SEC. ___. NONDISCLOSURE OF CERTAIN SENSITIVE MILITARY INFORMATION.

(a) SECTION HEADING.—The heading of section 130e of title 10, United States Code, is amended to read as follows:

"§130e. Nondisclosure of certain sensitive military information".

(b) EXEMPTION.—Section 130e(a) of title 10, Unites States Code, is amended—

(1) in the matter preceding paragraph (1)—

(A) by striking "critical infrastructure security"; and

(B) by striking "pursuant to section 552(b)(3) of title 5,"; and

(2) by amending paragraph (1) to read as follows:

"(1) the information is—

"(A) Department of Defense critical infrastructure security information;

"(B) covered information pertaining to military tactics, techniques, or procedures; or

"(C) covered information pertaining to rules of engagement or rules for the use of force; and".

(c) DESIGNATION OF DEPARTMENT OF INFORMATION.—Section 130e(b) of such title is amended—

(1) in the subsection heading, by striking "CRITICAL INFRASTRUCTURE SECURITY"; and

(2) in the first sentence, by striking "may designate information as being Department of Defense critical infrastructure security information" and inserting "may designate information as being information identified in subsection (a)(1)".

(d) INFORMATION PROVIDED TO STATE AND LOCAL GOVERNMENTS.—Section 130e(c) of such title is amended—

(1) in paragraphs (1) and (2)(A), by striking "critical infrastructure security"; and

(2) in paragraph (2)(B), by striking "Department of Defense critical infrastructure security information" and inserting "information exempt from disclosure".

(e) DELEGATION AND TRANSPARENCY.—Section 130e of such title is further amended—

(1) by striking subsection (d);

(2) by redesignating subsection (e) as subsection (d); and

(3) in subsection (d), as so redesignated—

(A) by striking ", or the Secretary's designee,"; and

(B) by striking "through the Office of the Director of Administration and Management" and inserting "in accordance with guidelines prescribed by the Secretary".

(f) CITATION FOR PURPOSES OF OPEN FOIA ACT OF 2009.—Section 130e of such title is further amended by inserting after subsection (d), as redesignated by subsection (e)(2) of this section, the following new subsection:

"(e) CITATION FOR PURPOSES OF OPEN FOIA ACT OF 2009.—This section shall be treated as a statute that specifically exempts certain matters from disclosure under section 552 of title 5, as described in subsection (b)(3) of that section.".

(g) DEFINITIONS.—Subsection (f) of such section is amended to read as follows:

"(f) DEFINITIONS.—In this section:

"(1) ADVERSARY.—The term 'adversary' means a party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged.

"(2) COVERED INFORMATION PERTAINING TO MILITARY TACTICS, TECHNIQUES, OR PROCEDURES.—The term 'covered information pertaining to military tactics, techniques, or procedures' means information pertaining to military tactics, techniques, or procedures that identifies a method for using equipment or personnel to accomplish a specific mission under a particular set of operational or exercise conditions (including offensive, defensive, force protection, cyberspace, stability, civil support, freedom of navigation, operations security, counter intelligence, and intelligence collection operations) the public disclosure of which could reasonably be expected to provide a military advantage to an adversary.

"(3) COVERED INFORMATION PERTAINING TO RULES OF ENGAGEMENT OR RULES FOR THE USE OF FORCE.—The term 'covered information pertaining to rules of engagement or rules for the use of force' means information pertaining to rules of engagement or rules for the use of force the public disclosure of which could reasonably be expected to provide an operational military advantage to an adversary.

"(4) DEPARTMENT OF DEFENSE CRITICAL INFRASTRUCTURE SECURITY INFORMATION.—The term 'Department of Defense critical infrastructure security information' means sensitive but unclassified information that, if disclosed, would reveal capabilities or vulnerabilities in Department of Defense critical infrastructure that, if exploited, would likely result in the significant disruption, destruction, or damage of or to Department of Defense operations, property, or facilities, including—

"(A) information regarding the securing and safeguarding of explosives, hazardous chemicals, or pipelines, related to critical infrastructure or protected systems owned or operated by or on behalf of the Department of Defense;

"(B) vulnerability assessments prepared by or on behalf of the Department of Defense;

"(C) explosives safety information, including storage and handling; and

"(D) other site-specific information on or relating to installation security.

"(5) MILITARY TACTICS, TECHNIQUES, AND PROCEDURES.—The term 'military tactics, techniques, and procedures' means—

"(A) the employment and ordered arrangement of military forces in relation to each other;

"(B) a non-prescriptive way or method used to perform a mission, function, or task that is—

"(i) related to or incidental to combat missions or contingency operations; or

"(ii) directly related to preparing for, going to, or returning from combat missions or contingency operations; or

"(C) detailed steps that prescribe how to perform a specific task that is—

"(i) related to, or incidental to, a combat mission, force protection operation, or contingency operation; or

"(ii) directly related to preparing for, going to, or returning from combat missions, force protection operations, or contingency operations.

