NORTHROP GRUMMAN SYSTEMS CORPORATION

ADDENDUM TO USE WITH TERMS FOR FIRM FIXED-PRICE SUBCONTRACTS IN SUPPORT OF THE NEXT GEN OPIR POLAR PROGRAM

Prime Contract FA8810-18-C-0006

All of the additional terms and conditions set forth below are incorporated in and made part of this Order. Any conflict between any of the conditions contained in this addendum and those appearing on Northrop Grumman Purchase Order Terms and Conditions shall be resolved in favor of the conditions in the addendum.

I. ADDITIONS

A. H001 CONTRACTOR CYBERSECURITY REQUIREMENTS (MAY 2019)

(a) Purpose. The purpose of this clause is to:

(1) Require the Contractor and all of its subcontractors to implement cybersecurity hygiene practices throughout their respective supply chains; and

(2) the Government provide visibility into the effectiveness of those provided practices in protecting the unauthorized exfiltration and use of Controlled Technical Information (CTI) residing within a covered contractor or subcontractor's information system.

(b) Definitions. As used in this clause-

"Adversary Emulation Testing" means testing of a network or information system using threat representative cyber exploitation techniques to identify security vulnerabilities and the effectiveness of defensive capabilities. Adversary emulation testing evaluates the ability of the system, tiered defenses, and defenders to protect critical functions; to detect and respond to cyber attack; and to survive and recover from cyber attack. Testing also examines relevant insider and outsider threat postures.

"Controlled Technical Information" (CTI) as defined in DFARS 252.204-7012.

"Covered Contractor Information System" as defined in DFARS 252.204-7012.

"Covered Contractor Location" means a Contractor facility that is owned or operated by or for the Contractor where Controlled Technical Information relevant to this Contract on a Covered Contractor Information System is processed, stored, or transmitted.

"Data Loss Detection" (DLD) are techniques that provide an ability to the Contractor to forensically locate and positively identify program information if it is stolen.

"Illicit Activity Alerts" (IAA) are ways to configure computer systems to provide indication and warning to the Contactor's network owners in advance of attempted data theft to assist in stopping the threat prior to losing key information.

"Routine" means no more often than one annual occurrence of the activity described, not including follow-on occurrences to assess any required remediations. Follow-on occurrence may occur more than once annually.

"Trusted Agent" means a Contractor employee with system, technical, managerial, or other knowledge relevant to the security and design of a network or information system who assists an assessor to perform testing on the network or information system.

(c) CTI Identification. Within 60 calendar days after Contract award, the Contractor shall identify the technologies being developed or used on this Contract that would result in the creation or use of CTI. Additionally, the Contractor shall identify the types of documents (e.g., PowerPoint, CAD drawings, excel) within which the technologies are memorialized physically, electronically, graphically, photographically, or in writing. (CDRL B078 Information Management Control Plan (IMCP), Part A & CDRL B079 Information Management Control Plan (IMCP) Part B). In accordance with DFARS 252.204-7012(a), the Government will mark or otherwise identify any covered defense information (as that term is defined in that clause) it will provide to the Contractor in support of the performance of this Contract.

(d) Information Management Control Plan (IMCP).

(1) IMCP Part A. The Contractor shall develop and provide an IMCP Part A. The Contractor shall deliver the IMCP Part A to the Government POC identified in subsection (l), Contact Information, and each of its subcontractors shall deliver the IMCP Part A only to the next higher tier subcontractor (or if the subcontractor is a first-tier subcontractor, only to the Contractor). (CDRL B078 Information Management Control Plan (IMCP), Part A).

(2) IMCP Part B, Supplier Compliance Supplement. If the Contractor has subcontractors that receive or generate CTI in performance of this Contract, the Contractor shall ensure those subcontractors submit an IMCP Part B, Supplier Compliance Supplement, directly to the Government POC identified in subsection (l), Contact Information, within 60 calendar days after award of the subcontract (CDRL B079).

