

Calendar No. 382

114TH CONGRESS }
2d Session }

SENATE

{ REPORT
114-222 }

AIRPORT SECURITY ENHANCEMENT AND
OVERSIGHT ACT

R E P O R T

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND
TRANSPORTATION

ON

S. 2361



MARCH 7, 2016.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE

59-010

WASHINGTON : 2016

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

JOHN THUNE, South Dakota, *Chairman*

ROGER F. WICKER, Mississippi	BILL NELSON, Florida
ROY BLUNT, Missouri	MARIA CANTWELL, Washington
MARCO RUBIO, Florida	CLAIRE MCCASKILL, Missouri
KELLY AYOTTE, New Hampshire	AMY KLOBUCHAR, Minnesota
TED CRUZ, Texas	RICHARD BLUMENTHAL, Connecticut
DEB FISCHER, Nebraska	BRIAN SCHATZ, Hawaii
JERRY MORAN, Kansas	ED MARKEY, Massachusetts
DAN SULLIVAN, Alaska	CORY BOOKER, New Jersey
RON JOHNSON, Wisconsin	TOM UDALL, New Mexico
DEAN HELLER, Nevada	JOE MANCHIN, West Virginia
CORY GARDNER, Colorado	GARY PETERS, Michigan
STEVE DAINES, Montana	

NICK ROSSI, *Staff Director*

ADRIAN ARNAKIS, *Deputy Staff Director*

REBECCA SEIDEL, *General Counsel*

KIM LIPSKY, *Democratic Staff Director*

CHRISTOPHER DAY, *Democratic Deputy Staff Director*

CLINT ODOM, *Democratic General Counsel*

Calendar No. 382

114TH CONGRESS }
2d Session }

SENATE

{ REPORT
{ 114-222

AIRPORT SECURITY ENHANCEMENT AND OVERSIGHT ACT

MARCH 7, 2016.—Ordered to be printed

Mr. THUNE, from the Committee on Commerce, Science, and
Transportation, submitted the following

R E P O R T

[To accompany S. 2361]

The Committee on Commerce, Science, and Transportation, to which was referred the bill (S. 2361) to enhance airport security, and for other purposes, having considered the same, reports favorably thereon with an amendment (in the nature of a substitute) and recommends that the bill (as amended) do pass.

PURPOSE OF THE BILL

The purpose of S. 2361 is to improve oversight, vetting, and credentialing of airport workers with access to the secure area of an airport, and for other purposes.

BACKGROUND AND NEEDS

The need for enhanced oversight of airport workers with access to secure areas stems from findings of recent security gaps and a growing concern about aviation security in an environment threatened by global terrorism. A number of airport security vulnerabilities exposed within the last year, including missing and improper use of Secure Identification Display Area (SIDA) badges by airport and airline workers, a Department of Homeland Security (DHS) Office of Inspector General (OIG) report finding that the Transportation Security Administration (TSA) did not identify 73 airport workers with potential links to terrorism due to gaps in current interagency watchlisting policy, and the fact that the TSA does not exercise an appropriately rigorous oversight plan related to lost or missing SIDA badges, have made it clear that enhancements to airport security are needed to ensure greater public safety.

The Airport Security Enhancement and Oversight Act of 2015 builds upon the bipartisan TSA oversight efforts of the Committee in 2015, including classified briefings and three oversight letters to the TSA on the improper use of SIDA badges and the TSA's access to the U.S. Government's consolidated terrorism database, known as the Terrorist Identities Datamart Environment (TIDE). Additionally, the bill would authorize activities recommended by the Aviation Stakeholder Advisory Committee (ASAC) for improving airport employee access controls, which the TSA has been slow to implement in some cases.

SUMMARY OF PROVISIONS

S. 2361 would improve vetting, credentialing, and inspections of airport workers with access to the SIDA of an airport, and would increase TSA oversight responsibilities regarding airport workers with missing SIDA credentials and airports with chronic under-performance on badge accountability. This bill also would require the TSA Administrator to conduct an updated threat assessment regarding airport workers with SIDA credentials and the security measures in place to address resulting vulnerabilities in light of recent international terrorist activity, to revise the rules on unescorted airport access controls, to make the expiration date on each airport credential issued to a non-United States citizen consistent with such individual's immigration status, and to enhance the eligibility requirements and disqualifying criminal offenses for individuals seeking or having unescorted access to a SIDA of an airport based on similar criteria utilized by U.S. Customs and Border Protection (CBP) and other DHS programs.

