GOVERNANCE

Accountability & Compensation

Rooted in Chesapeake's core values and industry-best management practices, our strong governance programs provide clear guidelines to define ethical behavior at every level. This commitment to rigorous corporate governance drives accountability, starting with our Board of Directors.

Core Values

Integrity and Trust	Respect	Transparency and Open Communication	Commercial Focus	Change Leadership

Director Qualifications and Experience

Chesapeake's Board is comprised of experienced business and technical leaders who provide high-level oversight of company activities. Accountable to our shareholders, our directors share different viewpoints and backgrounds, contributing to better dialogue and decision-making and generating more successful outcomes.

	Wichterich	Dell'Osso	Duncan	Duster	Emerson	Gallagher	Steck
Operational / Management Leadership	X	X	X	X	X	X	X
Current and/or Former Public Company CEO or Board Chair	X	X	X	X		X	X
Strategic Planning / Risk Management	X	X	X	X	X	X	X
Exploration and Production Industry	X	X	X	X	X	X	X
Environment / Sustainability and Safety Management		X	X		X	X	
International	X		X	X	X		X
Technology, Engineering and Geoscience			X	X		X	X
Financial Oversight and Accounting	X	X	X	X		X	X
Government / Legal				X	X		
Cybersecurity Oversight		X	X	X		X	

Board Committees

Our Board has four standing committees, each with a charter that articulates the committee's respective purpose and responsibilities.

- Audit
- Compensation
- Nominating and Corporate Governance
- Environmental and Social Governance

Diverse directors hold critical leadership positions as chairs of our ESG Committee and Audit Committee.

Engaging with Our Board

The Board takes the feedback of our stakeholders seriously. Our Director Access Line (866-291-3401) allows our shareholders and other interested parties to leave messages for individual directors or our entire Board. Shareholders may also email or send written communications. All forms of contact are promptly reviewed and forwarded to the appropriate contact at the Board level or within the company.

Independence

5 directors are independent

Director Distinctions

100% of Audit Committee members qualify as financial experts

Average Age

54 years old

Gender Diversity

14% of directors identify as women

Ethnic Diversity

14% of directors identify as racially diverse

Total Diversity

29% of directors identify as diverse

Sustainability Oversight

The Board's ESG Committee is dedicated to sustainability oversight and advising the Board-at-large on emerging ESG issues. This committee provides leadership and strategic counsel on all aspects of the company's ESG-related performance, including employee health and safety, social governance, climate-related risks and opportunities, environmental performance and stakeholder engagement.

Accountability at All Levels

BOARD OF DIRECTORS

BOARD COMMITTEES
ESG Committee

CHIEF EXECUTIVE OFFICER

ESG ADVISORY BOARD
Senior leaders across the company who provide oversight of ESG performance and disclosures

ESG WORKING GROUPS
Subject matter experts across multiple disciplines who help to implement the company's ESG strategy

OPERATIONAL AND SERVICE GROUPS

Board ESG Committee:

- Meets at least four times per year to discuss environmental, health and safety, and social matters
- 100% attendance at 2023 meetings
- Chaired by an independent Board member
- Reports quarterly to the Board on sustainability issues, including climate

Supporting the Board's sustainability oversight are two employee committees who meet quarterly and are responsible for the execution of ESG programs and procedures.

Tying Compensation to Performance and ESG

Our executive and employee compensation program not only attracts and retains top talent but is uncompromising in its performance demands. Program highlights include:

Long-Term Incentive Program (LTIP):

- Paid entirely in equity, 75% of executive award value is linked to total shareholder returns

Annual Incentive Program (AIP):

- Aligns payout with the value drivers and discipline our shareholders value including environmental and safety excellence, delivering free cash flow, lowering per unit operating costs, enhancing capital efficiency and reducing base production declines
- Of the total amounts payable under the 2023 AIP, 20% were based on the attainment of certain companywide strategic leadership goals
- Failure to meet environmental and safety performance thresholds caps the AIP payout at target for all other metrics regardless of results

Setting and Upholding High Standards of Conduct

Each Chesapeake director, officer and employee, regardless of position, must abide by Chesapeake's Code of Business Conduct (Code), which is structured around our core values. All new employees learn about the Code during their onboarding process.

