysis Centers (ISACs) and peer-to-peer learning through trade associations to force multiply individual companies' threat analysis assets and provide critical lines of defense.

INFORMATION SHARING AND ANALYSIS CENTERS (ISACS)

In 2015, the natural gas and oil industry was a leading supporter of the first-ever legal framework to govern cybersecurity information sharing. The Cybersecurity Act of 2015 enabled cybersecurity threat indicators to be shared between and among companies and the U.S. Government, established the legal requirements and protections for such sharing, and established DHS as the hub for government and private sector cybersecurity information sharing.[10]

While DHS leads the federal government's efforts to secure critical infrastructure, ISACs were created as the Department and other pillars of government recognized the importance of public-private partnerships in mitigating and rapidly responding to crises because of the extent to which critical infrastructure is operated by the private sector.[11]

Facing threats to our nation from cyberattacks that could disrupt power, water, communication and other critical systems, U.S. Presidents have issued Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity, Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience, and EO 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.[12, 13] These policies empower the private sector to discuss tactics and procedures that can be leveraged to protect individual companies, the industry and critical infrastructure from cyber attackers, and reinforce the need for holistic thinking about security and risk management.

Implementation of the EOs and PPD drive action toward system and network security and resiliency and enhance the efficiency and effectiveness of the U.S. government's work to secure critical infrastructure and make it more resilient.[14] The Oil and Natural Gas ISAC (ONG-ISAC) and Downstream Natural Gas ISAC (DNG-ISAC) provide a secure and trusted environment for the sharing of cybersecurity information across the natural gas and oil industry.[15, 16] Specifically, it is through these ISACs that natural gas and oil companies – including many of the nation's largest natural gas pipeline operators – share cyber threat indicators and intelligence with each other and with the U.S. Government, which is the primary mechanism through which DOE and other U.S. national security and law enforcement agencies continue to work together with the private sector to keep U.S. pipelines safe and secure. The structure is outlined in **FIGURE 5**.

NATURAL GAS AND OIL COMPANIES WORK COLLABORATIVELY WITH THE U.S. GOVERNMENT, ENABLED BY RECENT PUBLIC POLICY

CYBERSECURITY ACT OF 2015

Establishing the legal framework for cyber information sharing:

- Requires companies to protect information and share according to certain protocols
- Provides legal protections to companies when these requirements are met
- Establishes DHS as a hub for information sharing, providing a conduit for cyber threat indicators to flow back and forth from the private sector to the U.S. Government, including intelligence agencies
- Incentivizes the work of Information Sharing and Analysis Centers (ISACs) such as the Oil and Natural Gas ISAC (ONG-ISAC) and Downstream Natural Gas ISAC (DNG-ISAC)

EXECUTIVE ORDER 13636

Improving Critical Infrastructure Cybersecurity directs the Executive Branch to:

- Develop a technology-neutral voluntary cybersecurity framework
- Promote and incentivize the adoption of cybersecurity practices
- Increase the volume, timeliness and quality of cyber threat information sharing
- Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
- Explore the use of existing regulation to promote cyber security

PRESIDENTIAL POLICY DIRECTIVE-21

Critical Infrastructure Security and Resilience Directs the Executive Branch to:

- Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
- Understand the cascading consequences of infrastructure failures
- Evaluate and mature the public-private partnership
- Update the National Infrastructure Protection Plan
- Develop comprehensive research and development plan

EXECUTIVE ORDER 13800

Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure Directs the Executive Branch to:

- Enhance cybersecurity of federal government networks, including to use the NIST Cybersecurity Framework to manage federal agency's cybersecurity risk
- Enhance cybersecurity of critical infrastructure, including to provide support on cybersecurity to critical infrastructure at greatest risk
- Enhance cybersecurity of the nation through international efforts in deterrence, protection and cooperation; cybersecurity workforce development; and assessment of national-security-related cyber capabilities.

SOURCE: Department of Homeland Security, Executive Order 13636, Presidential Directive 21 Fact Sheet.