This bill also would improve airport worker vetting by requiring the TSA Administrator to implement the Federal Bureau of Investigation's (FBI) "Rap Back" service for recurrent background checks of SIDA badge holders, and by requiring that the TSA receive automated, real-time access to additional terrorism-related information in the TIDE database. Under the bill, airport operators also would be granted direct access to the E-Verify program and the Systematic Alien Verification for Entitlements (SAVE) automated system in order to determine the eligibility based on immigration status of individuals seeking unescorted access authority to a SIDA of an airport.

The bill also would require the TSA Administrator to develop and implement airport access control performance metrics and best practices, and expand the use of random physical inspections of airport workers with SIDA access. The TSA Administrator also would be directed to disseminate best practices on airport worker screening based on a review of airports that have implemented comprehensive screening, and conduct red-team, covert testing of SIDA access controls.

The bill also would require the TSA Administrator to conduct a comprehensive review of current security directives. The purpose of this review would be to streamline, consolidate, or revoke security directives to most efficiently maximize risk reduction as necessary. One year after the date of enactment, the Comptroller General of the United States would be required to submit a report to Congress that assesses the progress made by the TSA in implementing the

oversight, credentialing, vetting, and inspection requirements under the bill.

LEGISLATIVE HISTORY

On December 7, 2015, S. 2361, the Airport Security Enhancement and Oversight Act was introduced by Senators Thune, Nelson, Ayotte, and Cantwell. The bill is also cosponsored by Senators Johnson and Klobuchar. The bill is a complementary proposal to H.R. 2750, the Improved Security Vetting for Aviation Workers Act, and H.R. 3102, the Airport Access Control Security Improvement Act, which passed the House of Representatives by voice votes on July 27, 2015, and on October 6, 2015, respectively. H.R. 2750 was introduced by Representatives Katko (R-NY), Rice (D-NY), McCaul (R-TX), and Payne (D-NJ) in June 2015, and was ordered to be reported by the Committee on Homeland Security of the House of Representatives in July 2015. H.R. 3102 was introduced by Representatives Katko (R-NY), Rice (D-NY), and McCaul (R-TX) in July 2015, and was ordered to be reported by the Committee on Homeland Security of the House of Representatives in October 2015.

No Senate hearings were held on S. 2361 in the 114th Congress. The Committee on Commerce, Science, and Transportation of the Senate however held a hearing on March 17, 2015, entitled "TSA Oversight and Examination of the Fiscal Year 2016 Budget Request," and received testimony from Melvin Carraway, Acting Administrator, Transportation Security Administration, Department of Homeland Security, which responded to questions about SIDA badges. The Committee also held a hearing on May 21, 2015, to consider the nomination of Peter Neffenger to be the TSA Administrator, during which the issue of misused SIDA badges was addressed. The Committee also conducted oversight on missing SIDA badges and airport worker vetting in the 114th Congress with a series of three letters sent to the TSA Administrator by Chairman Thune, Ranking Member Nelson, and other Committee members. The TSA's responses to these letters indicated that the TSA does not maintain a list of lost or missing SIDA badges, and that it rarely uses its enforcement authority to fine airports that reach a certain threshold of missing SIDA badges, prompting related provisions in S. 2361.

In the House of Representatives in the 114th Congress, the Subcommittee on Transportation Security of the Committee on Homeland Security held a two-part hearing on airport access control entitled, "A Review of Access Control Measures at Our Nation's Airports." At part I of the hearing on February 3, 2015, the subcommittee received testimony from Mark Hatfield, Acting Deputy Administrator, TSA, DHS; Doug Perdue, Deputy Assistant Director, Counterterrorism Division, Federal Bureau of Investigation, Department of Justice; Sharon L. Pinkerton, Senior Vice President, Legislative and Regulatory Policy, Airlines for America; and Miguel Southwell, General Manager, Hartsfield-Jackson Atlanta International Airport.

At part II of the hearing on April 30, 2015, the subcommittee received testimony from Melvin J. Carraway, Acting Administrator, TSA, DHS; Jeanne M. Olivier, Assistant Director, Aviation Security and Technology, Security Operations and Programs Department,

the Port Authority of New York & New Jersey, testifying on behalf of the American Association of Airport Executives; and Steven Grossman, Chief Executive Officer/Executive Director, Jacksonville International Airport, Jacksonville Aviation Authority, testifying on behalf of the Airports Council International, North America.

