SEC. ___. EXPANSION OF AUTHORITY FOR ACCESS AND INFORMATION RELATING TO CYBERATTACKS ON OPERATIONALLY CRITICAL CONTRACTORS OF THE ARMED FORCES.

Section 391(c) of title 10, United States Code, is amended—

(1) in paragraph (3)—

(A) by striking "(3)" and all that follows through subparagraph (A) and inserting the following:

"(3) ARMED FORCES ASSISTANCE AND ACCESS TO EQUIPMENT AND INFORMATION BY MEMBERS OF THE ARMED FORCES.—The procedures established pursuant to subsection (a) shall—

"(A) include mechanisms for a member of the armed forces—

"(i) if requested by an operationally critical contractor, to assist the contractor in detecting and mitigating penetrations; or

"(ii) at the request of the Department or the Coast Guard, to obtain access to equipment or information of an operationally critical contractor necessary to conduct a forensic analysis, in addition to any analysis conducted by the contractor; and"; and

(B) in subparagraph (B)—

(i) by striking "to determine whether information" and inserting the following: "to determine whether—

"(i) information";

(ii) in clause (i), as so designated—

(I) by striking "the Department in connection with any Department program" and inserting "the armed forces in connection with any program of the armed forces";

(II) by inserting "or compromised on" after "exfiltrated from"; and

(III) by striking the period at the end and inserting "or compromised; or"; and

(iii) by adding at the end the following new clause:

"(ii) the ability of the contractor to provide operationally critical support has been affected and, if so, how and to what extent it has been affected."; and

(2) in paragraph (4), by inserting ", so as to minimize delays in or any curtailing of the Department's or Coast Guard's cyber response and defensive actions" after "specific person"; and

(3) in paragraph (5)(C), by inserting " or counterintelligence activities" after "investigations".

[Please note: The "Changes to Existing Law" section below sets out in red-line format how the legislative text would amend existing law.]

Section-by-Section Analysis

This proposal would amend section 391 of title 10, United States Code, by extending the ability of the Department of Defense (DoD) and the Coast Guard to react immediately to reports of intrusions that may affect critical data of the Armed Forces.

A number of the commercial transportation service providers of DoD and the Coast Guard are operationally critical contractors as defined in section 391 of title 10, United States Code. They are key conduits of logistics-related data, including the personally identifiable information relating to the transportation of members of the Armed Forces and their belongings. Due to this interconnected relationship, the security of defense contractor networks and

information systems has been highlighted as a key risk in the mission assurance analysis of support to a contingency operation or in times of crisis. Although the data relating to the Armed Forces that resides in these systems is usually unclassified, its security and integrity is absolutely critical to the effective management of the worldwide logistics enterprise, especially during wartime or a contingency. The purpose of this legislative proposal is to facilitate the same level of proactive support by the Armed Forces in responding to a cyber incident as that authorized for cleared defense contractors. Specifically, this proposal would require DoD and the Coast Guard to contract in such a way that operationally critical contractors would provide through contract, at DoD or Coast Guard request, access to contractor systems and information to the extent necessary to determine the impact of the incident on the Armed Forces. At present, the operationally critical contractor may request forensic support from DoD in the event of a cyber incident, but the implementing contract clauses do require the operationally critical contractor to accept such support if offered.

The enhanced level of access by the Armed Forces sought in this proposal may be required by contract and would thus appear to make additional legislation unnecessary. However, the liability protections provided to an operationally critical contractor under section 391 only extend to the activities currently addressed in that section. While a contractor may agree by contract to provide greater access to the Armed Forces than the law requires, it does so at its own risk. Not only does this increase the contractor's potential liability exposure, but it may also serve as a deterrent to doing business with DoD or the Coast Guard in the first place. Since the Armed Forces need greater access than the law currently requires, it is imperative that this greater level of access be incorporated into section 391--rather than just required by contract--in order to accord the contractor liability protections commensurate with the level of access it is required to provide.

This proposal would facilitate proactive support by the Armed Forces to operationally critical contractors to allow for immediate forensic analysis and the protection of crucial information of the Armed Forces. In addition, it would expand the liability protections currently available to such contractors under the law to cover the level of access being sought by the Armed Forces with this proposal.

Budget Implications: This proposal has no significant budgetary impact. Resources impacted are incidental in nature and amount and are included within the Fiscal Year (FY) 2021 President's Budget request.

Changes to Existing Law: This proposal would make the following changes to section 391 of title 10, United States Code:

§391. Reporting on cyber incidents with respect to networks and information systems of operationally critical contractors and certain other contractors

(a) DESIGNATION OF DEPARTMENT COMPONENT TO RECEIVE REPORTS.—The Secretary of Defense shall designate a component of the Department of Defense to receive reports of cyber incidents from contractors in accordance with this section and section 393 of this title or from other governmental entities.

