

ment (including but not limited to analysis of chemical, biological, radiological, and nuclear agents, the means by which such agents could be weaponized or used in a terrorist attack, and the capabilities, plans, and intentions of terrorists and other non-state actors who may have or acquire such agents). All such analysts shall meet the applicable standards and qualifications for the performance of intelligence activities promulgated by the Director of Central Intelligence pursuant to section 403-4<sup>1</sup> of title 50.

**(2) Intelligence sharing infrastructure**

For the purpose of carrying out the acquisition and deployment of secure facilities (including information technology and physical infrastructure, whether mobile and temporary, or permanent) sufficient to permit the Secretary to receive, not later than 180 days after July 21, 2004, all classified information and products to which the Under Secretary for Intelligence and Analysis is entitled under part A of subchapter II, there are authorized to be appropriated such sums as may be necessary for each of the fiscal years 2004 through 2006.

(Pub. L. 107-296, title V, § 521, formerly § 510, as added Pub. L. 108-276, § 3(b)(2), July 21, 2004, 118 Stat. 852; renumbered § 521, Pub. L. 109-295, title VI, § 611(7), Oct. 4, 2006, 120 Stat. 1395; amended Pub. L. 109-417, title IV, § 403(c), Dec. 19, 2006, 120 Stat. 2874; Pub. L. 110-53, title V, § 531(b)(1)(D), Aug. 3, 2007, 121 Stat. 334.)

REFERENCES IN TEXT

Section 247d-6b(c)(1)(B) of title 42, referred to in subsec. (a), was in the original “section 319F-2(c)(1)(B)”, which was translated as meaning section 319F-2(c)(1)(B) of the Public Health Service Act, to reflect the probable intent of Congress.

Section 403-4 of title 50, referred to in subsec. (d)(1), was repealed and a new section 403-4 enacted by Pub. L. 108-458, title I, § 1011(a), Dec. 17, 2004, 118 Stat. 3660, and subsequently editorially reclassified to section 3035 of Title 50, War and National Defense; as so enacted, section 3035 no longer relates to promulgation of standards and qualifications for the performance of intelligence activities.

Part A of subchapter II of this chapter, referred to in subsec. (d)(2), was in the original “subtitle A of title II”, meaning subtitle A of title II of Pub. L. 107-296, Nov. 25, 2002, 116 Stat. 2145, which is classified generally to part A (§121 et seq.) of subchapter II of this chapter. For complete classification of part A to the Code, see Tables.

CODIFICATION

Section was formerly classified to section 320 of this title prior to renumbering by Pub. L. 109-295.

AMENDMENTS

2007—Subsec. (d)(1). Pub. L. 110-53, § 531(b)(1)(D)(i), substituted “Office of Intelligence and Analysis” for “Directorate for Information Analysis and Infrastructure Protection”.

Subsec. (d)(2). Pub. L. 110-53, § 531(b)(1)(D)(ii), substituted “Under Secretary for Intelligence and Analysis” for “Under Secretary for Information Analysis and Infrastructure Protection”.

2006—Subsec. (a). Pub. L. 109-417, which directed amendment of section 510(a) of the Homeland Security Act of 2002, Pub. L. 107-296, by inserting a new last sentence, was executed to subsec. (a) of this section to reflect the probable intent of Congress and the redesignation of section 510(a) as 521(a) by Pub. L. 109-295, § 611(7).

CHANGE OF NAME

Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director’s capacity as the head of the intelligence community deemed to be a reference to the Director of National Intelligence. Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director’s capacity as the head of the Central Intelligence Agency deemed to be a reference to the Director of the Central Intelligence Agency. See section 1081(a), (b) of Pub. L. 108-458, set out as a note under section 3001 of Title 50, War and National Defense.

**§ 321k. Model standards and guidelines for critical infrastructure workers**

**(a) In general**

Not later than 12 months after August 3, 2007, and in coordination with appropriate national professional organizations, Federal, State, local, and tribal government agencies, and private-sector and nongovernmental entities, the Administrator shall establish model standards and guidelines for credentialing critical infrastructure workers that may be used by a State to credential critical infrastructure workers that may respond to a natural disaster, act of terrorism, or other man-made disaster.

**(b) Distribution and assistance**

The Administrator shall provide the standards developed under subsection (a), including detailed written guidance, to State, local, and tribal governments, and provide expertise and technical assistance to aid such governments with credentialing critical infrastructure workers that may respond to a natural disaster, act of terrorism, or other manmade disaster.

(Pub. L. 107-296, title V, § 522, as added Pub. L. 110-53, title IV, § 409(a), Aug. 3, 2007, 121 Stat. 305.)

**§ 321l. Guidance and recommendations**

**(a) In general**

Consistent with their responsibilities and authorities under law, as of the day before August 3, 2007, the Administrator and the Director of Cybersecurity and Infrastructure Security, in consultation with the private sector, may develop guidance or recommendations and identify best practices to assist or foster action by the private sector in—

- (1) identifying potential hazards and assessing risks and impacts;
- (2) mitigating the impact of a wide variety of hazards, including weapons of mass destruction;
- (3) managing necessary emergency preparedness and response resources;
- (4) developing mutual aid agreements;
- (5) developing and maintaining emergency preparedness and response plans, and associated operational procedures;
- (6) developing and conducting training and exercises to support and evaluate emergency preparedness and response plans and operational procedures;
- (7) developing and conducting training programs for security guards to implement emergency preparedness and response plans and operations procedures; and