SEC. ___. EXEMPTION OF INFORMATION ON MILITARY TACTICS, TECHNIQUES, AND PROCEDURES, AND OF MILITARY RULES OF ENGAGEMENT, FROM RELEASE UNDER FREEDOM OF INFORMATION ACT.

(a) EXEMPTION.—Subsection (a) of section 130e of title 10, United States Code, is amended—

(1) in the matter preceding paragraph (1), by inserting “, military tactic, technique, or procedure information, or rule of engagement information” after “security information”; and

(2) by striking paragraph (1) and inserting the following:

“(1) the information is—

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

“(B) military tactic, technique, or procedure information that identifies a method for using equipment and personnel to accomplish a specific mission under a particular set of operational or exercise conditions, including offensive, defensive, cyberspace, stability, civil support, freedom of navigation, and intelligence collection operations, the public disclosure of which could reasonably be expected to provide an operational military advantage to an adversary; or

“(C) rule of engagement information, the public disclosure of which could reasonably be expected to provide an operational military advantage to an adversary;”.

(b) DELEGATION AND TRANSPARENCY.—Such section is further amended—

(1) by striking subsection (d);

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

(3) in subsection (d), as redesignated by paragraph (2)—

(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”.

(c) CITATION FOR PURPOSES OF OPEN FOIA ACT OF 2009.—Such section is further amended—

(1) in the matter preceding paragraph (1) of subsection (a), as amended by subsection (a) of this section, by striking “pursuant to section 552(b)(3) of title 5”; and

(2) by inserting after subsection (d), as redesignated by subsection (b)(2), the following new subsection:

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

(d) 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) 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 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.

"(3) PROCEDURE.—The term 'procedure' means standard, detailed steps that prescribe how to perform a specific task.

"(4) RULE OF ENGAGEMENT.—The term 'rule of engagement' means a directive issued by a competent military authority that delineates the circumstances and limitations under which the armed forces will initiate or continue combat engagement with other forces encountered.

"(5) TACTIC.—The term 'tactic' means the employment and ordered arrangement of forces in relation to each other.

"(6) TECHNIQUE.—The term 'technique' means a non-prescriptive way or method used to perform a mission, function, or task.".

(e) SECTION HEADING AND CLERICAL AMENDMENT.—

(1) The heading of such section is amended to read as follows:

"§130e. Nondisclosure of information: critical infrastructure; military tactics, techniques, and procedures; military rules of engagement".

(2) The item relating to such section in the table of sections at the beginning of chapter 3 of such title is amended to read as follows:

"130e. Nondisclosure of information: critical infrastructure; military tactics, techniques, and procedures; military rules of engagement.".

[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, 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), and rules of engagement that, if publicly disclosed, could reasonably be expected to provide an operational military advantage to an adversary. Military TTPs 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 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 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.

Budget Implications: 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. The resources reflected in the table below are funded within the FY 2019 President's Budget.

RESOURCE REQUIREMENTS ($MILLIONS)									
	FY 2019	**FY 2020**	**FY 2021**	**FY 2022**	**FY 2023**	**Appropriations From**	**Budget Activity**	**Dash-1 Line Item**	**Program Element**
FOIA Cost Avoidance Army	$-.001	$-.001	$-.001	$-.001	$-.001	Operation and Maintenance, Army	Various	Various	Various
FOIA Cost Avoidance Navy	$-.001	$-.001	$-.001	$-.001	$-.001	Operation and Maintenance, Navy	Various	Various	Various
FOIA Cost Avoidance Air Force	$-.001	$-.001	$-.001	$-.001	$-.001	Operation and Maintenance, Air Force	Various	Various	Various
FOIA Cost Avoidance Defense-Wide	$-.001	$-.001	$-.001	$-.001	$-.001	Operation and Maintenance, Defense-Wide	Various	Various	Various
Total	$-.004	$-.004	$-.004	$-.004	$-.004	--	--	--	--

Changes to Existing Law: The proposal would make the following changes to existing law:

TITLE 10, UNITED STATES CODE

* * * * * * *

CHAPTER 3—General Power and Functions

* * * * * * *

130. Authority to withhold from public disclosure certain technical data.
[130a. Repealed.]
130b. Personnel in overseas, sensitive, or routinely deployable units: nondisclosure of personally identifying information.
130c. Nondisclosure of information: certain sensitive information of foreign governments and international organizations.
130d. Treatment under Freedom of Information Act of certain confidential information shared with State and local personnel.
130e. ~~Treatment under Freedom of Information Act of critical infrastructure security information~~Nondisclosure of information: critical infrastructure; military tactics, techniques, and procedures; military rules of engagement.
130f. Congressional notification regarding sensitive military operations.

* * * * * * *

§130e. ~~Treatment under Freedom of Information Act of critical infrastructure security information~~Nondisclosure of information: critical infrastructure; military tactics, techniques, and procedures; military rules of engagement

(a) EXEMPTION.—The Secretary of Defense may exempt Department of Defense critical infrastructure security information, military tactic, technique, or procedure information, or rule of engagement 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) military tactic, technique, or procedure information that identifies a method for using equipment and personnel to accomplish a specific mission under a particular set of operational or exercise conditions, including offensive, defensive, cyberspace, stability, civil support, freedom of navigation, and intelligence collection operations, the public disclosure of which could reasonably be expected to provide an operational military advantage to an adversary; or

(C) rule of engagement information, the public disclosure of which could reasonably be expected to provide an operational military advantage to an adversary; 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 information, 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 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 is 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~~, t~~:

(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) 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 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) ~~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.

(3) PROCEDURE.—The term "procedure" means standard, detailed steps that prescribe how to perform a specific task.

(4) RULE OF ENGAGEMENT.—The term "rule of engagement" means a directive issued by a competent military authority that delineates the circumstances and limitations

under which the armed forces will initiate or continue combat engagement with other forces encountered.

(5) TACTIC.—The term "tactic" means the employment and ordered arrangement of forces in relation to each other.

(6) TECHNIQUE.—The term "technique" means a non-prescriptive way or method used to perform a mission, function, or task.