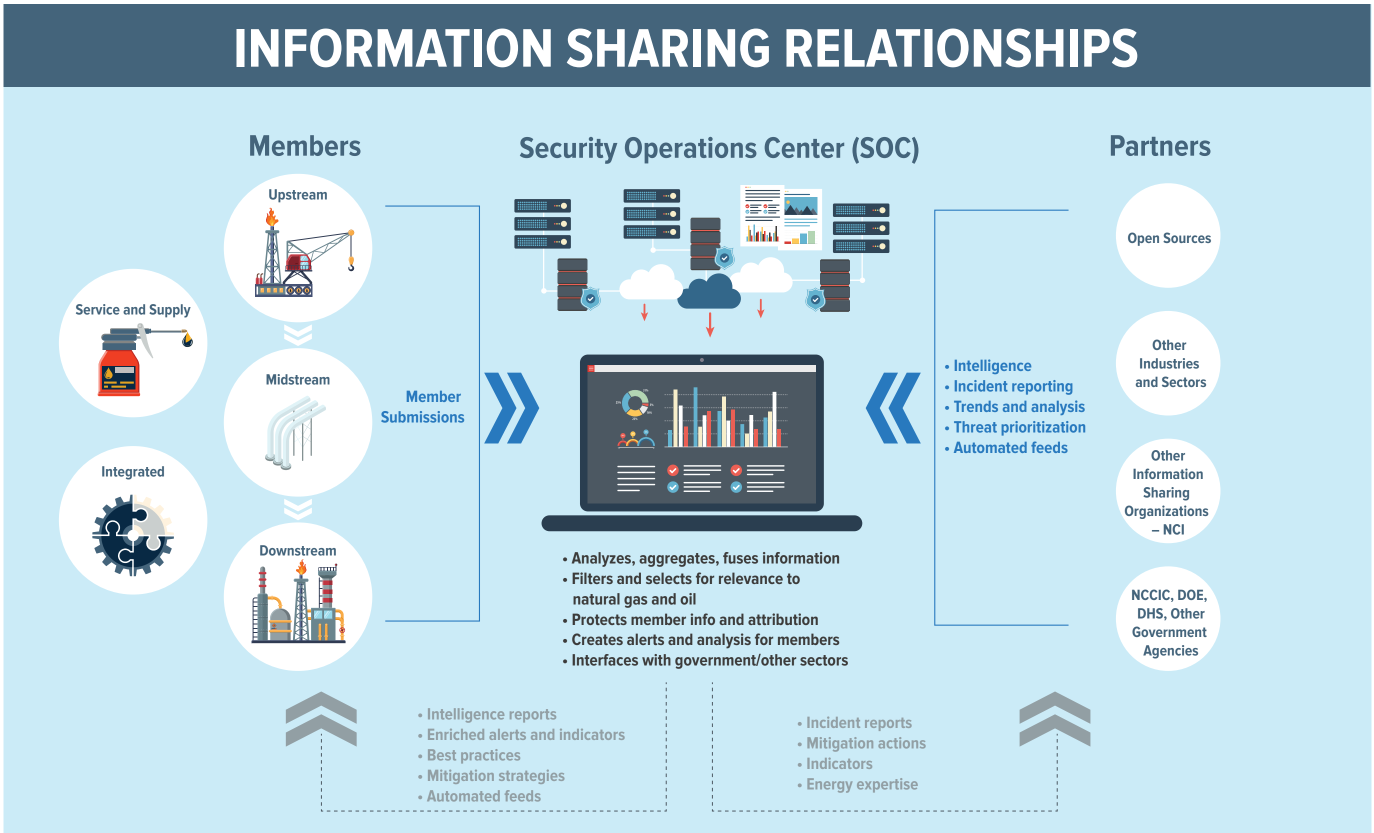

INFORMATION SHARING RELATIONSHIPS
Members
Security Operations Center (SOC)
Partners
Upstream
Service and Supply
Midstream
Integrated
Downstream
Member Submissions
• Intelligence
• Incident reporting
• Trends and analysis
• Threat prioritization
• Automated feeds
• Analyzes, aggregates, fuses information
• Filters and selects for relevance to natural gas and oil
• Protects member info and attribution
• Creates alerts and analysis for members
• Interfaces with government/other sectors
Open Sources
Other Industries and Sectors
Other Information Sharing Organizations – NCI
NCCIC, DOE, DHS, Other Government Agencies
• Intelligence reports
• Enriched alerts and indicators
• Best practices
• Mitigation strategies
• Automated feeds
• Incident reports
• Mitigation actions
• Indicators
• Energy expertise

FIGURE 5. ONG-ISAC and DNG-ISAC Information Sharing Relationships.

As illustrated in **FIGURE 5**, the ISAC facilitates the peer-to-peer sharing of cyber threat information between natural gas and oil companies and instituting bi-directional sharing with the U.S. Intelligence Community (IC) via DHS/NCCIC, DOE, FBI and others. This information sharing also extends to the Electricity ISAC (E-ISAC), with the participation of all three ISACs in regular intelligence briefings with DOE and the bi-directional communication with NCCIC.

As the threat landscape is ever-changing and the needs of individual companies vary, ONG-ISAC and DNG-ISAC member companies utilize this framework to communicate leading practices in threat detection and cybersecurity mitigations and provide support where needed. Companies share information related to cyberattacks, threats and vulnerabilities as well as the TTPs of cyber attackers and Indicators of Compromise (IOC).

The ONG-ISAC and DNG-ISAC, as well as the DHS/NCCIC and other government agencies, utilize the Forum of Incident Response and Security Teams (FIRST) Traffic Light Protocol (TLP) to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s).[17] TLP definitions are identified in **APPENDIX D**.

Both the ONG-ISAC and DNG-ISAC facilitate ongoing information sharing through a variety of work products in order to provide the necessary level of intelligence guidance, whether strategic, tactical or immediate, providing a comprehensive structure of support to ISAC member companies. A detailed list of the work products organized by the ONG-ISAC and DNG-ISAC are available in **APPENDIX D**.

This structure allows companies to participate in guided, anonymous information sharing via a threat intelligence platform. The sharing of threat indicators is automated and disseminated in a machine-readable format, providing real-time notifications for near-real-time analyses. Companies have open access to community leaders and security analyst experts, as well as organized intelligence in one central place: federal feeds, third-party vendors, ISAC members and cross-sector sharing with other ISACs.[18] Ultimately, both the ONG-ISAC and DNG-ISAC allow natural gas and oil companies to quickly detect or respond to threats before they create an enterprise impact; learn from others to decrease overall risk, increase safety and avoid loss of revenue; protect company reputations and position organizations ahead of attackers; and avoid data overload to improve critical decision making.[19]

ACTUAL EXAMPLES OF SUCCESSFUL INFORMATION SHARING WITH INDUSTRY PARTNERS VIA ONG-ISAC, DNG-ISAC AND OTHER INFORMATION SHARING MECHANISMS:

- **ONG COMPANY A** shares information about an email phishing campaign via ONG-ISAC that **COMPANY B**'s Security Operations Center (SOC) has not detected. SOC receives this information and identifies that users at **COMPANY B** received these phishing emails and that a **COMPANY B** user has clicked on the malicious content. From this sharing, SOC identifies a cyber incident that occurred at **COMPANY B** which potentially would have not been detected and was able to contain/prevent other users from also attempting to access the malicious content.

- Analysts from **DNG COMPANY F** and **E-ISAC COMPANY G** share watch duty twice weekly. **E-ISAC COMPANY H** shares information about NotPetya ransomware via E-ISAC minutes after its outbreak. **E-ISAC COMPANY G** collaborates with **DNG COMPANY F** to warn DNG-ISAC members, provide members of both ISACs with indicators of compromise (IOCs), and begin to research and publish potential mitigations three hours before the first U.S. Government warning is released.

- **ONG COMPANY C** has a direct and open dialogue about security technologies (specifically email security technologies) that have been valuable to them in detecting/preventing cyber incidents from occurring. **COMPANY C** shared this information with **COMPANY D**'s SOC. **COMPANY D**'s OC passed this information along to the **COMPANY D**'s security technology/design team as an input into their alternative evaluation process when they reviewed different email security technologies.

- **DNG COMPANY J** analyst researches known personalities, their associates and supporters involved in illegal activities during global natural gas and oil protests. **DNG COMPANY J** determines highest priority targets and shares a threat information package via DNG-ISAC along with successful legal mitigations used by Federal, State, Local, Tribal and Territorial partners. E-ISAC requests DNG-ISAC support to Federal Energy Regulatory Commission security office and averts a potential facility penetration during an important FERC hearing.

