(A) teach employees how to identify counterfeit parts;

(B) educate employees on procedures to follow if they suspect a part is counterfeit;

(C) regularly update employees on new threats, identification techniques, and reporting requirements; and

(D) integrate industry associations, manufacturers, suppliers, and other Federal agencies, as appropriate;

(2) an internal database to track all suspected and confirmed counterfeit electronic parts that will maintain, at a minimum—

(A) companies and individuals known and suspected of selling counterfeit parts;

(B) parts known and suspected of being counterfeit, including lot and date codes, part numbers, and part images;

(C) countries of origin;

(D) sources of reporting;

(E) United States Customs seizures; and

(F) Government-Industry Data Exchange Program reports and other public or private sector database notifications; and

(3) a mechanism to report all information on suspected and confirmed counterfeit electronic parts to law enforcement agencies, industry associations, and other databases, and to issue bulletins to industry on counterfeit electronic parts and related counterfeit activity.

(c) Review of procurement and acquisition policy

(1) In general

In establishing the program, the Administrator shall amend existing acquisition and procurement policy to purchase electronic parts from trusted or approved manufacturers. To determine trusted or approved manufacturers, the Administrator shall establish a list, assessed and adjusted at least annually, and create criteria for manufacturers to meet in order to be placed onto the list.

(2) Criteria

The criteria may include—

(A) authentication or encryption codes;

(B) embedded security markings in parts;

(C) unique, harder to copy labels and markings;

(D) identifying distinct lot and serial codes on external packaging;

(E) radio frequency identification embedded into high-value parts;

(F) physical destruction of all defective, damaged, and sub-standard parts that are by-products of the manufacturing process;

(G) testing certifications;

(H) maintenance of procedures for handling any counterfeit parts that slip through;

(I) maintenance of secure facilities to prevent unauthorized access to proprietary information; and

(J) maintenance of product return, buy back, and inventory control practices that limit counterfeiting.

(d) Report to Congress

Within one year after October 11, 2010, the Administrator shall report on the progress of implementing this section to the appropriate committees of Congress.

(Pub. L. 111–267, title XII, §1206, Oct. 11, 2010, 124 Stat. 2843.)

§ 18445. Information security

(a) Monitoring risk

(1) Update on system implementation

Not later than 120 days after October 11, 2010, and on a biennial basis thereafter, the chief information officer of NASA, in coordination with other national security agencies, shall provide to the appropriate committees of Congress—

(A) an update on efforts to implement a system to provide dynamic, comprehensive, real-time information regarding risk of unauthorized remote, proximity, and insider use or access, for all information infrastructure under the responsibility of the chief information officer, and mission-related networks, including contractor networks;

(B) an assessment of whether the system has demonstrably and quantifiably reduced network risk compared to alternative methods of measuring security; and

(C) an assessment of the progress that each center and facility has made toward implementing the system.

(2) Existing assessments

The assessments required of the Inspector General under section 3545[1] of title 44 shall evaluate the effectiveness of the system described in this subsection.

(b) Information security awareness and education

(1) In general

In consultation with the Department of Education, other national security agencies, and other agency directorates, the chief information officer shall institute an information security awareness and education program for all operators and users of NASA information infrastructure, with the goal of reducing unauthorized remote, proximity, and insider use or access.

(2) Program requirements

(A) The program shall include, at a minimum, ongoing classified and unclassified threat-based briefings, and automated exercises and examinations that simulate common attack techniques.

(B) All agency employees and contractors engaged in the operation or use of agency information infrastructure shall participate in the program.

(C) Access to NASA information infrastructure shall only be granted to operators and users who regularly satisfy the requirements of the program.

(D) The chief human capital officer of NASA, in consultation with the chief information officer, shall create a system to reward operators and users of agency information infrastructure for continuous high achievement in the program.

[1] See References in Text note below.

(c) Information infrastructure defined

In this section, the term ''information infrastructure'' means the underlying framework that information systems and assets rely on to process, transmit, receive, or store information electronically, including programmable electronic devices and communications networks and any associated hardware, software, or data.

(Pub. L. 111–267, title XII, § 1207, Oct. 11, 2010, 124 Stat. 2844.)

REFERENCES IN TEXT

Section 3545 of title 44, referred to in subsec. (a)(2), was repealed by Pub. L. 113–283, § 2(a), Dec. 18, 2014, 128 Stat. 3073. Provisions similar to section 3545 of title 44 are now contained in section 3555 of title 44, as enacted by Pub. L. 113–283.