(b) PROCEDURES FOR REPORTING CYBER INCIDENTS.—The Secretary of Defense shall establish procedures that require an operationally critical contractor to report in a timely manner to component designated under subsection (a) each time a cyber incident occurs with respect to a network or information system of such operationally critical contractor.

(c) PROCEDURE REQUIREMENTS.—

(1) DESIGNATION AND NOTIFICATION.—The procedures established pursuant to subsection (a) shall include a process for—

(A) designating operationally critical contractors; and

(B) notifying a contractor that it has been designated as an operationally critical contractor.

(2) RAPID REPORTING.—The procedures established pursuant to subsection (a) shall require each operationally critical contractor to rapidly report to the component of the Department designated pursuant to subsection (d)(2)(A) on each cyber incident with respect to any network or information systems of such contractor. Each such report shall include the following:

(A) An assessment by the contractor of the effect of the cyber incident on the ability of the contractor to meet the contractual requirements of the Department.

(B) The technique or method used in such cyber incident.

(C) A sample of any malicious software, if discovered and isolated by the contractor, involved in such cyber incident.

(D) A summary of information compromised by such cyber incident.

(3) ~~DEPARTMENT~~ ARMED FORCES ASSISTANCE AND ACCESS TO EQUIPMENT AND INFORMATION BY ~~DEPARTMENT PERSONNEL~~ MEMBERS OF THE ARMED FORCES.—The procedures established pursuant to subsection (a) shall—

~~(A) include mechanisms for Department personnel to, if requested, assist operationally critical contractors in detecting and mitigating penetrations; and~~

(A) include mechanisms for a member of the armed forces—

(i) if requested by an operationally critical contractor, to assist the contractor in detecting and mitigating penetrations; or

(ii) at the request of the Department or the Coast Guard, to obtain access to equipment or information of an operationally critical contractor necessary to conduct a forensic analysis, in addition to any analysis conducted by the contractor; and

(B) provide that an operationally critical contractor is only required to provide access to equipment or information as described in subparagraph (A) ~~to determine whether information~~ to determine whether—

(i) information created by or for the ~~Department~~ armed forces in connection with any ~~Department~~ program of the armed forces was successfully exfiltrated from or compromised on a network or information system of such contractor and, if so, what information was exfiltrated~~.~~ or compromised; or

(ii) the ability of the contractor to provide operationally critical support has been affected and, if so, how and to what extent it has been affected.

(4) PROTECTION OF TRADE SECRETS AND OTHER INFORMATION.—The procedures established pursuant to subsection (a) shall provide for the reasonable protection of trade secrets, commercial or financial information, and information that can be used to identify a specific person, so as to minimize delays in or any curtailing of the Department's or Coast Guard's cyber response and defensive actions.

(5) DISSEMINATION OF INFORMATION.—The procedures established pursuant to subsection (a) shall limit the dissemination of information obtained or derived through the procedures to entities—

(A) with missions that may be affected by such information;

(B) that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;

(C) that conduct counterintelligence or law enforcement investigations or counterintelligence activities; or

(D) for national security purposes, including cyber situational awareness and defense purposes.

(d) PROTECTION FROM LIABILITY OF OPERATIONALLY CRITICAL CONTRACTORS.—

(1) No cause of action shall lie or be maintained in any court against any operationally critical contractor, and such action shall be promptly dismissed, for compliance with this section that is conducted in accordance with procedures established pursuant to subsection (b).

(2)(A) Nothing in this section shall be construed—

(i) to require dismissal of a cause of action against an operationally critical contractor that has engaged in willful misconduct in the course of complying with the procedures established pursuant to subsection (b); or

(ii) to undermine or limit the availability of otherwise applicable common law or statutory defenses.

(B) In any action claiming that paragraph (1) does not apply due to willful misconduct described in subparagraph (A), the plaintiff shall have the burden of proving by clear and convincing evidence the willful misconduct by each operationally critical contractor subject to such claim and that such willful misconduct proximately caused injury to the plaintiff.

(C) In this subsection, the term "willful misconduct" means an act or omission that is taken—

(i) intentionally to achieve a wrongful purpose;

(ii) knowingly without legal or factual justification; and

(iii) in disregard of a known or obvious risk that is so great as to make it highly probable that the harm will outweigh the benefit.

(e) DEFINITIONS.—In this section:

(1) CYBER INCIDENT.—The term "cyber incident" means actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system or the information residing therein.

(2) OPERATIONALLY CRITICAL CONTRACTOR.—The term "operationally critical contractor" means a contractor designated by the Secretary for purposes of this section as a critical source of supply for airlift, sealift, intermodal transportation services, or logistical

support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.