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 fulfilling its oversight responsibilities with respect to the Company's systems (*i.e.*, processes, policies, controls and procedures) to (i) identify, assess and mitigate risks related to cybersecurity and information technology, (ii) 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, (iii) respond to and manage cybersecurity threats, including data breach incidents and (iv) 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 and chairpersons of the Committee are appointed by the Board based upon 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 upon the recommendations of the Governance and Policy Committee.

Meetings

A majority of the members of the Committee shall constitute a quorum for any meeting. Members of the Board who are not members of the Committee may attend meetings of the Committee, but may not vote. 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 shall:

1. Review with management on a periodic basis the Company's enterprise cybersecurity strategy and framework, including the Company's assessment of cybersecurity threats and risk, data security programs (including data management systems and controls over Company data and systems to protect customer and other third-party data, including confidential information in the Company's possession or custody) and the Company's management and mitigation of cybersecurity and information technology risks and potential breach incidents.

2. Review with management any significant cybersecurity incident (as defined in the Company's Cybersecurity Incident Response Plan) that has occurred, reports to or from regulators with respect thereto and steps that have been taken to mitigate against reoccurrence.

3. Evaluate the effectiveness of the Company's cyber risk management and data security programs measured against the Company's cybersecurity threat landscape, including the following program components: cybersecurity risk monitoring, effectiveness testing, integrity of information security systems and controls, implementations of new cyber technology programs, adequacy of resources and security awareness training.

4. Review and discuss with management the laws and regulations, as well as significant legislative and regulatory developments, that could materially impact the Company's cybersecurity risk exposure. Evaluate the integrity of the Company's information technology systems, processes, policies and controls to oversee compliance.

5. Assess the effectiveness of the Company's data breach incident response plan, including detection, disclosure, investigation, remediation and post breach security measures.

6. Review with management on a periodic basis and assess the Company's information technology disaster recovery capabilities.

7. Review and assess the Company's cybersecurity risk systems against industry benchmarks and best practices, and make recommendations on enhancements. Receive reports from management on cybersecurity and data management assessments, surveys, audits and examinations that management shall direct third-party experts to conduct on a periodic basis.

8. Receive on a periodic basis reports on the metrics used to measure, monitor and manage cyber risks posed to the Company, including those related to potential cyber incidents.

9. Review the Company's information security planning and resources to manage changes in the Company's cybersecurity threat landscape. Assess the potential impact of cyber security risk on the Company's business, operations and reputation.

10. Review with management the Company's assessment of cybersecurity threats and risk associated with the Company's supply chain and actions the Company is taking to address such threats and risks.

11. Review at least annually the appropriateness and adequacy of the Company's cyber insurance coverage.

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

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

14. Conduct an annual performance evaluation of the Committee, including the Committee's compliance with this Charter.

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

Effective: December 13, 2019.