



AGENDA STAFF REPORT

ASR Control 24-000810

**MEETING DATE:** 12/17/24  
**LEGAL ENTITY TAKING ACTION:** Board of Supervisors  
**BOARD OF SUPERVISORS DISTRICT(S):** 5  
**SUBMITTING AGENCY/DEPARTMENT:** John Wayne Airport (Approved)  
**DEPARTMENT CONTACT PERSON(S):** Charlene Reynolds (949) 252-5183  
 Richard Steele (949) 252-5264

**SUBJECT:** Approve Amendment Number One for Armed Security Guard Services

<b>CEO CONCUR</b> Concur	<b>COUNTY COUNSEL REVIEW</b> Approved Agreement to Form	<b>CLERK OF THE BOARD</b> Discussion 3 Votes Board Majority
-----------------------------	--	---

**Budgeted:** Yes                      **Current Year Cost:** \$1,614,766                      **Annual Cost:**  
 FY 2025-26 \$3,987,016  
 FY 2026-27 \$2,416,882

**Staffing Impact:** No                      **# of Positions:**                      **Sole Source:** No  
**Current Fiscal Year Revenue:** N/A  
**Funding Source:** Fund 280: 100%                      **County Audit in last 3 years:** No  
**Levine Act Review Completed:** Yes  
**Prior Board Action:** 12/14/2021 #27

**RECOMMENDED ACTION(S):**

1. Authorize the County Procurement Officer or Deputized designee to execute Amendment Number One to the Subordinate Contract with Universal Protection Service, LP dba Allied Universal Security Services for Armed Security Guard Services, effective February 1, 2025, through January 31, 2027, in an amount not to exceed \$8,018,664.
2. Pursuant to Contract Policy Manual Section 3.3-113, authorize the County Procurement Officer or Deputized designee to exercise a contingency contract increase, not to exceed a total of 10 percent of the Contract amount for the first year of the Contract, for the entire term of the Contract, including renewals, and within the scope of work set forth in the Contract. The use of this contingency contract increase is subject to approval requirements established by the County Procurement Officer.

**SUMMARY:**

Approval of the subordinate contract with Universal Protection Service, LP dba Allied Universal Security Services will fulfill a critical security function by providing continued private security guard services at John Wayne Airport.

**BACKGROUND INFORMATION:**

On December 14, 2021, the Board of Supervisors (Board) approved and executed Subordinate Contract MA-280-22010553 with Universal Protection Service, LP dba Allied Universal Security Services (AUS), effective February 1, 2022, through January 31, 2025, in an amount not to exceed \$8,618,267, with the option to renew for one additional two-year term.

AUS provides services necessary to meet Title 49 CFR 1542 Airport Security Regulations related to the enforcement of airport access control procedure, applicable elements of the Airport Security Plan, Department of Homeland Security (DHS)/Transportation Security Administration security directives; vehicle traffic management; escorting; assisting airport tenants, authorized visitors, and guests; and administrative requirements. Assignments include: seven posts that provide departure and arrival level curbside traffic management for all terminals (18 hours a day/seven days per week), one air cargo vehicle access post (eight hours a day/five days per week), three airfield vehicle access posts (24 hours a day/seven days per week), one post that monitors the Terminal C Sterile Area exit stairway and escalator (18 hours/seven days per week), one post that conducts concession product inspection prior to entry into the terminal sterile area (16 hours/seven days per week), one shift supervisor (24 hours/seven days per week) for airfield security posts, and one shift supervisor (18 hours/seven days per week) for terminal and curbside traffic posts. One Account Manager (40 hours/seven hours per week) and one Post Commander (8 hours/five days per week) are assigned to effectively manage logistics, training, hiring, coaching, counseling, terminations and administrative functions related to the private security workforce covering over 8,000 monthly staffing hours at John Wayne Airport (JWA).

AUS is also the only private security company that maintains a DHS Safety Act Certification, which would provide liability protections to JWA in the event of a terrorist attack.