- **ONG OMPANY E**'s SOC detects a cyber incident that is interesting and shares IOC with other ONG companies to identify if this activity is widespread, targeted towards **COMPANY E**, or targeted towards the ONG sector. This information helps **COMPANY E**'s SOC and **other companies** in scoping the sophistication/motive of an adversary.

As was identified in **FIGURE 5**, both ISACs also provide a structure for bi-directional information sharing with the U.S. Intelligence Community. Through the hub of the DHS/NCCIC, with reach-back to TSA and DOE as the sector-specific agencies as well as the FBI, the ISACs share incident reports, mitigation actions and indicators of compromise as well as energy expertise. In return, the ISACs receive intelligence, incident reports, trends, analyses and threat prioritization information, and is able to triage that information back to industry.

This process not only ensures that industry and government parties receive the appropriate and necessary information, but ensures consistent messaging, allows for anonymity when needed, and enables the near-real-time dissemination of information.

TRADE ASSOCIATION FACILITATION OF CYBERSECURITY COMMUNICATION AND LEARNING

In support of PPD-21, the owners and operators of natural gas and oil infrastructure, and the industry trade associations that represent them, formalized coordination efforts under the Oil and Natural Gas Subsector Coordinating Council (ONG SCC). The ONG SCC provides a private forum for effective coordination of natural gas and oil security strategies and activities, policy, and communication across the sector to support the nation's homeland security mission through the protection of the sector's critical infrastructure.[20]

The trade associations that make up the Oil and Natural Gas Subsector Coordinating Council (ONG SCC) represent the vast majority of the natural gas and oil value chain and are committed to the protection of industry assets from cyberattacks. Those associations include:

AMERICAN PETROLEUM INSTITUTE

The American Petroleum Institute (API) is the only national trade association that represents all aspects of America's natural gas and oil industry. API's 625+ corporate members, from the largest major oil company to the smallest of independents, come from all segments of the industry. They are producers, refiners, suppliers, pipeline operators and marine transporters, as well as service and supply companies that support all segments of the industry.

As operators and service providers of energy critical infrastructure in the United States and globally, protecting networks from cyberattacks is a priority of API members. As such, member companies regularly share their leading practices in cybersecurity.

AMERICAN GAS ASSOCIATION

The American Gas Association (AGA) represents more than 200 local energy companies that deliver clean natural gas to homes and businesses throughout the United States. AGA and its members are dedicated to helping ensure that natural gas pipeline infrastructure remains resilient to growing and dynamic cyber and physical security threats. AGA is committed to proactively collaborating with federal and state governments, public officials, law enforcement, emergency responders, research consortiums, and the public to continue improving the security posture of local energy companies and the industry's longstanding record of providing natural gas service safely, reliably and efficiently across America.

AGA and its operators implement security programs and actively engage in voluntary actions to help enhance the physical and cybersecurity of the nation's 2.5 million miles of natural gas pipeline, which span all 50 states with diverse geographic and operating conditions.

INTERSTATE NATURAL GAS ASSOCIATION OF AMERICA

The Interstate Natural Gas Association of America (INGAA) is the North American association representing the interstate and interprovincial natural gas pipeline industry. INGAA's 27 members represent the majority of the interstate natural gas transmission pipeline companies in the United States, operating approximately 200,000 miles of pipelines and serving as an indispensable link between natural gas producers and consumers.

INGAA and its members are committed to promoting the reliability of interstate natural gas transmission pipelines. INGAA members implement security programs and take action to ensure pipeline infrastructure remains resilient and secure. As such, INGAA members have signed commitments to following the TSA Pipeline Security Guidelines and NIST Cybersecurity Framework, and engage in information sharing platforms such as the DNG-ISAC.

ASSOCIATION OF OIL PIPE LINES

The Association of Oil Pipe Lines (AOPL) represents pipeline owners and operators carrying crude oil, refined petroleum products, natural gas liquids and other liquids. AOPL membership comprises 97 percent of the liquids pipeline industry. AOPL member company leaders share information and lessons about safety and security, including in leadership roundtables and a Pipeline Security Team. AOPL participates in discussions on cybersecurity issues with government representatives and other stakeholders.

AMERICAN FUEL AND PETROCHEMICAL MANUFACTURERS

The American Fuel and Petrochemical Manufacturers (AFPM) is a trade association representing high-tech American manufacturers of virtually the entire U.S. supply of gasoline, diesel, jet fuel, other fuels and home heating oil, as well as the petrochemicals used as building blocks for thousands of vital products in daily life.

AFPM's Cybersecurity Subcommittee was formed in 2005. The 40+ members of the Subcommittee comprise both owner operators and vendors, as AFPM considers both to be industry stakeholders. There is a cybersecurity track at the AFPM Operations & Process Technology Summit each fall and cybersecurity presentations at the AFPM Security Conference. The Subcommittee provides technical information that AFPM uses in legislative and regulatory activities. AFPM members participate in DOE and DHS cybersecurity exercises. AFPM is a participating steering committee member on both the DHS Industrial Control Systems Joint Working Group (ICSJWG) and Cyber Resilient Energy Delivery Consortium (CREDC).

INTERNATIONAL LIQUID TERMINALS ASSOCIATION

The International Liquid Terminals Association (ILTA) is an advocate and key resource for the liquid terminal industry. Liquid terminals and aboveground storage tank facilities interconnect with and provide services to the various modes of liquid transportation, including ships, barges, tank trucks, rail cars and pipelines. The commodities handled include a large variety of chemicals, along with crude oil, petroleum products, renewable fuels and other resources.

Terminal companies are continuously evaluating how they protect their most important assets, their critical intellectual property and sensitive customer information. ILTA helps member companies evaluate their cyber defenses and identify and address vulnerabilities.

INTERNATIONAL ASSOCIATION OF DRILLING CONTRACTORS

The International Association of Drilling

Contractors (IADC) exclusively represents the worldwide oil and gas drilling industry. The drilling industry plays a vital role in enabling the global economy, and in recognition of this role the industry maintains high standards of safety, environmental stewardship and operational efficiency. Through conferences, training seminars, print and electronic publications and a comprehensive network of technical publications, IADC continually fosters industry education and communication on critical issues including cybersecurity.