(3) The Government reserves the right to review and inspect the IMCPs to verify implementation of the IMCP and DFARS 252.204-7012. Further, the Government reserves the right to use the IMCPs to iteratively navigate

through the tiered supply chain to accomplish the activities as enumerated in this clause. The Contractor will only have visibility to their next lower-tier subcontractor IMCP(s) Part A.

(e) Compliance Auditing. The Contractor shall assist the Government during routine onsite compliance audits conducted by Defense Contracting Management Agency (DCMA) or by a third-party firm that satisfies the definition of a Covered Government Support Contractor in DFARS 252.227-7013(a)(5) and DFARS 252.227-7014(a)(6)) at Government-selected Covered Contractor Locations to ensure compliance with DFARS 252.204-7012 and the Contractor's System Security Plan (including all relevant Plan of Actions and Milestones (POAMs)). Prior to any such audit, the Government and the Contractor will work jointly to avoid or mitigate any conflicts of interest or potential conflicts of interest as set forth in FAR Part 9.5. The Government will provide written notification at least 30 calendar days prior to performing a routine audit.

(f) Adversary Emulation Testing.

(1) The Contractor, at its sole discretion and option, shall choose one of the three options below:

(i) Conduct at a regular interval, based on the Contractor's risk-based determination, adversary emulation testing on Covered Contractor Information Systems, or a subset thereof, as mutually agreed to between the Contracting Officer and Contractor. The Contractor shall provide the Contracting Officer or Government Point of Contact (POC) identified in subsection (l) 30 calendar day notice of planned adversary emulation testing. The Contractor shall provide the opportunity for the Government or a third party firm that satisfies the definition of a Covered Government Support Contractor in DFARS 252.227-7013(a)(5) and DFARS 252.227- 7014(a)(6)) to observe the testing, review the results, and verify the level of testing meets the criteria outlined in CDRL B080, Adversary Emulation Testing, derived from the National Institute of Standards and Technology Special Publication (NIST SP) 800-115, Section 5.2 Penetration Testing. The Contractor shall use the MITRE ATT&CK Framework and the current Open Web Application Security Project (OWASP) Top Ten vulnerabilities as published at the time of Contract award when planning its Adversary Emulation Testing, which will be verified in CDRL B080. Prior to any such testing, the Government and the Contractor will work jointly to avoid or mitigate any conflicts of interest or potential conflicts of interest as set forth in FAR Part 9.5.

(A) The Contractor shall deliver the Adversary Emulation Testing process documentation outlined in CDRL B080, Adversary Emulation Testing, to the Government, and each of its subcontractors shall, deliver CDRL B080 to the Government POC identified in subsection (l), Contact Information.

Or,

(ii) Permit the Government to, and assist the Government in, performing routine Adversary Emulation Testing conducted by a third-party firm that satisfies the definition of a Covered Government Support Contractor in DFARS 252.227-7013(a)(5) and DFARS 252.227-7014(a)(6)) on Government-selected Covered Contractor Information Systems. Prior to any such testing, the Government and the Contractor will work jointly to avoid or mitigate any conflicts of interest or potential conflicts of interest as set forth in FAR Part 9.5. Prior to conducting the Adversary Emulation Testing, the Government-selected assessor shall initiate a Collaborative Onsite Security Assessment (COSA). The Contractor shall mutually agree to a COSA with the Government. The COSA agreement shall address:

(A) Any Adversary Emulation Testing in-process or those already conducted on the selected Covered Contractor Information Systems;

(B) Rules of engagement;

(C) Roles and responsibilities of the parties;

(D) Pre-assessment activities;

(E) Scope of the assessment;

(F) Assessment methodology;

(G) Assessment tools used;

(H) Frequency of assessment;

(I) Confidentiality and handling of data;

(J) Schedule;

(K) Cost Implications; and

(L) Post assessment obligations of the parties.

For the routine Adversary Emulation Testing, the Contractor shall provide at least one trusted agent. The Government assessor will coordinate activities and results relating to routine Adversary Emulation Testing with the trusted agent(s).