On June 16, 2015, the subcommittee also held a hearing entitled, “How TSA Can Improve Aviation Worker Vetting,” and received testimony from John Roth, Inspector General, Department of Homeland Security; Stacey Fitzmaurice, Deputy Assistant Administrator, Office of Intelligence and Analysis, Transportation Security Administration, DHS; and Jennifer Grover, Director, Transportation Security and Coast Guard Issues, Homeland Security and Justice Team, Government Accountability Office.

On December 9, 2015, the Committee on Commerce, Science, and Transportation of the Senate met in open Executive Session to consider S. 2361, and ordered the bill to be reported to the Senate favorably, with a first degree amendment, by voice vote. The first degree amendment, sponsored by Senators Nelson, Blumenthal, and Booker, added language that would ensure there exists or is developed a waiver process for airport workers for denied SIDA credentials.

ESTIMATED COSTS

In accordance with paragraph 11(a) of rule XXVI of the Standing Rules of the Senate and section 403 of the Congressional Budget Act of 1974, the Committee provides the following cost estimate, prepared by the Congressional Budget Office:

S. 2361—Airport Security Enhancement and Oversight Act

S. 2361 would require the Administrator of the Transportation Security Administration (TSA) to undertake a variety of activities to improve the effectiveness of processes for screening, vetting, and credentialing personnel at airports, particularly individuals with access to secure areas. Such activities would include using risk-based models for screening airport employees based on the level of security of areas they access, reviewing procedures related to vetting employees and auditing airports’ issuance of credentials, studying opportunities to enhance security of entry and exit areas of secure areas of airports, and other security-related and administrative activities. The bill also would direct the agency to increase covert tests of security measures at secure areas of airports and require a variety of studies and reports.

According to TSA, many of the requirements specified in S. 2361 are largely consistent with current administrative policy. As a result, CBO estimates that any increased spending by TSA to meet the bill’s requirements would total less than \$500,000; any such spending would be subject to the availability of appropriated funds. According to TSA, some of the analyses and reports required by the bill could result in changes in policies that, if implemented, might affect the agency’s costs in future years. Any such effects would depend on the outcome of such analyses and are not reflected in this estimate.

Because enacting S. 2361 would not affect direct spending or revenues, pay-as-you-go procedures do not apply. CBO estimates that enacting S. 2361 would not increase net direct spending or on-

budget deficits in any of the four consecutive 10-year periods beginning in 2027.

S. 2361 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act.

S. 2361 contains provisions related to screening personnel at airports that are similar to provisions in other bills for which CBO has transmitted cost estimates. In all cases, our estimates of budgetary effects of such provisions are the same. In particular:

- On July 24, 2015, CBO transmitted a cost estimate for H.R. 2750, the Improved Security Vetting for Aviation Workers Act of 2015, as ordered reported by the House Committee on Homeland Security on June 25, 2015;
- On November 4, 2015, CBO transmitted a cost estimate for H.R. 3102, the Airport Access Control Security Improvement Act of 2015, as passed by the House of Representatives on October 6, 2015; and,
- On November 4, 2015, CBO transmitted a cost estimate for H.R. 3584, the Transportation Security Administration Reform and Improvement Act of 2015, as ordered reported by the House Committee on Homeland Security on September 30, 2015.

The CBO staff contact for this estimate is Megan Carroll. The estimate was approved by H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.

REGULATORY IMPACT

In accordance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee provides the following evaluation of the regulatory impact of the legislation, as reported:

NUMBER OF PERSONS COVERED

The bill would cover foreign and domestic air carriers and the approximately 440 U.S. airports which are currently subject to TSA rules and regulations on SIDA access control. The bill would also cover the tens of thousands of SIDA badge holders that currently work at U.S. airports, as well as an even greater number of total future SIDA badge applicants.

