SEC. 17. STRATEGY TO SECURE EMAIL.

(a) IN GENERAL.—Not later than December 31, 2021, the Secretary of Homeland Security shall develop and submit to Congress a strategy, including recommendations, to implement across all United States-based email providers Domain-based Message Authentication, Reporting, and Conformance standard at scale.

(b) ELEMENTS.—The strategy required under subsection (a) shall include the following:

(1) A recommendation for the minimum size threshold for United States-based email providers for applicability of Domain-based Message Authentication, Reporting, and Conformance.

(2) A description of the security and privacy benefits of implementing the Domain-based Message Authentication, Reporting, and Conformance standard at scale, including recommendations for national security exemptions, as appropriate, as well as the burdens of such implementation and an identifica-
tion of the entities on which such burdens would most likely fall.

(3) An identification of key United States and international stakeholders associated with such implementation.

(4) An identification of any barriers to such implementing, including a cost-benefit analysis where feasible.

(5) An initial estimate of the total cost to the Federal Government and implementing entities in the private sector of such implementing, including recommendations for defraying such costs, if applicable.

(e) Consultation.—In developing the strategies and recommendations under subsection (a), the Secretary of Homeland Security may, as appropriate, consult with representatives from the information technology sector.

(d) Definition.—In this section, the term “Domain-based Message Authentication, Reporting, and Conformance” means an email authentication, policy, and reporting protocol that verifies the authenticity of the sender of an email and blocks and reports to the sender fraudulent accounts.