CYBERSECURITY-FOCUSED COMMITTEES AND PROGRAMS

API has convened its member companies on cybersecurity for more than 15 years. The Information Management and Technology Committee (IMTC) is comprised of Chief Information Officers (CIOs) from API member companies and serves as a forum for the natural gas and oil industry to address issues in systems technology including computers, communications, and electronic commerce. Key issues that the IMTC addresses include risk management, network security, critical infrastructure protection, information privacy, technological change, and knowledge management. The IMTC provides a forum for natural gas and oil company Chief Information Security Officers (CISOs) to discuss technological innovations, compare notes as peers and interact with policymakers and marketplace leaders regarding developments of common interest.[21]

The IMTC oversees the activities the API Information Technology Security Subcommittee (ITSS), the API cybersecurity-focused committee that has been in place since the early 2000s. The API ITSS is comprised of CISOs and a range of other cybersecurity professionals. The ITSS provides an opportunity for member companies to work together proactively to address areas of common interest to the industry and to demonstrate that the industry is taking prudent steps to protect cyber infrastructure.[22]

INGAA convenes member organizations through a Cyber and Physical Security Committee to ensure the physical and cybersecurity of natural gas pipeline systems. On a federal regulatory level, the committee primarily works with DHS, TSA, the Federal Energy Regulatory Commission (FERC), DOE, other agencies and Congress to ensure both the safety and reliability of the nation's pipeline network. This group holds security tabletop exercises and participates in information sharing with the government to stay ahead of cyber and physical threats.[23]

AGA's cybersecurity program takes a three-pronged approach to addressing cybersecurity threats to natural gas utilities. The first element, Cybersecurity Assessments, leverages AGA's Peer Cyber Review and Cybersecurity Capability Maturity Model (C2M2) programs to ensure that natural gas utilities of all sizes understand their current cybersecurity posture so that they can prioritize future security investments where they will be the most effective. The second prong, Education and Awareness, is accomplished by fostering a shared understanding of the threat via the AGA-managed DNG-ISAC and by convening utility representatives through AGA's Natural Gas Security Committee to share leading and emerging practices. The third element, Technical and Advocacy Guidance, draws on technical expertise from AGA's Cybersecurity Strategy Task Force to support the development of technical whitepapers, industry standards and policies, and other resources to ensure that all stakeholders - across industry and government - are driving towards a policy and technical environment that supports adaptive and continuous improvement.

AFPM has convened its member companies on a Cybersecurity Subcommittee under an Operational Planning Control and Automation Technologies Committee since 2005. This subcommittee has provided technical feedback on legislation and regulatory efforts. As many current cybersecurity issues need not only technical feedback, but feedback from higher levels within member companies, AFPM also engages members of a Government Regulations Committee on priority issues related to cybersecurity.[24]

IADC convenes its member companies through its Cybersecurity Committee to develop digital easy-to-use, practically applicable and tailored cybersecurity guidelines for drilling assets that are built upon existing industry standards and best practices. The committee reviews existing cybersecurity regulations, industry best practices and standards of relevance for industrial control systems and drilling assets, clearly defining the approach for standards to follow and subsequently moving to align with standards that can be practically applied to drilling assets.[25]

To address the growing risk of cyber threats, ILTA created a Cyber-Threat Resilience Assessment Program to help member companies evaluate their cyber defenses and identify and address vulnerabilities. The program focuses on operating models and skills that help companies build cyber threat resilience into their organization. Companies receive a detailed report that identifies gaps and areas of improvements and practical suggestions. The process also provides an educational and awareness platform for all employees on the topic of cybersecurity.[26]

CYBERSECURITY-FOCUSED EVENTS

Since 2006, API has convened the annual Cybersecurity Conference & Expo in the United States, which brings together over 600 participants including leading cybersecurity experts from natural gas and oil companies, government, academia and marketplace-leading vendors.[27]

Since 2017, API has partnered with the International Association of Oil and Gas Producers (IOGP) to convene the annual API-IOGP Europe Cybersecurity Conference.[28] This event expands the cybersecurity efforts of U.S.-based API members and promotes trans-Atlantic cooperation.

Additionally, API and ONG-ISAC members regularly attended the CyberStrike Workshop developed by DOE's Office of Electricity Delivery and Energy Reliability in collaboration with the Electricity Information Sharing and Analysis Center and Idaho National Lab (INL). The workshop was developed to enhance the ability of energy sector owners and operators in the U.S to prepare for a cyber incident impacting ICS. The training offers attendees a hands-on, simulated demonstration of a cyberattack, drawing from recent real-world cyber incidents. The instruction platform challenges course participants to defend against a cyberattack on the equipment they routinely encounter within their ICS. The CyberStrike workshop is a critical tool for actively enabling cybersecurity solutions to understand and manage the multifaceted interdependencies between the nation's energy infrastructure and other critical infrastructure, and to detect and respond within compressed timelines to prevent highly impactful consequences.[29]

Furthermore, security professionals from AGA's Natural Gas Security Committee, INGAA's Security Committee and the Edison Electric Institute's Security Committee meet jointly twice each year to foster improved coordination across the electric and natural gas subsectors, discuss emerging cyber and physical security trends and share leading practices.

PERSPECTIVES ON POLICYMAKING

VOLUNTARY GUIDELINES AND RECOMMENDATIONS FOR REGULATORY EFFORTS

The reliance upon voluntary mechanisms, including the aforementioned use of proven frameworks and public-private collaboration, rather than compulsory standards or regulations, is the most effective and robust way to bolster the cybersecurity of industry companies and the critical infrastructure they operate. As demonstrated in this paper, industry is already deeply engaged on the issue of cybersecurity and working to stay informed and ahead of our adversaries. With the increasing sophistication and adaptiveness of cyber adversaries, it is essential that industry be afforded the necessary flexibility and agility to respond to a constantly-changing threat landscape and the continuous innovation by cyber criminals.

Natural gas and oil companies support the NIST CSF as the pre-eminent standard for companies' cybersecurity programs and for policymaking globally because it is (a) comprehensive, (b) a risk management approach, (c) scalable to different types and sizes of companies, and (d) widely used across the natural gas and oil industry and other industry sectors.