Performance Metrics

The following metrics have been implemented to assess AUS’s performance:

<b>Goals</b>	<b>FY 22/23 Actual</b>	<b>FY23/24 Actual</b>
Staff 13 security posts with qualified, trained personnel 100% of the time to meet Title 49 CFR 1542 – Airport Security regulatory requirements	100%	100% (Average # of hours: 7,732)
Staff additional security posts and provide escort to support construction projects	100%	100% (Total # of hours: 20)
April 2023: Develop, train security officers, and implement a random employee screening (“Aviation Worker Screening”) Program to meet TSA Security Directive deadline of September 2023	N/A	Amendment One to AUS contract Program implemented before TSA required deadline
Conduct Aviation Worker Screening and report prohibited items when discovered to TSA and Orange County Sheriff’s Department personnel	N/A	Total Employees Screened: 8,924 Total Prohibited Items Reported: 5
Maintain DHS Safety Act Certification Rating (80 percent minimum to pass)	99%	99%
Report security incidents to the Orange County Sheriff’s Department – Airport Police Services	10	15

JWA is seeking to renew the contract with AUS for an additional two years, in an amount not to exceed \$8,018,664. This is an annual increase of \$1,136,576 compared to years one, two, and three. The reason for this annual cost increase is due to the following:

1. In April 2023, a TSA Security Amendment was published requiring all regulated airports to establish phase one of a program to randomly screen aviation workers, the “Aviation Worker Screening (AWS) Program” entering the Terminal Sterile Area before September 25, 2023. JWA was able to meet this regulatory deadline before the effective date due to AUS’ ability to hire, train, and support the additional security requirement. Phase two of this TSA Security Amendment will require additional responsibilities before April 2026. Two positions would be added. A female and male security officer are assigned to each AWS deployment.
2. On January 1, 2024, California Assembly Bill 1522 (AB 1522) enacted the “Healthy Workplaces, Healthy Families Act of 2014,” which requires employers to provide paid sick leave to employees. The implementation of this law has prompted an increase in sick leave requests, which in turn, contributes to AUS being below minimum staffing and several security officers not being relieved for breaks and lunches to comply with the California meal and rest break law. Two positions would be added to cover breaks and lunches.
3. The increased construction activity due to terminal tenant improvement projects and capital improvement projects has generated the need to enforce traffic Orange County Code of Ordinances (OCCO) and Airport Security Plan regulations. Vehicle drivers are regularly stopping in emergency lanes and drive lanes, and leaving unauthorized vehicles unattended prior to the first traffic signal on the lower level (Arrivals) curbsides. One position would be added seven days per week during peak traffic times to manage these areas.
4. The increased construction activity has also increased after-hours escort and security gate monitoring requests.
5. Promoting the Site Supervisor to an Assistant Account Manager position is necessary to accomplish the following:
  - Respond to private security complaints and emergency incidents, liaison with Airport Operations and Sheriff’s Department personnel, and generate daily TSA required reports seven days per week, 8:00 AM to 11:30 PM. Current manager coverage is Monday through Friday only, 8:00 AM to 5:00 PM.
  - Promptly coordinate late construction project escort and access requests.
  - Provide overtime authorization.
6. Allow AUS to replace an existing pickup truck (\$1,200 monthly) with a vehicle that has more seating capacity (\$1,500 monthly) to transport more security personnel between security posts and parking locations.

Prior to contract expiration, JWA will participate in the solicitation of a new Regional Cooperative Agreement (RCA) for Security Guard Services before the expiration date of September 30, 2026. JWA will then award a new Subordinate Contract prior to this amendment's expiration date, January 31, 2027.

JWA requests that the Board authorize, pursuant to Contract Policy Manual Section 3.3-114, the County Procurement Officer or Deputized designee to exercise a contingency contract cost increase in an amount not to exceed 10 percent of the contract amount for the first year of the contract, for the entire term of the

contract, including renewals, and within the scope of work set forth in the contract. The use of this contingency contract cost increase is subject to approval requirements established by the County Procurement Officer.

The Contractor's performance has been confirmed satisfactory. JWA has verified there are no concerns that must be addressed with respect to the Contractor's ownership/name, litigation status or conflicts with County interests.