Or,

(iii) Subcontract with a third party, approved by the Government (approval shall not be unreasonably withheld), that is capable of Adversary Emulation Testing and verify this third party is capable of Adversary Emulation Testing by delivering directly to the Government POC identified in subsection (l), Contact Information, the Adversary Emulation Testing Process (CDRL B080). If the Contractor elects to subcontract with a third party to perform Adversary Emulation Testing, they shall provide the Contracting Officer or Government Point of Contact (POC) identified in subsection (l) 30 calendar day notice of planned adversary emulation testing. The Contractor shall provide the opportunity for the Government or a third party firm that satisfies the definition of a Covered Government Support Contractor in DFARS 252.227-7013(a)(5) and DFARS 252.227-7014(a)(6)) to observe the testing, review the results, and verify the level of testing meets the criteria outlined in CDRL B080, Adversary Emulation Testing, derived from the National Institute of Standards and Technology Special Publication (NIST SP) 800-115, Section 5.2 Penetration Testing. Prior to any such testing, the Government and the Contractor will work jointly to avoid or mitigate any conflicts of interest or potential conflicts of interest as set forth in FAR Part 9.5.

(2) The Contractor shall, at its sole discretion with the exception of high level criticality findings, disposition

security-related findings from adversary emulation testing on a risk-based determination. If the Contractor determines disposition is required, the Contractor shall determine the manner of disposition. The Contractor shall mitigate high level criticality findings or work with the Government Point of Contact (POC) identified in subsection (l) to come to an agreement for a mitigation approach.

(g) Perimeter Threat Detection Augmentation.

(1) The Contractor, at its sole discretion and option, shall choose one of the three options below:

(i) Verify they are capable of Perimeter Threat Detection by delivering directly to the Government the Perimeter Threat Detection Process (CDRL B081). If the Contractor elects to do the above, they shall assist the Government in auditing against the above documentation in conjunction with the activities described in subsection (e). The Contractor shall deliver CDRL B081 to the Government POC identified in subsection (l), Contact Information, and each of its subcontractors shall deliver the CDRL B081 to the Government POC identified in subsection (l) Contact Information.

Or,

(ii) Provide the information requested in Perimeter Threat Detection Process Part B (CDRL B086) for the Government to provide threat detection augmentation on the forward facing IP space & domains of networks. CDRL B086 shall be delivered to the Government, and each of Contractor's subcontractors shall deliver CDRL B086 to the Government.

Or,

(iii) Subcontract with a third party, approved by the Government (approval shall not be unreasonably withheld), that is capable of Perimeter Threat Detection and verify this third party is capable of Perimeter Threat Detection by delivering directly to the Government POC identified in subsection (l), Contact Information, the Perimeter Threat Detection Process (CDRL B081). CDRL B081 shall be delivered to the Government, and each of Contractor's subcontractors shall deliver CDRL B081 to the Government. If the Contractor elects to subcontract with a third party to perform Perimeter Threat Detection, they shall assist the Government in auditing against the documentation in conjunction with the activities described in subsection (e).

(h) Illicit Data Loss Exploitation (IDLE).

(1) Upon written direction from the Contracting Officer, the Contractor shall follow the process identified in the IDLE Procedures.

(2) Upon receipt of the above written direction, and at any time thereafter during the period of performance of this contract, the Contracting Officer may direct the Contractor to perform IDLE efforts via CLIN 3000, IDLE Efforts.

(3) IDLE Upon receipt, the Contractor shall submit to the Government an estimate which shall include, at a minimum, a description of the effort, the number of hours required for completion broken out by skill mix, the total estimated cost, Government Fiscal Year (GFY) and Contractor Accounting Year (CY), and a period of performance.

(ii) Each effort performed in accordance with this clause shall be directed by the Contracting Officer via unilateral modification to the contract. IDLE efforts shall be incorporated into Attachment 15, "NEXT GEN OPIR POLAR - PHASE 1 ILLICIT DATA LOSS EXPLOITATION (IDLE) (Reserved)." Such modification shall:

(A) Provide specific direction as to effort to be accomplished;

(B) Establish a period of performance for the effort;

(C) Establish the maximum number of hours; and

(D) Establish the estimated cost.

(iii) In no event shall the Contractor exceed the established hours, total estimated cost, or period of performance authorized in each individual modification without written approval from the Contracting Officer.