Cybersecurity regulation must balance the government's interest in guidance and oversight against the risk that static rules will quickly become obsolete. Focusing regulation on one type of attack or business activity could force companies to overweight activities in that direction to the detriment of other needs. This can generate significant unintended consequences stemming from the removal of resources otherwise directed to proactive cybersecurity efforts in order to comply with and respond to regulatory obligations.

Regulatory efforts must also be cognizant that companies operate in many different jurisdictions, whether geographically or by industry sector. Cybersecurity guidance must not be so specific that it cannot accommodate the potential of multiple administrative regimes.

Government must partner with industry to ensure that companies establish and maintain an active and agile cyber defense posture, but it must also recognize the limits of prescriptive mandates in this area and guard against regulatory overreach and the imposition of redundant or conflicting rules.

Industry companies urge policymakers to take a measured and coordinated approach to any potential new cybersecurity laws or regulations for the natural gas and oil industry, ideally based on a common understanding with industry on risks and based on the NIST Cybersecurity Framework.

CONCLUSION

Natural gas and oil companies agree with policymakers and others that cybersecurity of the nation's critical infrastructure is a priority, and take seriously the responsibility to protect it, provide reliable energy for society and safeguard the public and the environment. The industry faces an increasing number of cyberattacks and evolving, sophisticated cyber threats from a variety of malicious actors including nation states, criminal organizations and others. These threats are not unique or new to pipelines; they are prevalent across the energy system, including at coal and nuclear plants.

In recognition of the sophistication and dedication of cyber attackers, as well as the enterprise risk presented by cyberattacks, natural gas and oil companies have developed multi-dimensional "defense-in-depth" approaches to cybersecurity similar to industry's approach to managing risks of safety: a robust governance that integrates Board and executive-level oversight, systematic risk-based management, technology solutions and programs based on best-in-class standards and proven frameworks.

Cybersecurity in the natural gas and oil industry applies throughout the value chain and includes collaboration and communication with government at every point. Companies also participate in information sharing through ISACs and peer-to-peer learning through trade associations to force multiply individual companies' threat analysis assets and provide critical lines of defense.

The reliance upon voluntary mechanisms including proven frameworks and public-private collaboration, rather than compulsory standards or regulations, is the best way to bolster the cybersecurity of industry companies and the critical infrastructure they operate. Cybersecurity regulation must balance the government's interest in guidance and oversight against the risk that static rules will quickly become obsolete. Further, regulation might cause companies to focus their defenses on a limited number of types of attacks or business activities to the detriment of other existing or emerging needs. There also is the risk that such rules might create a window into industry defenses that could be exploited. This can generate significant unintended consequences.

ACRONYMS AND ABBREVIATIONS

DOE	Department of Energy
(AFPM)	American Fuel & Petrochemical Manufacturers
(AGA)	American Gas Association
(API)	American Petroleum Institute
(AOPL)	Association of Oil Pipe Lines
(IADC)	International Association of Drilling Contractors
(ILTA)	International Liquid Terminals Association
(INGAA)	Interstate Natural Gas Association of America
CI	Critical Infrastructure
DDOS	Distributed Denial of Service
DHS	Department of Homeland Security
DHS IP	Department of Homeland Security Office of Infrastructure Protection
DHS ISCD	DHS Infrastructure Security Compliance Division
DHS NCCIC	DHS National Cybersecurity Communications and Integration Center
DHS NPP	DHS National Protection and Programs Directorate
DDMZ	Cyber "Demilitarized Zone"
DNG-ISAC	Downstream Natural Gas Information Sharing and Analysis Center
DOT	Department of Transportation
E-ISAC	Electricity Information Sharing and Analysis Center
FERC	Federal Energy Regulatory Commission
FIRST TLP	Forum of Incident Response and Security Teams Traffic Light Protocol
GRF	Global Resilience Federation
IACS	Industrial Automation and Control Systems
IAM	Identity Access Management
IC	U.S. Intelligence Community
ICS	Industrial Control System(s)
IMTC	API's Information Management and Technology Committee
INL	Idaho National Lab Electricity Information Sharing and Analysis Center
IOC	Indicators of Compromise
IOGP	International Association of Oil and Gas Producers
IP	Intellectual Property
IPS	ntrusion Prevention System(s)
ISAC/ISACs	Information Sharing Analysis Center(s)
IT	Information Technology
ITSS	API's Information Technology Security Subcommittee
LNG	Liquified Natural Gas
NCCIC	NIST's National Cybersecurity & Communications Integration Center
NCCOE	National Cybersecurity Center of Excellence
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
ONG	Oil and Natural Gas
ONG-ISAC	Oil and Natural Gas Information Sharing and Analysis Center
OS	Operating System
OT	Operational Technology
PCD	Process Control Domain

ACRONYMS AND ABBREVIATIONS

PCN	Process Control Network
PHMSA	Department of Transportation Pipeline and Hazardous Materials Safety Administration
QPS	Quick Pulse Survey
RFI	Request for Information
SIEM	Security Information and Event Management
SOC	Security Operations Center
TSA	Transportation Security Administration
TTPs	Techniques, Tactics and Procedures
VPN	Virtual Private Network(s)

APPENDICES

APPENDIX A: NIST CYBERSECURITY FRAMEWORK

The five core functions of the NIST CSF provide a base by which companies can structure comprehensive cybersecurity programs. These five programmatic areas are:

- **IDENTIFY:** The identification and understanding of asset management, business environment, governance, risk assessment and risk management strategy to support operational risk decisions.[30]

- **PROTECT:** The establishment of access controls, implementation of cybersecurity awareness training, secure management of data, maintenance and usage of information protection processes and procedures, maintenance and repair of industrial control and information system components, and secure management of protective technical solutions.[31]

- **DETECT:** The detection of anomalous activity and understanding of the potential impact of events, monitoring of information systems and assets and verification of effectiveness of protective measures, and maintenance and testing of detection processes and procedures.[32]

- **RESPOND:** The execution and maintenance of response processes and procedures, coordination of response activities with internal and external stakeholders, conducting of analysis to ensure adequate response and support recovery activities, performance of activities to prevent expansion of an event, mitigate its effects and eradicate the incident, and improvement of organizational response activities.[33]