"(6) RULES FOR THE USE OF FORCE.—The term 'rules for the use of force' means directives issued to guide United States forces on the use of force during various operations.

"(7) RULES OF ENGAGEMENT.—The term 'rules of engagement' means directives issued by a competent military authority that delineate the circumstances and limitations under which the armed forces will initiate or continue combat engagement with other forces encountered.".

(i) CLERICAL AMENDMENT.—The item relating to section 130e in the table of sections at the beginning of chapter 3 of such title is amended to read as follows:

"130e. Nondisclosure of certain sensitive military information.".

[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 130e of title 10, United States Code (U.S.C.), to authorize the Department of Defense to withhold sensitive, but unclassified, military tactics, techniques, or procedures; rules for the use of force; and military rules of engagement, from release to the public under section 552 of title 5, U.S.C. (known as the Freedom of Information Act (FOIA)), if public disclosure could reasonably be expected to provide an operational military advantage to an adversary.

The decision of the Supreme Court in *Milner v. Department of the Navy*, 131 S. Ct. 1259 (2011), significantly narrowed the long-standing administrative understanding of the scope of Exemption 2 of the FOIA (5 U.S.C. 552(b)(2)). Before that decision, the Department was authorized to withhold sensitive information on critical infrastructure and military tactics, techniques, and procedures from release under FOIA pursuant to Exemption 2. Section 130e of title 10, U.S.C., was established in the National Defense Authorization Act for Fiscal Year 2012 to reinstate protection from disclosure of critical infrastructure security information. This proposal similarly would amend section 130e to add protections for military tactics, techniques, and procedures (TTPs); rules for the use of force; and rules of engagement that, if publicly disclosed, could reasonably be expected to provide an operational or tactical military advantage to an adversary such that the adversary could potentially use the information to circumvent or negatively impact military operations or actions in whole or in part. Military TTPs, rules for the use of force; and rules of engagement are analogous to law enforcement techniques and procedures, which Congress has afforded protection under FOIA Exemption 7(E).

The effectiveness of U.S. military operations is dependent upon adversaries, or potential adversaries, not obtaining advance knowledge of sensitive TTPs, rules for the use of force; or rules of engagement that will be employed in such tactical operations. If an adversary or potential adversary obtains knowledge of this sensitive information, the adversary would gain invaluable knowledge on how our forces operate in given tactical military situations. This knowledge could then, in turn, enable the adversary to counter the TTPs, rules for use of force, or rules of engagement by identifying and exploiting any weaknesses. From this, the defense of the homeland, success of the operation, and the lives of U.S. military forces would be seriously jeopardized. Furthermore, the probability of successful cyber operations would be limited with the public release of cyber-related TTPs. This proposal would add a layer of mission assurance to unclassified cyber operations and enhance the Department of Defense's ability to project cyber effects while protecting national security resources.

This proposal additionally would make minor amendments in section 130e to: (1) clarify the citation for the purposes of the OPEN FOIA Act of 2009; (2) remove references to reflect the merger of the Director of Administration and Management with the Deputy Chief Management Officer of the Department of Defense; and (3) remove the prohibition on further delegation.

It is important to note that the terms tactics, techniques, and procedures, as used in the context of this proposal, will not be applied in an overly broad manner to withhold from public disclosure information related to the handling of disciplinary matters, investigations, acquisitions, intelligence oversight, oversight of contractors, allegations of sexual harassment or sexual assault, allegations of prisoner and detainee maltreatment, installation management activities, etc. However, depending on the nature of the information, other provisions of law may require that such information not be released publicly in whole or in part.

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. Exemptions for the release of certain information under FOIA would generate minimal savings to the Administration by avoiding the preparation of select materials for release.

Changes to Existing Law: The proposal would make the following changes to section 130e of title 10, United States Code:

§130e. ~~Treatment under Freedom of Information Act of critical infrastructure security information~~ Nondisclosure of certain sensitive military information

(a) EXEMPTION.—The Secretary of Defense may exempt Department of Defense ~~critical infrastructure security~~ information from disclosure ~~pursuant to section 552(b)(3) of title 5,~~ upon a written determination that—

(1) the information is—

(A) Department of Defense critical infrastructure security information;

(B) covered information pertaining to military tactics, techniques, or procedures; or

(C) covered information pertaining to rules of engagement or rules for the use of force; and

(2) the public interest consideration in the disclosure of such information does not outweigh preventing the disclosure of such information.