ECONOMIC IMPACT

The bill would not authorize new spending by the Federal Government. Under the bill, the TSA Administrator would be required to conduct two rulemakings subject to notice and comment, which would update existing rules and regulations to which airport operators and airlines are already subject. Depending on the outcome of the TSA's rulemaking updates, airport operators may be required to pay increased fines and undergo additional audits if they report certain percentages of missing SIDA badges. They also may be encouraged by the TSA to issue temporary SIDA badges to airport workers under limited circumstances. Airport operators may also be required develop a waiver process for denied SIDA credentials if one does not already exist. In addition, under a rule of construction in the bill, the rulemaking update related to vetting cannot be construed to affect existing airport worker vetting fees imposed by the TSA. Finally, the requirement to streamline security directives

under the bill may result in economic efficiencies to airport operators and air carriers.

PRIVACY

The bill would impact the personal privacy of individuals who apply to receive and who already possess SIDA badges for unescorted access to secure areas of airports. Specifically, the bill would require the TSA Administrator to enhance the criminal history background checks that SIDA badge applicants must already undergo as part of the vetting process. The bill also would subject SIDA badge applicants to additional checks against terrorism and immigration status databases, and would require all SIDA badge holders to undergo recurrent criminal history background checks. The bill would subject SIDA badge holders to expanded use of random physical inspections and covert testing, which are existing practices.

PAPERWORK

The bill would not significantly increase paperwork requirements for private individuals or businesses. The enhanced regulatory requirements under the bill for oversight of missing airport SIDA badges would be enforced using information gained from existing audits and reporting procedures. Additionally, the TSA would be required to track and keep records on multiple years of airport audit data related to missing SIDA badges for oversight purposes. The updated vetting requirements under the bill would be implemented using existing background check, certification, and waiver processes. The bill also would require the Federal Government to produce eight reports (one of which is an annual report), one regular update to Congress, and a notification to Congress triggered by certain occurrences.

CONGRESSIONALLY DIRECTED SPENDING

In compliance with paragraph 4(b) of rule XLIV of the Standing Rules of the Senate, the Committee provides that no provisions contained in the bill, as reported, meet the definition of congressionally directed spending items under the rule.

SECTION-BY-SECTION ANALYSIS

Section 1. Short title.

This section would designate the short title of the bill as the, “Airport Security Enhancement and Oversight Act.”

Section 2. Findings.

This section would state findings of the Committee’s oversight efforts in the last year regarding recent lapses in security at domestic airports, including improper use of SIDA badges by airport and airline workers and a group of contractors indicted for participating in a drug smuggling ring. The findings also would highlight a DHS OIG report finding that the TSA did not identify 73 airport workers with potential links to terrorism due to gaps in current interagency watchlisting policy. Noted also in this section would be the finding that the TSA does not maintain a list of lost or missing SIDA

badges, and that it rarely uses its enforcement authority to fine airports that reach a certain threshold of missing SIDA badges.

Section 3. Definitions.

This section would provide relevant definitions of terms used in the legislation.

Section 4. Threat assessment.

This section would instruct the TSA Administrator to update an assessment to determine the level of risk posed to airport security by workers with access to secure areas of domestic airports in light of recent terrorist activity. Factors for the TSA Administrator to consider would include domestic and international intelligence, the recent security breaches at domestic and international airports, and the recent security improvements at domestic airports, including the implementation of recommendations made by the ASAC. This section also would require the TSA Administrator to report to Congress the results of this assessment, as well as a report on the implementation status of recent recommendations made by the ASAC to the TSA. Finally, the TSA Administrator also would be required to report to Congress with regular updates about the threat environment as new information becomes available and as needed.

Section 5. Oversight.

This section would require the TSA Administrator to update, in consultation with airport operators, the rules on unescorted airport access controls issued by the Secretary of Homeland Security. In updating these rules, the TSA Administrator would have to consider increased fines and oversight for airport operators that report missing more than five percent of credentials for unescorted access to any SIDA of an airport, and best practices for Category X airports (the largest airports) that report missing three percent of credentials to any SIDA of an airport. The TSA Administrator also would be required to consider additional audits and status checks for airport operators that report missing more than three percent of credentials, as well as a review and analysis of the prior five years of audits for those same airport operators to improve accountability by airports and badge holders alike. The Committee does not intend for the TSA Administrator to retroactively request five years' worth of audit data from airports upon the date of enactment; instead, the Committee expects the TSA Administrator to implement this review and analysis requirement as soon as the data can be practically collected through existing airport audit procedures, and to build the database going forward. Finally, in updating these rules, the TSA Administrator would be required to consider increased fines and direct enforcement requirements for airport workers and their employers that fail to report within 24 hours an employment termination or a missing credential, and termination of any airport worker that fails to report in a timely manner missing credentials.

