

Subsec. (a). Pub. L. 116-283, §1851(c)(4), substituted “sections 3201 through 3205” for “section 2304” in introductory provisions.

#### Statutory Notes and Related Subsidiaries

##### EFFECTIVE DATE OF 2021 AMENDMENT

Amendment by Pub. L. 116-283 effective Jan. 1, 2022, with additional provisions for delayed implementation and applicability of existing law, see section 1801(d) of Pub. L. 116-283, set out as a note preceding section 3001 of this title.

##### EFFECTIVE DATE

Section effective Jan. 1, 2017, see section 806(a)(2) of Pub. L. 114-328, set out as a note under section 4421 of this title.

#### § 4425. Definition of weapon system component

In this subchapter, the term “weapon system component” has the meaning given the term “major system component” in section 4401 of this title.

(Added Pub. L. 114-328, div. A, title VIII, §806(a)(1), Dec. 23, 2016, 130 Stat. 2259, §2447e; renumbered §4425 and amended Pub. L. 116-283, div. A, title XVIII, §1851(c)(1), (5), Jan. 1, 2021, 134 Stat. 4272, 4273.)

#### Editorial Notes

##### AMENDMENTS

2021—Pub. L. 116-283, §1851(c)(5), substituted “section 4401” for “section 2446a”.

Pub. L. 116-283, §1851(c)(1), renumbered section 2447e of this title as this section.

#### Statutory Notes and Related Subsidiaries

##### EFFECTIVE DATE OF 2021 AMENDMENT

Amendment by Pub. L. 116-283 effective Jan. 1, 2022, with additional provisions for delayed implementation and applicability of existing law, see section 1801(d) of Pub. L. 116-283, set out as a note preceding section 3001 of this title.

##### EFFECTIVE DATE

Section effective Jan. 1, 2017, see section 806(a)(2) of Pub. L. 114-328, set out as a note under section 4421 of this title.

### Subpart G—Other Special Categories Of Contracting

#### Editorial Notes

##### AMENDMENTS

2018—Pub. L. 115-232, div. A, title VIII, §801(a), Aug. 13, 2018, 132 Stat. 1830, added subpart heading.

#### Statutory Notes and Related Subsidiaries

REQUIRING DEFENSE MICROELECTRONICS PRODUCTS AND SERVICES MEET TRUSTED SUPPLY CHAIN AND OPERATIONAL SECURITY STANDARDS

Pub. L. 116-92, div. A, title II, §224, Dec. 20, 2019, 133 Stat. 1266, provided that:

“(a) PURCHASES.—To protect the United States from intellectual property theft and to ensure national security and public safety in the application of new generations of wireless network technology and microelectronics, beginning no later than January 1, 2023, the Secretary of Defense shall ensure that each microelectronics product or service that the Department of De-

fense purchases on or after such date meets the applicable trusted supply chain and operational security standards established pursuant to subsection (b), except in a case in which the Department seeks to purchase a microelectronics product or service but—

“(1) no such product or service is available for purchase that meets such standards; or

“(2) no such product or service is available for purchase that—

“(A) meets such standards; and

“(B) is available at a price that the Secretary does not consider prohibitively expensive.

“(b) TRUSTED SUPPLY CHAIN AND OPERATIONAL SECURITY STANDARDS.—

“(1) STANDARDS REQUIRED.—(A) Not later than January 1, 2021, the Secretary shall establish trusted supply chain and operational security standards for the purchase of microelectronics products and services by the Department.

“(B) For purposes of this section, a trusted supply chain and operational security standard—

“(i) is a standard that systematizes best practices relevant to—

“(I) manufacturing location;

“(II) company ownership;

“(III) workforce composition;

“(IV) access during manufacturing, suppliers’ design, sourcing, manufacturing, packaging, and distribution processes;

“(V) reliability of the supply chain; and

“(VI) other matters germane to supply chain and operational security; and

“(ii) is not a military standard (also known as ‘MIL-STD’) or a military specification (also known as ‘MIL-SPEC’) for microelectronics that—

“(I) specifies individual features for Department of Defense microelectronics; or

“(II) otherwise inhibits the acquisition by the Department of securely manufactured, commercially-available products.

“(2) CONSULTATION REQUIRED.—In developing standards under paragraph (1), the Secretary shall consult with the following:

“(A) The Secretary of Homeland Security, the Secretary of State, the Secretary of Commerce, and the Director of the National Institute of Standards and Technology.

“(B) Suppliers of microelectronics products and services from the United States and allies and partners of the United States.

“(C) Representatives of major United States industry sectors that rely on a trusted supply chain and the operational security of microelectronics products and services.

“(D) Representatives of the United States insurance industry.

“(3) TIERS OF TRUST AND LEVELS OF SECURITY AUTHORIZED.—In carrying out paragraph (1), the Secretary may establish tiers and levels of trust and security within the supply chain and operational security standards for microelectronics products and services.

“(4) GENERAL APPLICABILITY.—The standards established pursuant to paragraph (1) shall be, to the greatest extent practicable, generally applicable to the trusted supply chain and operational security needs and use cases of the United States Government and commercial industry, such that the standards could be widely adopted by government agencies, commercial industry, and allies and partners of the United States as the basis for procuring microelectronics products and services.

“(5) ANNUAL REVIEW.—Not later than October 1 of each year, the Secretary shall, in consultation with persons and entities set forth under paragraph (2), review the standards established pursuant to paragraph (1) and issue updates or modifications as the Secretary considers necessary or appropriate.

“(c) ENSURING ABILITY TO SELL COMMERCIALY.—

“(1) IN GENERAL.—The Secretary shall, to the greatest extent practicable, ensure that suppliers of micro-