- **RECOVER:** The execution of recovery processes and procedures to ensure timely restoration of systems or assets affected by cybersecurity events, improvement of recovery planning and processes by incorporating lessons learned into future activities, and coordination of restoration activities with internal and external parties.[33]

APPENDIX B: CRITICAL TECHNOLOGY SYSTEM COMPONENTS

The nine critical system areas that typically comprise a natural gas and oil production company are:

- **NETWORK SECURITY:** Measures taken to protect a communications pathway from unauthorized access to, and accidental or willful interference of, regular operations.[34]

- **IDENTITY AND ACCESS MANAGEMENT (IAM):** The cybersecurity discipline that enables the right individuals to access the right resources at the right times for the right reasons. IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous internal requirements. This security practice is a crucial undertaking for the natural gas and oil industry as it is for any business. It is increasingly business-aligned, and it requires business skills, not just technical expertise.[36]

- **DATA PROTECTION:** Securing digital data, such as those in a database, from destructive forces and from the unwanted actions of unauthorized users, such as a cyberattack or a data breach.[37] Data protection includes user-facing areas such as the reporting of phishing attempts and email scanning as well as system areas like data leakage protection, database protection and automated data categorization.

- **APPLICATION SECURITY:** Measures taken to protect an application or website from attack, including static application scanning of web, non-web and mobile applications as well as web application firewalls.

- **ENDPOINT SECURITY:** The process of securing the various endpoints on a network including mobile devices, laptops and desktops, as well as hardware such as servers in a data center, and addressing the risks presented by devices connecting to an enterprise network.[38] Increasingly important with greater use of mobile devices, endpoint security protects the corporate network in addition to allowing the endpoint device to operate outside of the network – accessing the cloud or other services – without being easily compromised.

- **VULNERABILITY MANAGEMENT:** The ongoing practice of identifying, classifying, remediating, and mitigating vulnerabilities, particularly in software as well as firmware.[39]

- **THREAT PROTECTION:** A category of cybersecurity solutions that defend against malware or hacking-based attacks targeting sensitive data.[40]

- **RISK AND COMPLIANCE:** The investigation of external and internal threats that could compromise assets, and the implementation of effective internal policies for mitigating risks and cybersecurity and remediation measures in organizations.[41]

- **FORENSICS AND INSIDER RISK:** Digital forensics encompasses the recovery and investigation of material found in digital devices.[42] Insider risk management includes activities such as user behavior analytics and/or endpoint monitoring intended to detect potential malicious activities by a current or former employee, contractor or other person who has or had authorized access to an organization's network systems, data or premises.

APPENDIX C: GOVERNMENT AND REGULATORY BODIES COVERING AND/ OR WORKING WITH INDUSTRY

Transportation Security Administration (TSA)

Government efforts related to pipeline security are covered by the TSA's Office of Security Policy and Industry Engagement's Surface Division. With the assistance of industry and government members of the Pipeline Sector and Government Coordinating Councils, industry association representatives, and other interested parties, TSA developed the Pipeline Security Guidelines. Utilizing a similar industry and government collaborative approach, these guidelines are regularly updated to reflect the advancement of security practices to meet the ever-changing threat environment in both the physical and cybersecurity realms.[43]

Natural gas and oil companies provided input to TSA as it developed and updated the Pipeline Security Guidelines. Pipeline operators also partner with TSA through its Pipeline Corporate Security Review program as TSA has completed reviews of all the nation's top 100 pipeline systems, which transport 84 percent of the nation's energy.[44]

Department of Homeland Security (DHS)

DHS leads the Federal government's efforts to secure our nation's critical infrastructure by working with owners and operators to prepare for, prevent, mitigate and respond to threats.[45] In partnership with industry, the DHS Office of Infrastructure Protection (IP) division of the National Protection and Programs Directorate (NPPD) leads and coordinates national programs and policies on critical infrastructure security and resilience. The office conducts and facilitates vulnerability and consequence assessments to help critical infrastructure owners and operators and state, local, tribal and territorial partners understand and address risks to critical infrastructure. IP provides information on emerging threats and hazards so that appropriate actions can be taken. The office also offers tools and training to help partners such as the natural gas and oil industry manage the risks to their assets, systems and networks.[46]

DHS operates the National Cybersecurity & Communications Center (NCCIC), which serves as the hub for information sharing of cyber threats to-and-from the US Intelligence Community and natural gas and oil companies, primarily through the ONG-ISAC. Cyber threat analysts in the security operations centers of the member companies of the ONG-ISAC share and receive cyber threat indicators with their counterpart analysts in the NCCIC and in US intelligence agencies.

Industry also works with the DHS Infrastructure Security Compliance Division (ISCD) of the Office of Infrastructure Protection of the National Protection.

U.S. Coast Guard (USCG)

USCG oversees both physical and cybersecurity for the natural gas and oil industry through its authorities under the Maritime Transportation Security Act (MTSA) of 2002. Through MTSA, USCG is tasked with the regulation of all marine terminals used to load or unload vessels that transport unrefined petroleum, petroleum products, or liquefied natural gas (LNG). USCG jurisdiction extends from the first isolation valve inside of the secondary containment of the marine terminal to the vessel.[47]

The USCG's work on cybersecurity also includes a mandate, per the 2018 FAA Reauthorization, for it to create a Cybersecurity Maritime Risk Acceptance Model (Cyber MSRAM).

USCG is developing a Navigation and Vessel Inspection Circular (NVIC) titled "Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act- Regulated Facilities" focused on the prevention of "[c]yber attacks [targeting] industrial control systems [that] could kill or injure workers, damage equipment, expose the public and the environment to harmful pollutants, and lead to extensive economic damage."[48] Once finalized, this NVIC on cybersecurity will prompt companies that operate natural gas and oil facilities under USCG jurisdiction to take certain steps to address cyber risks.

In addition, USCG has developed a series of "Profiles"for cybersecurity that provide guidance on implementation of the NIST CSF.[49] The natural gas and oil industry worked closely with USCG and the NIST National Cybersecurity Center of Excellence to develop cybersecurity Profiles on Maritime Bulk Liquid Transfer – security ICS used to transfer hydrocarbons in a maritime environment – and Offshore Operations – offshore natural gas and oil exploration and production.[50,51]

Cybersecurity experts from natural gas and oil companies have worked collaboratively with the USCG and their advisors from the NIST National Cybersecurity Center of Excellence (NCCOE) and from The MITRE Corporation to develop the cybersecurity Profiles. Together, these experts co-defined the mission critical objectives of natural gas and oil facilities and operations and defined the aspects of the NIST CSF that should be emphasized by companies to mitigate the risks that a cyber attack could compromise these mission objectives.