This section also would allow the TSA Administrator to encourage the issuance of free, one-time, 24-hour temporary credentials for workers who have reported their credentials missing but not permanently lost, stolen, or destroyed, in a timely manner, much

like a hold on a credit card, until the badge is found and reactivated or the replacement of the credential is necessary. This section also would require the TSA Administrator to report to Congress each time an airport operator reports missing more than three percent of credentials at Category X airports and more than five percent of credentials at all other airports, and to submit an annual report on the number of violations and fines related to unescorted access authority to the SIDA of an airport collected in the preceding fiscal year.

Section 6. Credentials.

This section would require the TSA Administrator to issue guidance to airport operators requiring that they place an expiration date on each airport credential issued to a non-United States citizen commensurate with the period of time during which that non-United States citizen is lawfully authorized to work in the United States. In addition, the TSA Administrator would have to issue guidance for transportation security inspectors to annually review the procedures of airport operators for applicants seeking unescorted access authority to any SIDA of airports. This guidance should include a review of background check and employment authorization documents.

Section 7. Vetting.

This section would require the TSA Administrator to update and enhance, through a notice and comment rulemaking, the eligibility requirements and disqualifying criminal offenses for individuals seeking or having unescorted access to a SIDA of an airport. In revising these regulations, the TSA Administrator would have to consider adding to the list of disqualifying criminal offenses the offenses and criteria used by CBP and those used for the Transportation Worker Identification Credential (known as TWIC) for access to secure areas, with the goal of streamlining and making consistent similar airport worker requirements, where appropriate. This section also would require the TSA Administrator to propose in the Notice of Proposed Rulemaking an extension of the look-back period for disqualifying criminal offenses and other disqualifying criteria from 10 to 15 years before the date of an individual's application. The rulemaking also would require an airport or aircraft operator to certify that there is a specific need and that the individual understands the requirements for possessing a SIDA badge for each individual who receives unescorted access authority.

This section would require the TSA Administrator to ensure that there exists or is developed a waiver process for approving the issuance of credentials for SIDA access for individuals who are denied a credential due to a criminal history background check. As part of the rulemaking update, the Committee expects the TSA Administrator to carefully weigh the costs and administrative burdens associated with this requirement. Consideration should be given to airport community preferences to retain control of the waiver process and employee group concerns about the lack of a centralized system. The Committee does not intend to create a significant financial burden associated with the development of such a waiver process at airports where one does not currently exist.

In addition, this section would require the TSA Administrator and the Director of the FBI to fully implement the Rap Back service for recurrent vetting of individuals with SIDA badges. As part of this program, the TSA Administrator would be required to ensure that the TSA only receives status notifications through the Rap Back service about disqualifying criminal offenses in accordance with regulations, and that any information received by the TSA through the Rap Back service is provided directly and immediately to the relevant airport and aircraft operators. The Secretary of Homeland Security also would be required to authorize the TSA Administrator to receive automated, real-time access to additional TIDE data and to authorize each airport operator to have direct access to the E-Verify program and the SAVE automated system to determine the eligibility based on immigration status of individuals seeking unescorted access authority to a SIDA of an airport.

Section 8. Metrics.

This section would require the TSA Administrator to develop and implement performance metrics to measure the effectiveness of security for secured areas of airports. The TSA Administrator may consider such factors as adherence to access point procedures, proper use of credentials, differences in access point characteristics across the national airport system, and other factors in developing these metrics. A report by the Comptroller General on the impact of the new performance metrics implemented in this section would be due to Congress two years after the date of enactment.

Section 9. Inspections and assessments.