The Orange County Preference Policy (OCPP) was applicable and incorporated into this RCA. There was one OCPP qualified proposal submitted into this solicitation, High Level Security Solutions, Inc. and based on the final scoring, a contract was awarded to this OCPP qualified vendor, receiving an eight percent point advantage as a qualified Disabled Veteran Business Enterprise/Orange County Local Small Business.

The Contract does not currently include subcontractors or pass through to other providers. See Attachment C for the Contract Summary Form.

**Compliance with CEQA:** This action is not a project within the meaning of the California Environmental Quality Act (CEQA) Guidelines Section 15378 and is therefore not subject to CEQA, since it does not have the potential for resulting in either a direct physical change in the environment; or a reasonably foreseeable indirect physical change in the environment. The approval of this agenda item does not commit the County to a definite course of action in regard to a project since it is an amendment to a contract for security protection services. This proposed activity is therefore not subject to CEQA. Any future action connected to this approval that constitutes a project will be reviewed for compliance with CEQA.

**FINANCIAL IMPACT:**

Appropriations for this Contract are included in Fund 280, Airport Operating Fund, FY 2024-25 Budget and will be included in the budgeting process for future years.

The Contract referenced in this agenda item contains language that permits reductions or termination of the Contract immediately and without penalty if approved funding or appropriations are not forthcoming.

**STAFFING IMPACT:**

N/A

**ATTACHMENT(S):**

Attachment A – Amendment Number One to Subordinate Contract MA-280-22010553 with Universal Protection Service, LP dba Allied Universal Security Services

Attachment B – Contract Summary Form

Attachment C – Title 49 Code of Federal Regulations Part 1542 - Airport Security and the Airport Security Plan

Attachment D – California Assembly Bill 1522 (AB 1522)





**AMENDMENT NUMBER ONE  
FOR  
ARMED SECURITY GUARD SERVICES**

This Amendment is made and entered into as of the date fully executed by and between the County of Orange, a political subdivision of the State of California, through its department John Wayne Airport (“County” or “JWA”) and Universal Protection Service, LP DBA Allied Universal Security Services (“Contractor”), with County and Contractor sometimes individually referred to as “Party” or collectively referred to as “Parties.”

**RECITALS**

**WHEREAS**, the County acting through the County Procurement Office, (“CPO”) issued a Regional Cooperative Agreement RCA-017-22010008, for Armed Security Guard Services (“RCA”), effective October 1, 2021 through September 30, 2026 (“Master Contract”); and,

**WHEREAS**, the Parties entered into Subordinate Contract MA-280-22010553 for Armed Security Guard Services, in accordance with the terms, conditions and pricing of the Master Contract, effective February 1, 2022, through January 31, 2025, for a Total Contract Amount Not to Exceed \$8,618,266.82 (“Contract”); and,

**WHEREAS**, pursuant to Amendment One of the Master Contract, the Compensation and Pricing was updated to reflect Armed Security Guard Holiday Rate; and,

**WHEREAS**, pursuant to Amendment Two of the Master Contract, Attachment B: Pricing and Compensation was replaced in its entirety with revised rates; and,

**WHEREAS**, the Parties now desire to renew the Subordinate Contract for two additional (2) years effective February 1, 2025 through January 31, 2027 in accordance with the terms, conditions and amendments of the Master Contract, for a renewed Total Contract Amount Not to Exceed \$8,018,663.23 replace Attachment C and Attachment D in its entirety as attached hereto, amend Holiday and Overtime pay; and update County’s Notice requirements and,

**NOW, THEREFORE**, the Parties mutually agree as follows:

**AMENDMENT TO CONTRACT ARTICLES**

1. Section 2 of the Contract’s Additional Terms and Conditions shall be amended to read in its entirety as follows:
  2. **Term of Subordinate Contract:** The renewal term of this Contract shall become effective February 1, 2025 and shall continue for two (2) years, unless otherwise as terminated as provided herein. This Contract may be renewed as set forth in paragraph 3 below.
2. Section 3 of the Contract’s Additional Terms and Conditions shall be amended to read in its entirety as follows:
  3. **Renewal:** Reserved.
3. Section 4 of the Contract’s Additional Terms and Conditions shall be amended to read in its entirety as follows:



- 4. Compensation & Payment:** Contractor agrees to provide Armed Security Guard Services in accordance with the terms and conditions of the Master Contract and its amendments, including its attachments, at the fixed rates as set forth in Attachment B – Compensation and Pricing with a Total Contract Amount of \$8,018,663.23.