(iv) The Contractor shall segregate all costs associated with CLIN 3000, IDLE Efforts, from the costs associated with all other CLINs. The Contractor shall segregate the costs for each IDLE effort from the costs of every other IDLE effort.

(v) The table below states the total hours available, the total hours used, and the composite hourly rate for each GFY.

(vi) In accordance with FAR 16.306, the IDLE scope will be performed on a level of effort basis within the time periods specified and is a CPFF term form. The below stated hours designate the available hours Contractor may expend on a level of effort basis as unilaterally required by the Government for the time period specified.

(i) RESERVED.

(j) Subcontractors. The Contractor shall include this H001 clause, including this subsection (j), in all subcontracts, or similar contractual instruments, for which the subcontractor has Covered Contractor Locations, without alteration except to identify the parties and to properly flow the requirements in the CDRLs B078-B086 to subcontractors, except as provided in subsection (k), Waiver.

(k) Waiver. The Contractor may submit in writing to the Contracting Officer a request to waive, in part, the requirements of subsections (e) through (h) of this clause accompanied by a detailed rationale for the request.

(1) The Contractor, and if necessary any lower tier subs in the requisite chain, shall flow this H001 clause in its entirety to the following subcontractors:

1. Northrop Grumman Systems Corporation
2. Ball Aerospace
3. Raytheon

For all other subcontractors, the Government hereby waives the requirement to flow down subsections (e) through (h) of this H001 clause. This waiver list will be reviewed annually by the Contractor and Government PCO. The Contractor shall submit a list of new 1st tier subcontractors 30 calendar days prior to the annual

review. At its discretion, the Government may unilaterally direct the flow of the entirety of this clause to any specific subcontractor subject to equitable relief within the requisite chain.

(l) Contact Information. For questions on this clause or to notify the Government as directed by the subsections above, contact directly the following organization inbox: SMC.RS.OPIR@us.af.mil.

(m) Nondisclosure agreements (NDA). If the Government-selected third-party firm is a Covered Government Support contractor, that firm will sign a nondisclosure agreement with the Contractor prior to starting work under this H001 clause. Any such Government-selected third-party firm shall not be a competitor of the Contractor and shall not create a conflict of interest as set forth in FAR Part 9.5. The Government and the Contractor will work jointly to avoid or mitigate any conflicts of interest or potential conflicts of interest that arise. The nondisclosure agreement will describe the conditions under which the Contractor will agree to furnish the Covered Government Support Contractor access and proprietary data prior to, during, or subsequent to the Covered Government Support Contractor conducting routine onsite compliance audits (per (e)) or routine Adversary Emulation Testing (per (f)(1)(i) or (f)(1)(ii)). No NDA shall prohibit the Government-selected third-party firm from disclosing relevant information to the Government.

(n) RESERVED.

(o) Other compliances. The Contractor shall not be required to perform any requirement of this clause that violates applicable U.S. federal, state, or non-U.S. laws or regulations unless an exception to those laws or regulations applies due to the use of log-on consent banners.

(p) Duration. The rights and obligations of the parties under this clause shall end upon the period of performance defined in the prime contract.

(q) CDRLs. All CDRLs delivered under this H001 clause do not contain technical data, computer software, or computer software documentation and are data incidental to contract administration, such as management information. All CDRLs will be marked as Contractor's proprietary or confidential information.

(End of Clause)

B. 252.219-7003 SMALL BUSINESS SUBCONTRACTING PLAN (DOD CONTRACTS) (DEVIATION 2018-00007) (DEC 2017)

This clause supplements the Federal Acquisition Regulation 52.219-9, Small Business Subcontracting Plan, clause of this contract.

(a) Definitions. "Summary Subcontract Report (SSR) Coordinator," as used in this clause, means the individual who is registered in the Electronic Subcontracting Reporting System (eSRS) at the Department of Defense (9700) and is responsible for acknowledging receipt or rejecting SSRs in eSRS for the Department of Defense.