Each year employees must acknowledge their understanding of the Code and related policies and the high standards expected of them. We encourage and expect employees to report conduct that may be unethical, illegal or in violation of the Code, and offer our Ethics and Integrity Helpline, an anonymous, third-party hotline and website, for confidential reporting.

Our Non-Retaliation Policy encourages employees to know their rights (and duty) to raise genuine concerns. Chesapeake does not retaliate against anyone who raises issues in good faith, cooperates with an investigation of a concern or refuses to carry out an instruction that would violate laws or our Code or our core values. Confidentiality is maintained to the fullest extent possible. Retaliation, or threats of retaliation, against employees or business partners will result in disciplinary action, up to and including separation.

All reports of unethical business conduct are investigated and reported to appropriate levels of management and, as appropriate, the Board's Audit Committee. Corrective actions are taken when necessary.

ESG-Related Policies and Positions

Although not exhaustive, the below list highlights those policies and position statements relevant to significant ESG-related topics. Policies and positions that are available to external audiences are linked here.

- Anti-Corruption Policy
- Antitrust Policy and Compliance Manual
- Biodiversity Stewardship Position
- Code of Business Conduct
- Conflict of Interest Policy
- Drug and Alcohol Policy
- Environmental Policy
- Equal Employment Opportunity Policy
- Gifts and Entertainment Policy
- Human Rights Policy
- Information Security Policy
- Insider Trading Policy
- Non-Retaliation Policy
- Protection of Chesapeake Assets Policy
- Safe and Compliant Operations Policy
- Social Media and External Communication Policy
- Supplier Code of Conduct
- Water Stewardship Position
- Zero Tolerance Anti-Harassment, Anti-Discrimination and No Violence in the Workplace Policy

Risk Management

Through our Enterprise Risk Management (ERM) program and internal operational audits, Chesapeake takes a comprehensive approach to identifying, assessing and managing sustainability-related risks.

Risk Management Process

We use the Three Lines of Defense as our framework for risk management, helping ensure employees play a role in risk identification and mitigation.

1st Line of Defense	2nd Line of Defense	3rd Line of Defense
Owns and Manages Risk *(Operational and Service Groups)*	Oversees Risks, Controls and Compliance *(Internal Controls)*	Provides Independent Assurance *(Internal Audit)*
Encourages identification and control of risks at the front lines Internal risk owners (senior managers and subject matter experts) regularly review and assess company risks Annual risk survey asks employees throughout the organization to review existing risk drivers and identify emerging risks	Provides impartial enterprise risk and compliance analyses	Uses a standardized, objective process to identify risk-based audits of department and business unit controls and processes Reports directly to the Board Audit Committee

Risk Measurement Characteristics

On a quarterly basis, members of our Internal Audit and Internal Controls teams and risk owners review all identified enterprise-level risks according to our risk-measurement characteristics:

- **Impact:** The expected effects of a risk on an organization
- **Likelihood:** The potential for a risk to occur in various scenarios
- **Velocity:** The speed at which a risk could impact an organization

Enterprise risks are also regularly evaluated by our executive team and Board with quarterly ERM updates provided to the Board Audit Committee. The Board ESG Committee governs ESG-related risks. This comprehensive reporting allows Board committees to analyze the company's material risks and direct business strategies accordingly.

Risk Mitigation and Business Continuity

If it's determined that a risk requires mitigation, management develops and executes specific plans to reduce the risk to an acceptable level. Mitigation options include:

- Adopting or enhancing corporate policies
- Implementing new or enhancing existing procedures
- Developing contingency plans
- Adopting technology solutions

Our business continuity and disaster recovery programs are examples of Chesapeake's enterprise-level, risk-mitigation controls. Through these programs, a cross-functional task force assesses the business impacts of certain risks and develops response and recovery plans to reduce potential interruptions.

Protecting employees and maintaining operations during sustained incidents (such as natural disasters, pandemics and other disruptive events) is the primary goal of our business continuity program.

