SEC. 1014. TREATMENT UNDER FREEDOM OF INFORMATION ACT OF CERTAIN DEPARTMENT OF DEFENSE CRITICAL INFRASTRUCTURE INFORMATION.

(a) IN GENERAL.—Chapter 3 of title 10, United States Code, is amended by adding at the end the following new section:

"§ 130e. Treatment under Freedom of Information Act of critical infrastructure information

"(a) EXEMPTION.—Department of Defense critical infrastructure information that, if disclosed, may result in the disruption, degradation, or destruction of Department of Defense operations, property, or facilities, shall be exempt from disclosure pursuant to section 552(b)(3) of title 5.

"(b) INFORMATION PROVIDED TO STATE AND LOCAL GOVERNMENTS.—Department of Defense critical infrastructure information obtained by a State or local government from a Federal agency shall remain under the control of the Federal agency, and a State or local law authorizing or requiring such a government to disclose information shall not apply to such critical infrastructure information.

"(c) DEFINITION.—In this section, the term 'Department of Defense critical infrastructure information', as determined by the Secretary of Defense, means sensitive but unclassified information related to critical infrastructure or protected systems owned or operated by or on behalf of the Department of Defense, including vulnerability assessments prepared by or on behalf of the Department of Defense, explosives safety information (including storage and handling), and other site-specific information on or relating to installation security.".

1 (b) CLERICAL AMENDMENT.—The table of sections at the beginning of such chapter is

2 amended at the end by adding the following new item:

"130e. Treatment under Freedom of Information Act of certain critical infrastructure information."

Section-by-Section Analysis

This proposal would protect the disclosure of critical infrastructure information, which could threaten the security of the operations, facilities and property of military installations and jeopardize the safety of the people who work in or live near them. Sensitive but unclassified information about critical Department of Defense infrastructure can be used by terrorists and criminals to maximize the effectiveness of their unlawful activities. For example, knowledge of the specific location of explosives, harmful chemicals, alarms, pipelines and manifolds, security stations and devices, or communication centers aboard a military base substantially could facilitate the effectiveness of an attack designed to destroy equipment, create maximum casualties, or steal particularly sensitive military weapons. This proposal enables the Department of Defense to evaluate the vulnerabilities of its critical infrastructure without concern that the information could be used to disrupt or attack Department of Defense operations, property, or life.

Such information is generally not classified because it must be shared with first responders and community officials on a restricted, need-to-know basis to assist in planning for emergency responses and other planning functions. Classifying the information would hinder the Department of Defense's ability to provide critical information to first responders and, as a result, degrade the ability of State and local responders to provide required emergency assistance.

Federal law provides for protection of similar information when it is voluntarily provided to the Federal government by critical infrastructure owners and operators. *See* 6 U.S.C. §§ 131-134. The Critical Infrastructure Information Act of 2002 and the PCII Final Rule (6 CFR Part 29) provide authority and direction for the process, requirements, and protections under which the Federal government may obtain, use, and disclose critical infrastructure information. Since the PCII program currently protects non-Federal information, sensitive critical infrastructure information related to DOD owned or managed infrastructure is currently vulnerable to release under FOIA and needs to be explicitly protected. This legislation will provide this sensitive information effective protection to reduce the risks of unauthorized or inadvertent disclosure by making such material exempt from disclosure under exemption (b)(3) of the Freedom of Information Act and any similar State or local law(s).

Budget Implications: The proposal does not impact budgetary resources because protecting this material will not require an expenditure of funds.

Changes to Existing Law: This proposal would add a new section 130e to title 10, United States Code. The text of the new section is set forth in the legislative proposal.