(b) Subcontracts awarded to workshops approved by the Committee for Purchase from People Who are Blind or Severely Disabled (41 U.S.C. 8502-8504), may be counted toward the Contractor's small business subcontracting goal.

(c) A mentor firm, under the Pilot Mentor-Protege Program established under section 831 of Public Law 101-510, as amended, may count toward its small disadvantaged business goal, subcontracts awarded to-

(1) Protege firms which are qualified organizations employing the severely disabled; and

(2) Former protege firms that meet the criteria in section 831 (g)(4) of Public Law 101-510.

(d) The master plan is approved by the Contractor's cognizant contract administration activity.

(e) In those subcontracting plans which specifically identify small businesses, the Contractor shall notify the Administrative Contracting Officer of any substitutions of firms that are not small business firms, for the small business firms specifically identified in the subcontracting plan. Notifications shall be in writing and shall occur within a reasonable period of time after award of the subcontract. Contractor-specified formats shall be acceptable.

(f)(1) For DoD, the Contractor shall submit reports in eSRS as follows:

(i) The Individual Subcontract Report (ISR) shall be submitted to the contracting officer at the procuring contracting office, even when contract administration has been delegated to the Defense Contract Management Agency.

(ii) Submit the consolidated SSR for an individual subcontracting plan in eSRS by selecting "Department of Defense (DoD) (9700)" from the top of the second dropdown menu. The contractor shall not select anything lower.

(2) For DoD, the authority to acknowledge receipt or reject reports in eSRS is as follows:

(i) The authority to acknowledge receipt or reject the ISR resides with the contracting officer who receives it, as described in paragraph (f)(1)(i) of this clause.

(ii) The authority to acknowledge receipt or reject SSRs resides with the SSR Coordinator.

C. 252.234-7002 EARNED VALUE MANAGEMENT SYSTEM (DEVIATION 2015-00017) (SEP 2015)

(a) Definitions. As used in this clause--

"Acceptable earned value management system" means an earned value management system that generally complies with system criteria in paragraph (b) of this clause.

"Earned value management system" means an earned value management system that complies with the eamed value management system guidelines in the ANSI/EIA-748.

"Significant deficiency" means a shortcoming in the system that materially affects the ability of officials of the Department of Defense to rely upon information produced by the system that is needed for management purposes.

(b) System criteria. In the performance of th is contract, the Contractor shall use-

(1) An Earned Value Management System (EVMS) that complies with the EVMS guidelines in the American

National Standards Institute/Electronic Industries Alliance Standard 748, Earned Value Management Systems (ANSI/EIA-748); and

(2) Management procedures that provide for generation of timely, reliable, and verifiable information for the Contract Performance Report (CPR) and the Integrated Master Schedule (IMS) required by the CPR and IMS data items of this contract.

(c) If this contract has a value of $100 million or more, the Contractor shall use an EVMS that has been determined to be acceptable by the Cognizant Federal Agency (CFA). If, at the time of award, the Contractor's EVMS has not been determined by the CFA to be in compliance with the EVMS guidelines as stated in paragraph (b)(1) of this clause, the Contractor shall apply its current system to the contract and shall take necessary actions to meet the milestones in the Contractor's EVMS plan.

(d) If this contract has a value of less than $100 million, the Government will not make a formal determination that the Contractor's EVMS complies with the EVMS guidelines in ANSI/EIA-748 with respect to the contract. The use of the Contractor's EVMS for this contract does not imply a Government determination of the Contractor's compliance with the EVMS guidelines in ANSI/EIA-7 48 for application to future contracts. The Government will allow the use of a Contractor's EVMS that has been formally reviewed and determined by the CFA to be in compliance with the EVMS guidelines in ANSI/EIA-748.

(e) The Contractor shall submit notification of any proposed substantive changes to the EVMS procedures and the impact of those changes to the CFA. If this contract has a value of $100 million or more, unless a waiver is granted by the CFA, any EVMS changes proposed by the Contractor require approval of the CFA prior to implementation. The CFA will advise the Contractor of the acceptability of such changes as soon as practicable (generally within 30 calendar days) after receipt of the Contractor's notice of proposed changes. If the CFA waives the advance approval requirements, the Contractor shall disclose EVMS changes to the CFA at least 14 calendar days prior to the effective date of implementation.