Department of Energy (DOE)

Industry works closely with DOE to protect against cyber and physical attacks on U.S. energy infrastructure, ensure worker health and safety and provide training tools and procedures for emergency response and preparedness.[52]

This partnership is exemplified by industry's collaboration with DOE to provide rapid response to significant recent cyberattacks including WannaCry and NotPetya. Furthermore, through open communication between industry and DOE's Office of Cybersecurity, Energy Security and Emergency Response, both parties can better address the emerging threats of tomorrow to protect the reliable flow of energy to Americans and improving energy infrastructure security.[53]

The natural gas and oil industry also collaborates with DOE by participating in the training and research of the DOE National Laboratories. Cybersecurity personnel from the natural gas and oil industry participate regularly in the ICS Cybersecurity Training offered by the Idaho National Laboratory. Natural gas and oil companies also participate in several DOE-sponsored research projects of the "Cybersecurity for Energy Delivery Systems (CEDS)" and other applied research projects, modeling and studies by various DOE National Labs.

Oil and Natural Gas Subsector Coordinating Council (ONG SCC) and Energy Sector Government Coordinating Council (EGCC)

Industry is fundamentally engaged with the ONG SCC and EGCC, information-sharing bodies that cut across virtually all federal agencies involved in cybersecurity related to the natural gas and oil industry. The ONG SCC provides a venue for industry owners and operators to discuss sector-wide security programs, procedures and processes, exchange information and assess accomplishments and progress toward continuous improvement in the protection of the sector's critical infrastructure. The EGCC provides a private forum for effective coordination of security strategies as well as activities, policies and communication across the sector to support the nation's homeland security mission. The EGCC endeavors to serve as a single point of contact to facilitate communication between the government

and the private sector when preparing for and responding to issues and threats resulting from physical, cyber or weather-related occurrences impacting the energy sector.

APPENDIX D: INFORMATION SHARING

Forum of Incident Response and Security Teams (FIRST) Traffic Light Protocol (TLP) definitions:[54]

COLOR	WHEN SHOULD IT BE USED?	HOW MAY IT BE SHARED?
TLP:RED 🔴 ⚪ ⚪ **Not for disclosure, Restricted to participants only.**	Sources may use **TLP:RED** when Information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share **TLP:RED** Information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, **TLP:RED** information is limited to those present at the meeting. In most circumstances, **TLP:RED** should be exchanged verbally or in person.
TLP:AMBER ⚪ 🟡 ⚪ **Limited disclosure, Restricted to participants' organizations.**	Sources may use **TLP:AMBER** when Information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share **TLP:AMBER** information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing; these must be adhered to.**
TLP:GREEN ⚪ ⚪ 🟢 **Limited disclosure, restricted to the Community**	Sources may use **TLP:GREEN** when Information is useful for the awareness of all participating organ organizations as well as with peers with in the broader community or sector.	Recipients may share **TLP:GREEN** Information with peers and partner organizations within their sector or Community , but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP:GREEN** information may not be released outside of the community.
TLP:WHITE ⚪ ⚪ ⚪ **Disclosure is not Limited.**	Sources may use **TLP:WHITE** when information carries minimal or no Foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restrictions.

ONG-ISAC AND DNG-ISAC WORK PRODUCTS

PRODUCT	TLP LEVEL	FREQUENCY	DESCRIPTION
Automated Information Sharing*	Amber	Real-time	Machine speed solutions to facilitate the collection of cyber threat intelligence
Daily Cyber Vulnerabilities	Green	Daily	Highlights IT and ICS-specific vulnerabilities
Trusted Third-Party Reports	Amber	Weekly	Publishes trusted third-party reports on relevant sector-specific topics
Case Studies*	White/Green	Quarterly	The ONG-ISAC contributes collective intelligence on a variety of cyber hot topics
Annual Report*	Green	Annually	Highlights ONG-ISAC's activities over a yearly period
Collective Intelligence Report	White/Green	As needed	Technical analysis report of open-source intelligence
Cyber Threat Report	Green/Amber	As needed	Provides details on specific threats to any component or entity in ONG industry
Cyber Incident Report	Green/Amber	As needed	Reports on new/evolving cybersecurity breaches or incidents
Trusted Partner Submissions	Green	As needed	Submitted from cross-sector trusted partners reviewed by the ISACs
Member Submissions	Green/Amber	As needed	Shared immediately for situational awareness within the community
Ad-Hoc Reports	Green/Amber	As needed	Focused on urgent physical and/or cyberattacks impacting the industry
Request for Information (RFI)	Amber	As needed	The ISACs facilitates the exchange of information related to relevant topics
Quick Pulse Survey (QPS)*	Amber	As needed	The ONG-ISAC facilitates the exchange of information related to relevant topics
Bi-Monthly	White	Bi-Monthly	The ISACs contributes technical analysis to the Global Resilience Federation (GRF) bi-monthly report

*Work product specific to only the ONG-ISAC

REFERENCES

1. **Department of Homeland Security,** National Cybersecurity and Communications Integration Center, Industrial Control Systems Cyber Emergency Response Team, “FY2016 ICS-CERT Year in Review”, https://ics-cert.uscert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf

2. **Department of Homeland Security,** “Sector Risk Snapshot,” May 2014, https://www.hsdl.org/?view&did=754033

3. **U.S. Department of Energy,** Office of Electricity Delivery and Energy Reliability, “Energy Sector Cybersecurity Framework Implementation Guidance”, January 2015, https://www.energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf

4. **National Institute of Standards and Technology,** News, April 2018, https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

5. **Oil and Natural Gas Sector Coordinating Council,** “2015 Cybersecurity Survey”

6. **National Institute of Standards and Technology Cybersecurity Framework,** Perspectives on the Framework, https://www.nist.gov/cyberframework/perspectives

7. **ISA99 Committee,** Manufacturing and Control Systems Security Part 1: Models and Terminology, http://isa99.isa.org/