(b) DESIGNATION OF DEPARTMENT OF DEFENSE ~~CRITICAL INFRASTRUCTURE SECURITY~~ INFORMATION.—In addition to any other authority or requirement regarding protection from dissemination of information, the Secretary may designate information as being ~~Department of Defense critical infrastructure security identified~~ information identified in subsection (a)(1), including during the course of creating such information, to ensure that such information is not disseminated without authorization. Information so designated is subject to the determination process under subsection (a) to determine whether to exempt such information from disclosure described in such subsection.

(c) INFORMATION PROVIDED TO STATE AND LOCAL GOVERNMENTS.—(1) Department of Defense ~~critical infrastructure security~~ information covered by a written determination under subsection (a) or designated under subsection (b) that is provided to a State or local government shall remain under the control of the Department of Defense.

(2)(A) A State or local law authorizing or requiring a State or local government to disclose Department of Defense ~~critical infrastructure security~~ information that is covered by a written determination under subsection (a) shall not apply to such information.

(B) If a person requests pursuant to a State or local law that a State or local government disclose information that is designated as ~~Department of Defense critical infrastructure security~~ information exempt from disclosure under subsection (b), the State or local government shall provide the Secretary an opportunity to carry out the determination process under subsection (a) to determine whether to exempt such information from disclosure pursuant to subparagraph (A).

~~(d) DELEGATION.—The Secretary of Defense may delegate the authority to make a determination under subsection (a) to the Director of Administration and Management.~~

(~~e~~ d) TRANSPARENCY.—Each determination of the Secretary~~, or the Secretary's designee,~~ under subsection (a) shall be made in writing and accompanied by a statement of the basis for the determination. All such determinations and statements of basis shall be available to the public, upon request, ~~though the Office of the Director of Administration and Management~~ in accordance with guidelines prescribed by the Secretary.

(e) CITATION FOR PURPOSES OF OPEN FOIA ACT OF 2009.—This section shall be treated as a statute that specifically exempts certain matters from disclosure under section 552 of title 5, as described in subsection (b)(3) of that section.

(f) DEFINITIONS.—In this section~~, the term~~:

(1) ADVERSARY.—The term "adversary" means a party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged.

(2) COVERED INFORMATION PERTAINING TO MILITARY TACTICS, TECHNIQUES, OR PROCEDURES.—The term 'covered information pertaining to military tactics, techniques,

or procedures' means information pertaining to military tactics, techniques, or procedures that identifies a method for using equipment or personnel to accomplish a specific mission under a particular set of operational or exercise conditions (including offensive, defensive, force protection, cyberspace, stability, civil support, freedom of navigation, operations security, counter intelligence, and intelligence collection operations) the public disclosure of which could reasonably be expected to provide a military advantage to an adversary.

(3) COVERED INFORMATION PERTAINING TO RULES OF ENGAGEMENT OR RULES FOR THE USE OF FORCE.—The term 'covered information pertaining to rules of engagement or rules for the use of force' means information pertaining to rules of engagement or rules for the use of force the public disclosure of which could reasonably be expected to provide an operational military advantage to an adversary.

(4) DEPARTMENT OF DEFENSE CRITICAL INFRASTRUCTURE SECURITY INFORMATION.—The term "Department of Defense critical infrastructure security information" means sensitive but unclassified information that, if disclosed, would reveal capabilities or vulnerabilities in Department of Defense critical infrastructure that, if exploited, would likely result in the significant disruption, destruction, or damage of or to Department of Defense operations, property, or facilities, including—

(A) information regarding the securing and safeguarding of explosives, hazardous chemicals, or pipelines, related to critical infrastructure or protected equipment and systems owned or operated by or on behalf of the Department of Defense~~,~~;

(B) ~~including~~ vulnerability assessments prepared by or on behalf of the Department of Defense~~,~~;

(C) explosives safety information, ~~(~~including storage and handling information~~),~~; and

(D) other site-specific information on or relating to installation security.

(5) MILITARY TACTICS, TECHNIQUES, AND PROCEDURES.—The terms 'military tactics, techniques, and procedures' means—

(A) the employment and ordered arrangement of military forces in relation to each other;

(B) a non-prescriptive way or method used to perform a mission, function, or task that is—

(i) related to or incidental to combat missions or contingency operations; or

(ii) directly related to preparing for, going to, or returning from combat missions or contingency operations; or

(C) detailed steps that prescribe how to perform a specific task that is—

(i) related to, or incidental to, a combat mission, force protection operation, or contingency operation; or

(ii) directly related to preparing for, going to, or returning from combat missions, force protection operations, or contingency operations.

(6) RULES FOR THE USE OF FORCE.—The term "rules for the use of force" means directives issued to guide United States forces on the use of force during various operations.

(7) RULES OF ENGAGEMENT.—The term "rules of engagement" means directives issued by a competent military authority that delineate the circumstances and limitations under which the armed forces will initiate or continue combat engagement with other forces encountered.