Contract Amount for Year 4 shall not exceed: \$3,875,438.08

Contract Amount for Year 5 shall not exceed: \$4,143,225.15

4. Section 10 of the Contract’s Additional Terms and Conditions shall be amended in its entirety as follows:

- 10. Notices:** Any and all notices, requests demands and other communications contemplated, called for, permitted, or required to be given hereunder shall be in writing with a copy provided to the assigned Deputy Purchasing Agent (DPA), except through the course of the parties’ project managers’ routine exchange of information and cooperation during the terms of the work and services. Any written communications shall be deemed to have been duly given upon actual in-person delivery, if delivery is by direct hand, or upon delivery on the actual day of receipt or no greater than four (4) calendar days after being mailed by US certified or registered mail, return receipt requested, postage prepaid, whichever occurs first. The date of mailing shall count as the first day. All communications shall be addressed to the appropriate party at the address stated herein or such other address as the parties hereto may designate by written notice from time to time in the manner aforesaid.

Contractor: Universal Protection Service, LP,  
 DBA Allied Universal Security Services  
 Attn: Steve Nsaif, Project Manager  
 1551 N. Tustin Ave., Suite #650  
 Santa Ana, CA 92705  
 Phone: 714-231-5872  
 Email: [steve.nsaif@aus.com](mailto:steve.nsaif@aus.com)

County’s Project Manager:

JWA/Operations Administration  
 Attn: Richard Givens, Project Manager  
 18601 Airport Way  
 Santa Ana, CA 92707  
 Phone: 949-252-5151  
 Email: [rgivens@ocair.com](mailto:rgivens@ocair.com)

cc: JWA/Procurement  
 Attn: Gina Lozares, County DPA  
 3160 Airway Avenue  
 Costa Mesa, CA 92626  
 Phone: (949) 252-5175  
 Email: [glozares@ocair.com](mailto:glozares@ocair.com)

5. Attachment B, Section III. Holidays and Overtime shall be amended in its entirety as follows:

**III. HOLIDAYS AND OVERTIME**



- A. Overtime: Overtime is defined as the hourly rate paid to Contractor personnel performing services over forty (40) hours per week or eight (8) hours per workday. Overtime rates will only be paid with prior approval by JWA.
- B. Overtime shall be reimbursed in accordance with the State of California at the rate of:
- One and one-half times the employee's regular rate of pay for all hours worked in excess of eight hours up to and including 12 hours in any workday, and for the first eight hours worked on the seventh consecutive day of work in a workweek; and,
  - Double the employee's regular rate of pay for all hours in excess of 12 hours in any workday and for all hours worked in excess of eight on the seventh consecutive day of work in a workweek.
- C. Holiday Pay: JWA authorizes holiday pay on six (6) Contractor observed holidays. Contractor observed holidays include New Year's Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day and Christmas Day. Holiday rates shall be calculated at time and a half.
6. Attachment C, Staffing Plan and Hours shall be amended in its entirety as attached hereto.
7. Attachment D, JWA Specific Equipment, Information, And Uniforms shall be amended in its entirety as attached hereto.
8. All other terms and conditions in this of the Contract, except as specifically amended herein, shall remain unchanged and with full force and effect.





**ATTACHMENT C  
STAFFING PLAN AND HOURS**

The substitution or addition of other key individuals, in any given category or classification, shall be allowed only with prior written approval of County Project Manager or designee.

County, at its option, may adjust the schedule at any given location at any time during the term of the Contract upon written notice to Contractor.

Charges will be adjusted, as necessary, based on the hourly rates stated in the Master Contract.

\* All positions listed below shall be Standard Officer & SIDA Cleared.

