**HUNTINGTON INGALLS INDUSTRIES, INC.**
**CYBERSECURITY COMMITTEE CHARTER**

## Purpose

The Cybersecurity Committee (the "Committee") of the Board of Directors (the "Board") of Huntington Ingalls Industries, Inc. (the "Company") is organized and established by and among the Board for the purpose of assisting the Board in carrying out its oversight responsibilities with respect to the Company's systems (*i.e.*, processes, policies, controls and procedures) to (1) identify, assess and mitigate risks related to cybersecurity and information technology, (2) protect against security breaches and safeguard the Company's IT infrastructure, other critical assets and data and confidential information in the Company's possession or custody, (3) respond to and manage cybersecurity threats, including data breach incidents, and (4) comply with legal and regulatory requirements governing data security.

## Organization

The Committee shall consist of at least three directors, each of whom shall be independent. For purposes hereof, an "independent" director is a director who meets the New York Stock Exchange definition of "independence," as determined by the Board.

Members of the Committee, including the chair, are appointed by the Board based on the recommendations of the Governance and Policy Committee. The Board may remove any Committee member at any time, with or without cause. Any vacancies on the Committee will be filled by the Board based on the recommendations of the Governance and Policy Committee.

## Meetings

The Committee shall meet as often as it deems necessary in order to perform its responsibilities. The Committee shall also meet in an executive session of only the Committee members (and advisors) on a regular basis.

A majority of the members of the Committee shall constitute a quorum for any meeting. Any action of a majority of the members of the Committee present at any meeting at which a quorum is present shall be an action of the Committee. The Committee may also act by unanimous written consent in lieu of a meeting.

The Committee shall maintain written minutes of its meetings. These minutes shall be filed with the minutes of the meetings of the Board. All actions by the Committee shall be reported to the Board at the Board meeting next succeeding such Committee actions.

## Duties and Responsibilities

The Committee shall discharge its responsibilities and shall assess the information provided to it by the Company's management and others, in accordance with its business judgment.

The Committee's duties and responsibilities include the following:

*Strategy & Governance*

1. Regularly review with management the Company's cybersecurity leadership structure.

2. Receive reports from management on a periodic basis regarding the current state of the organization's cybersecurity strategy and framework and its alignment with the Company's corporate business strategy.

3. Review and discuss with management the appropriateness and adequacy of the Company's cyber insurance coverage in the event of a cyber incident.

4. Evaluate the prioritization of the Company's cybersecurity investments roadmap based on risk assessments, threat intelligence and organizational priorities.

5. Review and discuss with management the cybersecurity budget for the next fiscal year to evaluate the adequacy of funding and allocation of resources to key cyber initiatives.

6. Review and discuss with management the Company's cybersecurity in AI through upholding ethical, legal, and responsible use of data and AI technologies.

*Risk Management & Compliance*

7. Review and discuss with management threat intelligence sources to evaluate the evolving threat landscape and the potential impact on the organization.

8. Receive reports from management on security events and behavioral analytics for early threat detection.

9. Receive cybersecurity risk "deep dives" based on the results of current risk assessments.

10. Review and discuss with management the cybersecurity postures of third-party vendors and partners.

11. Receive periodic reports from management on the Company's penetration testing to identify and address vulnerabilities in the Company's systems and networks.

12. Review and discuss with management the organization's cybersecurity policies and procedures and compliance with relevant regulations.

13. Receive reports from management on compliance issues or violations and proposed corrective actions.

14. Receive periodic reports from management on the Company's compliance with industry regulations and standards.

*Security Operations*

15. Receive reports from management and evaluate the response to recent incidents, breaches and vulnerabilities and the effectiveness of mitigation efforts, including lessons learned.

16. Review and discuss with management the Company's incident response plan and readiness to address security incidents, which may include tabletop exercises.

17. Review with management the status of ongoing security projects and initiatives.

18. Review with management the Company's information technology disaster recovery capabilities.

19. Receive reports from management on the effectiveness of security awareness programs for employees.

20. Review with management ongoing training initiatives and their impact on reducing security risks.

*Internal Committee*

21. Appoint and delegate authority, as the Committee deems appropriate, to a subcommittee consisting of not less than two members of the Committee.

22. Review this charter at least annually and recommend to the Board any necessary or appropriate amendments.

23. Conduct an annual performance evaluation of the Committee

24. Perform such other duties as may be lawfully delegated by the Board.

Effective December 12, 2025