We consider climate-related risks as part of our ERM process, helping to ensure an effective review of the issue and its physical and transitional risks. To learn more, read our climate report.

Ready and Responsive in Emergencies

Should a risk escalate into an emergency, our Emergency Response Plan (ERP) provides employees with the framework and action steps critical for responding to an incident in a safe, rapid and efficient manner. Our priorities are protecting people and the environment, minimizing impact and limiting operational losses, in tandem with regulatory compliance.

Our ERP is built on:

- Well-trained personnel responding in a tiered approach based on incident level
- An assessment of potential scenarios followed by drills to help ensure response readiness
- Engaged partnerships with local responders and professional emergency response contractors
- Scalable, flexible and adaptable operational capabilities
- A unified Incident Command

As part of our robust ERP, Chesapeake utilizes the National Incident Management System (NIMS), a nationwide incident response template, to work cooperatively with local, state and federal agencies in the event of an emergency, regardless of location. NIMS also allows for the integration of facilities, equipment, personnel and communications to create common processes for planning and managing resources, all of which expedites the emergency response.

Field employees are trained in NIMS level 100 and 200 to provide a clear understanding of their responsibilities in an emergency. We also develop and prepare specialized teams of employees — Local Emergency Response Teams (LERT) — to assume command and control of an incident safely and efficiently. All of our operational areas have LERT teams made up of highly trained Health, Safety, Environment and Regulatory (HSER), Security and Operations employees who are ready to respond in the event of an emergency.

Supporting First Responders

We recognize that a strong ERP is further strengthened with a prepared local first responder team. For this reason, and to show our appreciation to the men and women who serve our local communities, we offer a number of partnership opportunities.

Relationship-Building

Members of our Emergency Preparedness and Response group and Operations teams interact regularly with local responders to understand department capabilities and establish partnerships.

Training

We also offer information sessions covering drilling, completions and production site equipment, potential hazards and key industry terminology to provide valuable safety awareness for fire responders. This training often includes site visits to all phases of our operations and discussion of the various scenario types they might encounter. Chesapeake hosts LERT trainings (simulated emergencies) at least twice a year in each of our business units. In 2023, 92 attendees participated in 7 exercises.

Resources

Many of our operational sites are served by rural, often volunteer, fire departments. Given their limited resources, we donate financially to meet local department needs and enhance community safety.

Security

Protecting our people and securing our assets are the goals of our security program. We monitor our on-site locations consistently for safety and security across our assets.

Our on-site security personnel include Chesapeake employees as well as third-party partners, many of whom are off-duty or former law enforcement officers. These security team members have established relationships with local first responders, as well as state and federal officials, for a joint approach to keeping Chesapeake sites and surrounding communities safe.

Site personnel (whether employees or contractors) must abide by our Code, Human Rights Policy and other policies governing health, environment and safety. These policies and procedures prohibit the possession or use of weapons, drugs or alcohol on company property and other undesirable or illegal workplace behaviors including money laundering and the financing of terrorism.

Any employee or partner not following these policies, or otherwise threatening the safety of our operations, will be removed. Our areas of operations are regulated by U.S. law, mitigating material risks related to security threats, terrorism or armed conflict, and company attacks.

Security Services

Our security personnel offer a number of services to protect our co-workers and assets. These services include:

- Code investigations
- Commercial kickback prevention
- Conflict-of-interest management
- Data loss protection
- Drug and alcohol compliance
- Due diligence investigations
- Entertainment and gift compliance
- Fraud prevention
- Forensic auditing
- Internet threats
- Operations emergency call-in
- Personnel protection
- Physical security
- Risk management
- Site assessment and protection
- Supply Chain onboarding
- Theft prevention
- Travel compliance
- Workplace violence prevention

Going Beyond the Traditional Security Role

In 2023, Chesapeake's Security team members partnered with our Operations Support Center to evaluate on-site camera analytics to detect spills or conditions that could cause a spill at our salt water disposal facilities. The enhanced site monitoring, facilitated by both teams, resulted in several 'good catches' that mitigated spill severity through early detection.