<b>Positions/Security Posts*</b>	<b>Approximate Daily Work Hours</b>	<b>Work Days</b>
On-Site Account Manager	Minimum of 8 hours per day	Monday to Friday, on call for emergency incidents
Asst, Account Manager	Minimum of 8 hours per day Swing (1430-2300)	Tuesday to Saturday On Call for Emergencies
Unarmed Supervisor - Airfield (Day, Swing, & Graveyard Shifts)	24 hours	7 days per week
Unarmed Supervisor - Terminal (Day & Swing Shifts)	18 hours	7 days per week
Unarmed Guard - Vehicle Access Post #1	24 hours	7 days per week
Unarmed Guard - Vehicle Access Post #2	24 hours	7 days per week
Unarmed Guard - Vehicle Access Post #3	24 hours	7 days per week
Unarmed Guard - Vehicle Access Post #4 (Air Cargo)	8 hours	Monday - Friday
Unarmed Guard - Terminal C Exit Post	18 hours	7 days per week
Unarmed Guard - Concession Product Delivery Post	16 hours	7 days per week
Unarmed Guard - Terminal A Departure Curbside Traffic	18 hours	7 days per week
Unarmed Guard - Terminal A Arrival Curbside Traffic	16 hours	7 days per week
Unarmed Guard - Terminal B Departure Unarmed Curbside Traffic	18 hours	7 days per week
Unarmed Guard - Terminal B Arrival Curbside Traffic	16 hours	7 days per week
Unarmed Guard - Terminal C Departure Curbside Traffic	18 hours	7 days per week
Unarmed Guard - Terminal C Arrival Curbside Traffic	16 hours	7 days per week
Unarmed Guard – Curbside Traffic Relief	16 hours	7 days per week
Guard – Additional Hours and other ‘as-needed’ Security Posts determined by TSA	As needed and preapproved by JWA	As needed and preapproved by JWA
Unarmed Arrival Officers (Prior to A-1)	8 Hours	7 Days Per Week



*County of Orange, John Wayne Airport*

Attachment A

*MA-280-22010553*

*Armed Security Guard Services*

---

Two (2) Unarmed Breaker	32 Hours	7 Days Per Week
Aviation Worker Screening Officer	Varies Daily	Random-30 to 40 Hours per week



**ATTACHMENT D  
JWA SPECIFIC EQUIPMENT, INFORMATION, AND UNIFORMS**

Contractor shall provide JWA assigned security personnel with the following equipment/items.

Note: the below list is to clarify, not add, items specific to JWA.

Only Contractor issued outer garments maybe worn while personnel are at their assigned post, i.e. coats, sweaters, safety vests, rain gear, etc.

Positions/Security Posts	Equipment/Items Provided by JWA	Equipment/Items Provided by Contractor
On-Site Account Manager	-Office space -Phone and computer port -800 MHZ Radio and accessories -Original Post Orders, amendments, and training documents (1) Explosive Detection System Equipment (EDSE) device with accessories	-VOIP Phone -Desktop PC -Desk -Chair -Mobile device and related accessories** -Emergency kit/first aid kit -Uniform -PPE -Reflective safety vest with "Security" printing on the back -Rain Gear
Supervisors	-Office space for shared desk -Phone and computer port -800 MHZ Radio and accessories (one issued to the Airfield Supervisor and one issued to the Terminal Supervisor)	-Vehicle* -VOIP Phone -Desktop PC -Desk -Chair -Mobile device and related accessories** -Emergency kit/first aid kit -Uniform -PPE -Rain Gear -Reflective safety vest with "Security" printing on the back -Post Orders, amendments, and training documents
Guard - Vehicle Access Post #1	-Guard Shack -Chair -VOIP Phone -800 MHZ Radio and accessories (one radio per post)	-Mobile device and related accessories**
Guard - Vehicle Access Post #2		-Emergency kit/first aid kit
Guard - Vehicle Access Post #3		-Uniform
Guard - Vehicle Access Post #4 (Air Cargo)		-PPE
		-Rain Gear
		-Reflective safety vest with "Security" printing on the back
		-Post Orders, amendments, and training documents
<b>Positions/Security Posts</b>	<b>Equipment/Items Provided by JWA</b>	<b>Equipment Provided By Contractor</b>



