SEC. ____. REPEAL OF PROCEDURES AND REPORTING REQUIREMENT ON LOSS OF PERSONALLY IDENTIFIABLE INFORMATION.

Section 1639 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 132 Stat. 2129; 10 U.S.C. 2224 is amended—

(1) in the section heading, by striking "**CYBERSECURITY BREACHES AND LOSS OF PERSONALLY IDENTIFIABLE INFORMATION**" and inserting "**SIGNIFICANT LOSSES OF CONTROLLED UNCLASSIFIED INFORMATION BY CLEARED DEFENSE CONTRACTORS"**;

(2) in subsection (a), by striking "a significant loss of personally identifiable information of civilian or uniformed members of the Armed Forces, or a";

(3) in subsection (b), by striking "the protection of personally identifiable information of civilian and uniformed members of the Armed Forces,"; and

(4) in subsection (c)—

(A) by striking paragraph (2); and

(B) by striking "DEFINITIONS.—" and all that follows through "The term" and inserting the following: "SIGNIFICANT LOSS OF CONTROLLED UNCLASSIFIED INFORMATION DEFINED.—The term".

[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 repeal the requirement for DoD to notify and establish reporting procedures to the congressional defense committees for significant losses of personally identifiable information (PII)—defined to include PII losses "involving 250 or more civilian or uniformed members of the Armed Forces". Repeal of this requirement would restore uniformity and consistency of breach reporting procedures to all executive branch agencies, without singling out DoD and requiring it to apply more restrictive, and potentially conflicting procedures outside of the framework established by the Office of Management and Budget in implementing the

Federal Information Security Modernization Act (FISMA), 44 U.S.C. Chapter 35.

Section 1639 of the FY 2019 National Defense Authorization Act (NDAA) (Public Law 115-232) requires the Department to report "significant losses of controlled unclassified information by a cleared defense contractor" and breaches "involving 250 or more civilian or uniformed members of the Armed Forces" to congressional defense committees. As Congress has already mandated under FISMA, OMB is required to provide guidance on data breach notification policies and procedures, including executive branch agency responsibilities for reporting breaches of PII and reporting other incidents to certain congressional committees. In accordance with FISMA, OMB promulgated its data breach notification guidance in M-17-12,[1] which requires all Federal executive branch agencies to report breaches that are deemed "major incidents" to 11 Congressional Committees[2] no later than seven days after the date on which there is a reasonable basis to conclude that a major incident has occurred, and to supplement the initial notification no later than 30 days after discovery of the breach. The OMB Memorandum M-20-04 defines "major incident" in relevant part as (1) "[a]ny incident[3] that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people…."; or (2) "a breach that involves personally identifiable information (PII) that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people." OMB Memorandum M-20-04 "requires a determination of major incident for any unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to the *PII of 100,000 or more people*." (emphasis added) Consistent with OMB guidance and the above definition of "major incident," DoD has made the determination that reaching the 100,000 individual threshold ***automatically*** constitutes a major incident. By repealing the PII requirement in section 1639, DoD would follow a singular framework for reporting breaches of PII to Congress afforded to all other executive branch agencies under the guidance issued by OMB pursuant to the FISMA.

In addition, the existing language from section 1639 of the FY 2019 NDAA uses improper and/or contradictory terminology, which results in interpretive difficulties and inconsistent application. For example, subsection (a) identifies the scope of the requirement to apply to the loss of personally identifiable information of ***civilian and uniformed members of the Armed Forces***. (emphasis added) First, there are no civilian members of the Armed Forces and, as written, the section would not require DoD to calculate breaches of personally identifiable information pertaining to DoD civilian employees whether employed by a military

---

[1] Office of Management and Budget Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," January 3, 2017.

[2] FISMA requires notification to the House Committees on Oversight and Government Reform; Homeland Security; Science, Space, and Technology; Judiciary; Armed Services; and Appropriations; and to the Senate Committees on Homeland Security and Governmental Affairs; Commerce, Science, and Transportation; Judiciary; Armed Services; and Appropriations. 44 U.S.C. §§ 3554(b)(7)(C)(iii)(III), 3554(c)(1), 3553 note

[3] FISMA 2014 defines "incident" as: "an occurrence that—(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." 44 U.S.C. § 3552(b)(2).

department or the fourth estate. Second, the intended scope of covered members is not entirely clear. The term "Armed Forces" applies to not only the Departments of the Army, Navy, and Air Force but also to the Coast Guard, which is usually under the control of the Secretary of Homeland Security. Moreover, another term "Uniformed Services," applies to not only the Departments of the Army, Navy, and Air Force, but also to the Coast Guard, United States Public Health Service, and National Oceanic and Atmospheric Administration. The Coast Guard, United States Public Health Service, and the National Oceanic and Atmospheric Administration do not report breaches through the DoD.

Further, subsection (c)(2) introduces a definition—"significant loss of personally identifiable information"—that implicates two existing and well recognized terms defined by OMB. The first, "significant loss" implicates and is at odds with the OMB definition of "major incident." The second term, "personally identifiable information," is inconsistent with the definition established by OMB as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."[4]

Repeal of the provisions pertaining to the PII reporting requirement would greatly clarify and unify DoD's reporting responsibilities as it would follow the rules already known and established by OMB in accordance with the FISMA.

Budget Implications: This proposal has no significant budgetary impact. Incidental costs or savings are accounted for within the Fiscal Year (FY) 2021 President's Budget.

Changes to Existing Law: This proposal would amend section 1639 of Public Law 115–232 as follows:

SEC. 1639. PROCEDURES AND REPORTING REQUIREMENT ON ~~CYBERSECURITY BREACHES AND LOSS OF PERSONALLY IDENTIFIABLE INFORMATION~~ SIGNIFICANT LOSSES OF CONTROLLED UNCLASSIFIED INFORMATION BY CLEARED DEFENSE CONTRACTORS.

(a) IN GENERAL.—In the event of a ~~significant loss of personally identifiable information of civilian or uniformed members of the Armed Forces, or a~~ significant loss of controlled unclassified information by a cleared defense contractor, the Secretary of Defense shall promptly submit to the congressional defense committees notice in writing of such loss. Such notice may be submitted in classified or unclassified formats.

(b) PROCEDURES.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall establish and submit to the congressional defense committees procedures for complying with the requirement of subsection (a). Such procedures shall be consistent with the national security of the United States, the protection of operational integrity, ~~the protection of personally identifiable information of civilian and uniformed members of the Armed Forces,~~ and the protection of controlled unclassified information.

[4] OMB Circular A-130, Managing Information as a Strategic Resource, July 28, 2016.

(c) ~~DEFINITIONS.—In this section:~~

~~(1)~~ SIGNIFICANT LOSS OF CONTROLLED UNCLASSIFIED INFORMATION DEFINED.—The term ''significant loss of controlled unclassified information'' means an intentional, accidental, or otherwise known theft, loss, or disclosure of Department of Defense programmatic or technical controlled unclassified information the loss of which would have significant impact or consequence to a program or mission of the Department of Defense, or the loss of which is of substantial volume.

~~(2) SIGNIFICANT LOSS OF PERSONALLY IDENTIFIABLE INFORMATION.—The term ''significant loss of personally identifiable information'' means an intentional, accidental, or otherwise known disclosure of information that can be used to distinguish or trace an individual's identity, such as the name, Social Security number, date and place of birth, biometric records, home or other phone numbers, or other demographic, personnel, medical, or financial information, involving 250 or more civilian or uniformed members of the Armed Forces.~~