This section would instruct the TSA Administrator, in consultation with ASAC, to develop best practices for unescorted access security that use intelligence, scientific algorithms, and risk-based factors, ensure integrity and accountability, subject airport workers to random physical security inspections, and appropriately manage the number of SIDA access points to reduce unauthorized access to these areas. This section also would require the TSA Administrator to expand the use of transportation security officers and inspectors to conduct enhanced, random, and unpredictable physical inspections of airport workers in each SIDA of an airport and at each SIDA access point. These inspections would be designed to verify the credentials of airport workers, determine whether airport workers possess prohibited items, and to verify whether airport workers are following appropriate procedures to access that SIDA of an airport. The Committee intends for this provision to be consistent with the TSA's increase in SIDA inspections under existing Playbook operations, and intends not to put a significant resource burden on the TSA to conduct all random physical inspections at airports, an effort which shall remain primarily the responsibility of airport operators. Additionally, this section would require the TSA Administrator to conduct a review of airports that have implemented comprehensive or additional employee screening or perimeter security to improve airport security and, upon completion of the review, to identify best practices for additional access control and employee security at airports and to disseminate the best practices identified to airport operators. The TSA Administrator also would be authorized in this section to conduct a pilot program at

one or more airports to test and validate the identified best practices, as appropriate.

Section 10. Covert testing.

This section would instruct the TSA Administrator to increase the use of red-team, covert testing of access controls to any secure area of an airport, and instructs the DHS OIG to conduct red-team covert testing of airport access controls to the SIDA of airports. This section would require the TSA Administrator to submit a report on the progress in expanding the use of red-team, covert testing to Congress 90 days after enactment, and the DHS OIG to submit a report on the effectiveness of airport access controls to the SIDA of airports 180 days after enactment.

Section 11. Security directives.

This section would require the TSA Administrator to begin, and then annually conduct, in consultation with the appropriate regulated entities, a comprehensive review of every current security directive addressed to any regulated entity. This review would be designed to determine whether the security directives continue to be relevant, whether the security directives should be streamlined or consolidated to most efficiently maximize risk reduction, and to update, consolidate, or revoke any security directive as necessary. Going forward, the TSA Administrator would have to notify Congress about the extent to which each security directive issued responds to a specific threat or emergency situation, and when it is anticipated that it will expire. The Committee understands that the TSA must be able to act quickly to effectively respond to security threats and situations. Therefore, the Committee does not intend to impose on the TSA a new standard for issuing security directives; it merely intends to create a new requirement for notice to Congress.

Section 12. Implementation report.

This section would require the Comptroller General to submit a report to Congress that assesses the progress made by the TSA in implementing the oversight, credentialing, vetting, and inspection requirements under this Act. The report would be due one year after enactment.

Section 13. Miscellaneous amendments.

This section would include a technical amendment extending the term of a member of ASAC beyond two years if the TSA Administrator does not appoint a successor. Additionally, it would include an amendment which requires the TSA Administrator to respond with feedback each time the TSA receives a recommendation from ASAC. The feedback also would be required to include an action plan to implement any of the recommendations with which the TSA Administrator concurs or a justification for why any of the recommendations have been rejected. This feedback would be due 90 days after the TSA Administrator receives the recommendations transmitted by ASAC.

CHANGES IN EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new material is printed in italic, existing law in which no change is proposed is shown in roman):

TITLE 49. TRANSPORTATION

SUBTITLE VII. AVIATION PROGRAMS

PART A. AIR COMMERCE AND SAFETY

SUBPART III. SAFETY

CHAPTER 449. SECURITY

SUBCHAPTER II. ADMINISTRATION AND PERSONNEL

§ 44946. Aviation Security Advisory Committee

(a) ESTABLISHMENT.—The Assistant Secretary shall establish within the Transportation Security Administration an aviation security advisory committee.

(b) DUTIES.—

(1) IN GENERAL.—The Assistant Secretary shall consult the Advisory Committee, as appropriate, on aviation security matters, including on the development, refinement, and implementation of policies, programs, rulemaking, and security directives pertaining to aviation security, while adhering to sensitive security guidelines.

(2) RECOMMENDATIONS.—

(A) IN GENERAL.—The Advisory Committee shall develop, at the request of the Assistant Secretary, recommendations for improvements to aviation security.

(B) RECOMMENDATIONS OF SUBCOMMITTEES.—Recommendations agreed upon by the subcommittees established under this section shall be approved by the Advisory Committee before transmission to the Assistant Secretary.

(3) PERIODIC REPORTS.—The Advisory Committee shall periodically submit to the Assistant Secretary—

(A) reports on matters identified by the Assistant Secretary; and

(B) reports on other matters identified by a majority of the members of the Advisory Committee.