Guard - Terminal C Exit Post	-Podium -Chair -VOIP Phone -800 MHZ Radio and accessories	-Mobile device and related accessories** -Emergency kit/first aid kit -Uniform -PPE -Reflective safety vest with "Security" printing on the back -Post Orders, amendments, and training documents
Guard - Concession Product Delivery Post		-Cell Phone/mobile device and related accessories*** -Emergency kit/first aid kit -Uniform -PPE -Post Orders, amendments, and training documents
Guard - Terminal A Departure Curbside Traffic	-Podium at each post -Chair at each post -800 MHZ Radio and accessories at each post -Suitable space for employees to eat meals.	-Cell Phones/mobile devices and related accessories at each position*** -Emergency kits/first aid kits at each position -Traffic Marshaling Wands -Uniform -PPE -Post Orders, amendments, and training documents
Guard - Terminal A Arrival Curbside Traffic		
Guard - Terminal B Departure Curbside Traffic		
Guard - Terminal B Arrival Curbside Traffic		
Guard - Terminal C Departure Curbside Traffic		
Guard - Terminal C Arrival Curbside Traffic		
Guard – Curbside Traffic Relief		
Guard – Additional Hours and other 'as-needed' Security Posts determined by TSA	As needed and preapproved by JWA	As needed and preapproved by JWA

\*Vehicle: One (1) small SUV for transportation between various security posts and is authorized at the rates set forth in Attachment B – Compensation and Pricing of RCA-017-22010008.

\*\*Mobile Devices: Security Guards and Supervisors must be able to complete Daily Activity Reports and Incident Reports electronically via a mobile device or laptop connected to a cellular signal. Mobile devices must be able to receive emergency notifications from the JWA Emergency Notification System (Alert JWA).

\*\*\*Cell Phone/Mobile Device: There is not a hard-wired phone in these locations. Security Guards working these posts must be able to use a Contractor provided cell phone to contact JWA, Orange County Sheriff's Department (OCSD), and Contractor Supervisors. If the cell phone can be used to make phone calls and complete reports, only one device is needed.

(Signature page follows)



County of Orange, John Wayne Airport

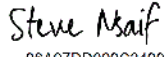
MA-280-22010553  
Armed Security Guard Services

**Signature Page**

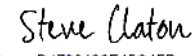
IN WITNESS WHEREOF, the Parties hereto have executed this Amendment on the date first above written.

**UNIVERSAL PROTECTION SERVICE, LP  
DRA ALLIED UNIVERSAL SECURITY SERVICES\***

DocuSigned by:

	Steve Nsaif	General Manager	11/1/2024
06A97DD999C2499...	Name	Title	Date

DocuSigned by:

	Steve Claton	Regional President	11/2/2024
D4738438E45C4FD...	Name	Title	Date

**COUNTY OF ORANGE**, A political subdivision of the State of California

**COUNTY AUTHORIZED SIGNATURE:**

		Deputy Purchasing Agent	
Signature	Name	Title	Date

**APPROVED AS TO FORM:**

County Counsel

By  \_\_\_\_\_  
 28F9D76C829A49E...  
 Deputy  
 Date 11/4/2024

\* If the contracting party is a corporation, (2) two signatures are required: one (1) signature by the Chairman of the Board, the President or any Vice President; and one (1) signature by the Secretary, any Assistant Secretary, the Chief Financial Officer or any Assistant Treasurer. The signature of one person alone is sufficient to bind a corporation, as long as he or she holds corporate offices in each of the two categories described above. For County purposes, proof of such dual office holding will be satisfied by having the individual sign the instrument twice, each time indicating his or her office that qualifies under the above described provision. In the alternative, a single corporate signature is acceptable when accompanied by a corporate resolution demonstrating the legal authority of the signatory to bind the corporation.