Managing Cybersecurity Risks

Information technology touches all aspects of our operations and cybersecurity risks continue to evolve. We understand these risks and are proactive about the security of our assets and the welfare of our employees. Through a comprehensive protection and defense strategy, we continue to improve upon an extensive framework of controls to detect, identify and protect against potential cyberattacks.

We have developed and implemented a cybersecurity risk management program intended to protect the confidentiality, integrity and availability of our critical systems and information. We integrate our cybersecurity risk management program into our overall enterprise risk management program, and share common methodologies, reporting channels and governance processes that apply across other risk areas within our ERM program.

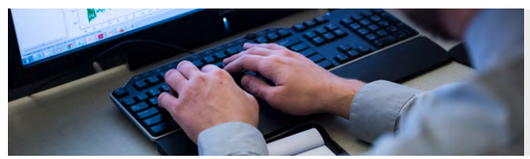
Our cybersecurity risk management program includes, but is not limited to:

- Risk assessments designed to help identify material cybersecurity risks to our critical systems and information.
- A security team principally responsible for managing our cybersecurity risk assessment processes, our security controls and our response to cybersecurity incidents.
- External service providers, where appropriate, to assess, test or otherwise assist with aspects of our security processes.
- Systems for protecting information technology systems and monitoring for suspicious events, such as threat protection, firewall and anti-virus software.
- Cybersecurity awareness training for our employees and contractors, including incident response personnel and senior management.
- A cybersecurity incident response plan that includes procedures for responding to cybersecurity incidents.
- A third-party risk management process for service providers, suppliers, software and vendors who access our data and/or systems.

Our Board considers cybersecurity risk as a critical part of the enterprise and has delegated it to its Audit Committee. Our Audit Committee oversees management's implementation of our cybersecurity risk management program and receives quarterly updates from management on cyber threats, potential vulnerabilities and the proactive security programs in place to protect our operations. In addition, management updates our Audit Committee, as necessary, regarding any material cybersecurity incidents.

Cybersecurity Protection Layers

Network and Application Security	Data Protection	Risk and Compliance
Protecting company networks and applications from attack and inappropriate access	Preventing data breaches and ransomware attacks through security layers and threat hunting	Managed as an enterprise risk, accountable to top company leadership
Identity and Access Management	**Incident Response and Business Recovery**	**Cybersecurity Awareness**
Protecting the attributes of individual digital identities	Cohesive planning to respond quickly and minimize impact	Training employees and contractors to help prevent cyber events



We have had no major cybersecurity breaches or system compromises in the last three years.

Should an incident occur, our Cybersecurity team has response and recovery plans closely aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework to best protect the data and programs critical to our business. We audit a portion of our information security program every year, using a third-party organization to review our cybersecurity posture from an external perspective.

Increasing Cybersecurity Awareness

As we continue to study and plan for evolving cyber risks, Chesapeake equips our first line of defense — our employees — with up-to-date information. Through targeted communications, annual trainings and cyber exercises, we work to raise cybersecurity awareness among our employees and partners, reminding them of the critical role they play in protecting our digital assets.

Political & Trade Participation

Chesapeake respects the U.S. political process and engages in several ways, including through selective trade associations and an employee Political Action Committee (PAC).

Political Process Engagement

- Employee PAC
- Trade association membership
- State and Federal political consultants

Chesapeake's participation in government affairs and the political process strictly adheres to high ethical standards and the company's core values of respect, integrity and trust. All activities comply with applicable laws and regulations, promote Chesapeake's business strategies and are made without regard for the personal political preferences of employees, officers and directors.

Our Government Affairs team engages in matters of public policy to help advance the company's business goals and interests. The team reports directly to our executive leadership. The Nominating and Corporate Governance Committee of the Board has oversight of Chesapeake's political activity.

PAC Activity

Chesapeake sponsors a PAC that allows eligible employees to voluntarily contribute and promote candidates for public office who support our industry. Our employee-run PAC Board is committed to educating, energizing and empowering our participating employees to become informed voters and actively participate in our political system at all levels of government.