(f) The Government will schedule integrated baseline reviews as early as practicable, and the review process will be conducted not later than 180 calendar days after-

(1) Contract award;

(2) The exercise of significant contract options; and

(3) The incorporation of major modifications.

During such reviews, the Government and the Contractor will jointly assess the Contractor's baseline to be used for performance measurement to ensure complete coverage of the statement of work, logical scheduling of the work activities, adequate resourcing, and identification of inherent risks.

(g) The Contractor shall provide access to all pertinent records and data requested by the Contracting Officer or duly authorized representative as necessary to permit Government surveillance to ensure that the EVMS complies, and continues to comply, with the performance criteria referenced in paragraph (b) of this clause.

(h) When indicated by contract performance, the Contractor shall submit a request for approval to initiate an over-target baseline or over-target schedule to the Contracting Officer. The request shall include a top-level projection of cost and/or schedule growth, a determination of whether or not performance variances will be retained, and a schedule of implementation for the rebaselining. The Government will acknowledge receipt of the request in a timely manner (generally within 30 calendar days).

(i) Significant deficiencies.

(1) The Contracting Officer will provide an initial determination to the Contractor, in writing, of any significant deficiencies. The initial determination will describe the deficiency in sufficient detail to allow the Contractor to understand the deficiency.

(2) The Contractor shall respond within 30 days to a written initial determination from the Contracting Officer that identifies significant deficiencies in the Contractor's EVMS. If the Contractor disagrees with the initial determination, the Contractor shall state, in writing, its rationale for disagreeing.

(3) The Contracting Officer will evaluate the Contractor's response and notify the Contractor, in writing, of the Contracting Officer's final determination concerning-

(i) Remaining significant deficiencies;

(ii) The adequacy of any proposed or completed corrective action;

(iii) System noncompliance, when the Contractor's existing EVMS fails to comply with the earned value management system guidelines in the ANSI/EIA-748; and

(iv) System disapproval, if initial EVMS validation is not successfully completed within the timeframe approved by the Contracting Officer, or if the Contracting Officer determines that the Contractor's earned value management system contains one or more significant deficiencies in high-risk guidelines in ANSI/EIA-748 standards (guidelines 1, 3, 6, 7, 8, 9, 10, 12, 16, 21, 23, 26, 27, 28, 30, or 32). When the Contracting Officer determines that the existing earned value management system contains one or more significant deficiencies in one or more of the remaining 16 guidelines in ANSI/EIA-748 standards, the Contracting Officer will use discretion to disapprove the system based on input received from functional specialists and the auditor.

(4) If the Contractor receives the Contracting Officer's final determination of significant deficiencies, the Contractor shall, within 45 days of receipt of the final determination, either correct the significant deficiencies or submit an acceptable corrective action plan showing milestones and actions to eliminate the significant deficiencies.

(j) Withholding payments. If the Contracting Officer makes a final determination to disapprove the Contractor's EVMS, and the contract includes the clause at 252.242-7005 http://www.acq.osd.mil/dpap/dars/dfars/html/current/252242.htm, Contractor Business Systems, the Contracting Officer will withhold payments in accordance with that clause.

(k) With the exception of paragraphs (i) and O) of this clause, the Contractor shall require its subcontractors to

comply with EVMS requirements as follows:
(1) For subcontracts valued at $100 million or more, the following subcontractors shall comply with the requirements of this clause: Selected Mission Payload Vendors (2) For subcontracts valued at less than $100 million, the following subcontractors shall comply with the requirements of this clause, excluding the requirements of paragraph (c) of this clause: Selected Mission Payload Vendors.

REVISIONS

A. The following changes are made to clause 199 entitled, "FAR Provisions/Clauses":

1. Add the following FAR clauses:

252.225-7047	EXPORTS BY APPROVED COMMUNITY MEMBERS IN PERFORMANCE OF THE CONTRACT
252.234-7004	COST AND SOFTWARE DATA REPORTING SYSTEM - BASIC