8. **Department of Homeland Security,** National Cybersecurity and Communications Integration Center, Industrial Control Systems Cyber Emergency Response Team, “Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies”, 2016, https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

9. **Department of Energy,** Cybersecurity Capability Maturity Model (C2M2), “https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-0

10. **U.S. Government.** “The Consolidate Appropriations Act, 2016,” https://www.congress.gov/bill/114th-congress/house-bill/2029?q=%7B%22search%22%3A%5B%22%5C%22cybersecurity+act+of+2015%5C%22%22%5D%7D&r=2

11. **Department of Homeland Security,** Executive Order 13636, “Presidential Directive 21 Fact Sheet,” https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf

12. Ibid.

13. **White House,** Executive Orders, “Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure”, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

14. Ibid.

15. **Downstream Natural Gas Information Sharing and Analysis Center,** https://www.dngisac.com/

16. **Oil and Natural Gas Information Sharing Analysis Center,** http://ongisac.org/

17. **United States Computer Emergency Readiness Team,** Traffic Light Protocols. https://www.us-cert.gov/tlp

18. **Oil and Natural Gas Information Sharing Analysis Center,** http://ongisac.org/

19. Ibid.

20. **Department of Homeland Security**, Oil and Natural Gas Subsector Coordinating Council, “Governance Principles and Operating Procedures,” https://www.dhs.gov/sites/default/files/publications/Energy-ONG-SCC-Charter-2015-508.pdf

21. **API Information Technology Committees,** https://www.api.org/about/organization/committees/information-technology

22. Ibid.

23. **Interstate Natural Gas Association of America,** Cyber and Physical Security Committee, https://www.ingaa.org/about/ingaa-committees/29297.aspx

24. **American Fuel and Petrochemical Manufacturers**, Cybersecurity, https://www.afpm.org/Cybersecurity/

25. **International Association of Drilling Contractors**, Cybersecurity Committee, http://www.iadc.org/cybersecurity-committee/

26. **International Liquid Terminals Association**, Cybersecurity, https://www.ilta.org/ILTA/Advocacy/Cybersecurity/ILTA/Advocacy/Cybersecurity.aspx

27. **API, Policy and Issues,** Cybersecurity. https://www.api.org/news-policy-and-issues/cybersecurity

28. Ibid.

29. **Public Power Association,** DOE CyberStrike Workshop. https://www.publicpower.org/event/session/pre-and-post-conference-seminars

30. **NIST Cybersecurity Framework Resources,** Identify, https://www.nist.gov/cyberframework/identify

31. **NIST Cybersecurity Framework Resources,** Protect, https://www.nist.gov/cyberframework/protect

32. **NIST Cybersecurity Framework Resources,** Detect, https://www.nist.gov/cyberframework/detect

33. **NIST Cybersecurity Framework Resources,** Respond, https://www.nist.gov/cyberframework/respond

34. **NIST Cybersecurity Framework Resources,** Recover, https://www.nist.gov/cyberframework/recover

35. **Gartner IT Glossary,** Network Security, https://www.gartner.com/it-glossary/network-security

36. **Gartner IT Glossary,** Identity and Access Management, https://www.gartner.com/it-glossary/identity-and-access-management-iam

37. **Summers, G. (2004). Data and databases.** In: Koehne, H Developing Databases with Access: Nelson Australia Pty Limited. p4-5.

38. **Digital Guardian,** Data Protection 101: What is endpoint security? https://digitalguardian.com/blog/what-endpoint-security-data-protection-101

39. **Foreman, P: Vulnerability Management,** page 1. Taylor & Francis Group, 2010. ISBN 978-1-4398-0150-5

40. **Digital Guardian,** https://digitalguardian.com/blog/what-advanced-threat-protection-atp

41. **NICCS National Initiative for Cybersecurity Careers and Studies,** Central Michigan University Training Program on Governance, Risk and Compliance in Cybersecurity, https://niccs.us-cert.gov/training/search/central-michigan-university/governance-risk-compliance-cybersecurity

42. **Carrier, B (2001). "Defining digital forensic examination and analysis tools".** Digital Research Workshop II. Archived from the original on 15 October 2012.

43. **Transportation Security Administration Office of Security Policy and Industry Engagement's Surface Division,** Pipeline Security Guidelines, March 2018. https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf

44. **Transportation Security Administration,** "Securing and Protecting Our Nation's Pipelines," 2016, https://www.tsa.gov/news/releases/2016/07/11/securing-and-protecting-our-nations-pipelines

45. **Department of Homeland Security,** Executive Order 13636, Presidential Directive 21 Fact Sheet. https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf

46. **Department of Homeland Security Office of Infrastructure Protection**, https://www.dhs.gov/office-infrastructure-protection

47. **Department of Transportation Pipeline and Hazardous Materials Safety Administration,** Marine Terminals Fact Sheet, https://primis.phmsa.dot.gov/comm/FactSheets/FSMarineTerminals.htm

48. **U.S. Coast Guard,** https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/Domestic-Ports-Division/cybersecurity/

49. **U.S. Coast Guard,** "Cybersecurity Framework Profiles Overview," 2018, https://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/Cyber%20Profiles%20Overview.docx?ver=2018-01-10-143126-467

50. **U.S. Coast Guard,** "Appendix A. Maritime Bulk Liquid Transfer Profile," https://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/Appendix%20A.%20Maritime%20Bulk%20Liquids%20Transfer%20Profile.docx?ver=2018-01-10-141700-073

51. **U.S. Coast Guard,** "Appendix B. Offshore Operations Profile," https://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/Appendix%20B.%20Offshore%20Operations%20Profile.docx?ver=2018-01-10-140108-557b

52. **Department of Energy,** National Security and Safety, https://www.energy.gov/national-security-safety

53. **Department of Energy Office of Cybersecurity,** Energy Security and Emergency Response, https://www.energy.gov/ceser/office-cybersecurity-energy-security-and-emergency-response

54. **United States Computer Emergency Readiness Team,** Traffic Light Protocols. https://www.us-cert.gov/tlp

NOTES

6426.74 130560 130560 130560
3716.8 6381.7
130560 130560 130560
4.8 488.6 2 0.39 2}
39 495.6 2 1.53 2}
5.6 509.2 2.8 1.89 2.8}
519.6 2.8 1.7 2.8}