PAC contributions and expenditures are disclosed in filings as required by law and can be accessed through the following organizations:

- Federal Election Commission
- Oklahoma Ethics Commission
- Pennsylvania Department of State
- Louisiana Ethics Administration

Chesapeake encourages but will never require any employee or business partner to make personal political contributions, including to a company-sponsored PAC. We also will never take retaliatory action against or compensate anyone, directly or indirectly, for making any political contributions.

PAC expenditures totaled $57,500 for the calendar year ending Dec. 31, 2023.

Chesapeake does not make corporate contributions to candidates, political campaign committees or Super PACs.

Lobbying and Trade Group Participation

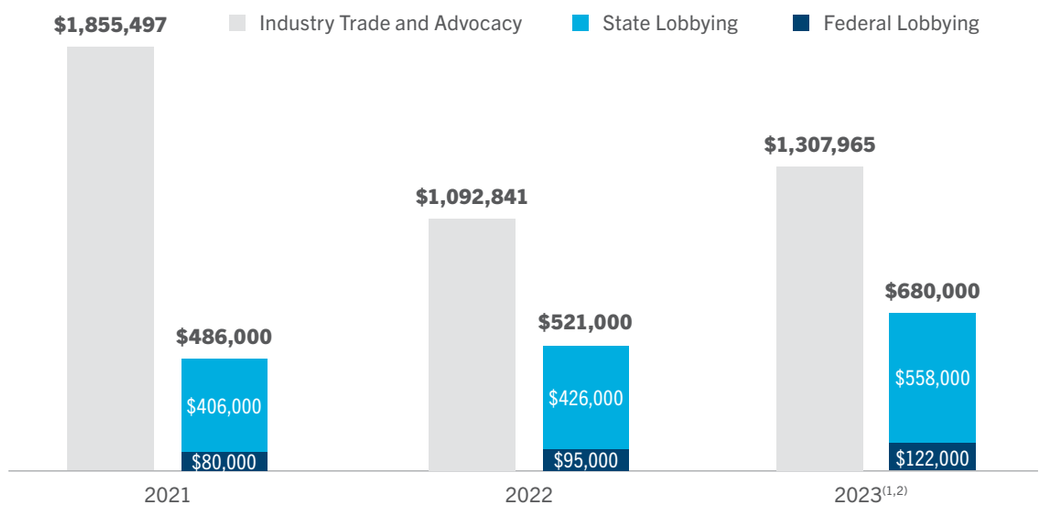
Chesapeake strictly adheres to all federal and state lobbying disclosure laws and we file publicly-available quarterly reports that describe issues lobbied and the amount spent on lobbying activity.

To facilitate our bipartisan lobbying efforts, we partner with external lobbying services. Our engagement is U.S.-only and focuses on advocating for balanced energy policy that is science based, equitable across sectors and helps to deliver affordable and reliable energy.

We're also members of and actively participate in selective federal, state and local trade associations, chambers of commerce and advocacy groups. Some of these groups participate in the political process through educational initiatives and engage in lobbying on important legislative and regulatory decisions that impact Chesapeake.

We don't belong to or financially support non-energy focused tax-exempt organizations such as the American Legislative Exchange Council (ALEC) or the National Conference of State Legislatures (NCSL) that routinely write and endorse model legislation for use in various state legislatures.

Political and Advocacy Expenses



(1) **National and state trade associations and chambers (contributions of $15,000+):** American Exploration and Production Council (AXPC), Columbia Center on Global Energy Policy, Energy Future Initiative (EFI), GTI Energy, Independent Petroleum Association of America (IPAA), Louisiana Mid-Continent Oil and Gas Association (LMOGA), Louisiana Oil and Gas Association (LOGA), Marcellus Shale Coalition (MSC), National Association of Manufacturers (NAM), The Petroleum Alliance of Oklahoma, Pennsylvania Chamber of Business and Industry, State Chamber of Oklahoma, Texas Oil and Gas Association (TXOGA), The USLNG Association (LNG Allies), World 50 Inc.
(2) The majority of 2023 lobbying expenses were external.