(4) ANNUAL REPORT.—The Advisory Committee shall submit to the Assistant Secretary an annual report providing information on the activities, findings, and recommendations of the Advisory Committee, including its subcommittees, for the preceding year. Not later than 6 months after the date that the Secretary receives the annual report, the Secretary shall publish a public version describing the Advisory Committee's activities and such related matters as would be informative to the public consistent with the policy of section 552(b) of title 5.

[(5) FEEDBACK.—Not later than 90 days after receiving recommendations transmitted by the Advisory Committee under paragraph (4), the Assistant Secretary shall respond in writing

to the Advisory Committee with feedback on each of the recommendations, an action plan to implement any of the recommendations with which the Assistant Secretary concurs, and a justification for why any of the recommendations have been rejected.】

(5) *FEEDBACK.*—*Not later than 90 days after receiving recommendations transmitted by the Advisory Committee under paragraph (2) or paragraph (4), the Assistant Secretary shall respond in writing to the Advisory Committee with feedback on each of the recommendations, an action plan to implement any of the recommendations with which the Assistant Secretary concurs, and a justification for why any of the recommendations have been rejected.*

(6) *CONGRESSIONAL NOTIFICATION.*—*Not later than 30 days after providing written feedback to the Advisory Committee under paragraph (5), the Assistant Secretary shall notify the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives on such feedback, and provide a briefing upon request.*

(7) *REPORT TO CONGRESS.*—*Prior to briefing the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives under paragraph (6), the Assistant Secretary shall submit to such committees a report containing information relating to the recommendations transmitted by the Advisory Committee in accordance with paragraph (4).*

(c) *MEMBERSHIP.*—

(1) *APPOINTMENT.*—

(A) *IN GENERAL.*—*Not later than 180 days after the date of enactment of the Aviation Security Stakeholder Participation Act of 2014, the Assistant Secretary shall appoint the members of the Advisory Committee.*

(B) *COMPOSITION.*—*The membership of the Advisory Committee shall consist of individuals representing not more than 34 member organizations. Each organization shall be represented by 1 individual (or the individual’s designee).*

(C) *REPRESENTATION.*—*The membership of the Advisory Committee shall include representatives of air carriers, all-cargo air transportation, indirect air carriers, labor organizations representing air carrier employees, labor organizations representing transportation security officers, aircraft manufacturers, airport operators, airport construction and maintenance contractors, labor organizations representing employees of airport construction and maintenance contractors, general aviation, privacy organizations, the travel industry, airport-based businesses (including minority-owned small businesses), businesses that conduct security screening operations at airports, aeronautical repair stations, passenger advocacy groups, the aviation security technology industry (including screening technology and biometrics), victims of terrorist acts against aviation, and law enforcement and security experts.*

(2) *TERM OF OFFICE.*—

[(A) TERMS.—The term of each member of the Advisory Committee shall be 2 years. A member of the Advisory Committee may be reappointed.]

(A) TERMS.—*The term of each member of the Advisory Committee shall be 2 years, but a member may continue to serve until the Assistant Secretary appoints a successor. A member of the Advisory Committee may be reappointed.*

(B) REMOVAL.—The Assistant Secretary may review the participation of a member of the Advisory Committee and remove such member for cause at any time.

(3) PROHIBITION ON COMPENSATION.—The members of the Advisory Committee shall not receive pay, allowances, or benefits from the Government by reason of their service on the Advisory Committee.

(4) MEETINGS.—

(A) IN GENERAL.—The Assistant Secretary shall require the Advisory Committee to meet at least semiannually and may convene additional meetings as necessary.

(B) PUBLIC MEETINGS.—At least 1 of the meetings described in subparagraph (A) shall be open to the public.

(C) ATTENDANCE.—The Advisory Committee shall maintain a record of the persons present at each meeting.

(5) MEMBER ACCESS TO SENSITIVE SECURITY INFORMATION.—Not later than 60 days after the date of a member’s appointment, the Assistant Secretary shall determine if there is cause for the member to be restricted from possessing sensitive security information. Without such cause, and upon the member voluntarily signing a non-disclosure agreement, the member may be granted access to sensitive security information that is relevant to the member’s advisory duties. The member shall protect the sensitive security information in accordance with part 1520 of title 49, Code of Federal Regulations.

(6) CHAIRPERSON.—A stakeholder representative on the Advisory Committee who is elected by the appointed membership of the Advisory Committee shall chair the Advisory Committee.

* * * * *