## Contract Summary Form

OC Expediter Requisition #: 1647168

Universal Protection Service, LP DBA Allied Universal Security Services

### SUMMARY OF SIGNIFICANT CHANGES

1. Costs: Annual increase of \$1,136,576 compared to years one, two, and three due to:
  - a. Additional staffing to support new Title 49 CFR 1542 Transportation Security regulatory requirements
  - b. Additional staffing to support meal and rest breaks due to California Assembly Bill 1522 enacted on January 1, 2024.
  - c. Planned construction activity.
  - d. Promotion of the current Site Supervisor to an Assistant Account Manager position and change of hours.
  - e. Replacement of existing duty vehicle.
  - f. Additional services to cover unforeseen private security needs.
2. Changes to Unarmed Private Security Positions

Contract/ Amendment Dates	Number of Security Positions/Posts
February 1, 2022 to January 31, 2025	JWA Subordinate Contract: (7) Curbside Traffic Posts (4) Airfield Vehicle Access Posts (2) Security Shift Supervisors (1) Terminal C Exit Lane Post (1) Concession Product Screening Post (1) Security Site Supervisor (1) Account Manager
February 1, 2025 to January 31, 2027	JWA Subordinate Contract: <b>(8) Curbside Traffic Posts – 1 additional position</b> (4) Airfield Vehicle Access Posts (2) Security Shift Supervisors <b>(2) Relief (Breaks, Lunches) - 2 new positions</b> <b>(2) Aviation Worker Screening (AWS) Post – 2 new positions</b> (1) Terminal C Exit Lane Post (1) Concession Product Screening Post <b>(1) Assistant Account Manager – Promotion (Former Security Site Supervisor)</b> (1) Account Manager

3. Term: Renew the contract for two additional years, effective February 1, 2025, through January 31, 2027.

#### **SUBCONTRACTORS**

This contract does not currently include subcontractors or pass-through to other providers.

#### **CONTRACT OPERATING EXPENSES**

Renew the contract for two additional (2) years (Year 4 and 5) in the amount not to exceed \$8,018,663.23.

2 Year Renewal Cost Breakdown:

- Year 4 contract not-to-exceed amount: \$3,875,438.08 including \$50,000 for unanticipated additional services.
- Year 5 contract not-to-exceed amount: \$4,143,225.15 including \$50,000 for unanticipated additional services.

---

This content is from the eCFR and is authoritative but unofficial.

---

## **Title 49 –Transportation**

### **Subtitle B –Other Regulations Relating to Transportation**

#### **Chapter XII –Transportation Security Administration, Department of Homeland Security**

##### **Subchapter C –Civil Aviation Security**

###### **Part 1542** Airport Security

###### **Subpart A** General

§ 1542.1 Applicability of this part.

§ 1542.3 Airport security coordinator.

§ 1542.5

###### **Subpart B** Airport Security Program

§ 1542.101 General requirements.

§ 1542.103 Content.

§ 1542.105 Approval and amendments.

§ 1542.107 Changed conditions affecting security.

§ 1542.109 Alternate means of compliance.

§ 1542.111 Exclusive area agreements.

§ 1542.113 Airport tenant security programs.

###### **Subpart C** Operations

§ 1542.201 Security of the secured area.

§ 1542.203 Security of the air operations area (AOA).

§ 1542.205 Security of the security identification display area (SIDA).

§ 1542.207 Access control systems.

§ 1542.209 Fingerprint-based criminal history records checks (CHRC).

§ 1542.211 Identification systems.

§ 1542.213 Training.

§ 1542.215 Law enforcement support.

§ 1542.217 Law enforcement personnel.

§ 1542.219 Supplementing law enforcement personnel.

§ 1542.221 Records of law enforcement response.

###### **Subpart D** Contingency Measures

§ 1542.301 Contingency plan.

§ 1542.303 Security Directives and Information Circulars.

§ 1542.305 Public advisories.

§ 1542.307 Incident management.



## PART 1542—AIRPORT SECURITY

**Authority:** 49 U.S.C. 114, 5103, 40113, 44901-44905, 44907, 44913-44914, 44916-44917, 44935-44936, 44942, 46105.

**Source:** 67 FR 8355, Feb. 22, 2002, unless otherwise noted.

### Subpart A—General

#### § 1542.1 Applicability of this part.

This part describes aviation security rules governing:

- (a) The operation of airports regularly serving aircraft operations required to be under a security program under part 1544 of this chapter, as described in this part.
- (b) The operation of airport regularly serving foreign air carrier operations required to be under a security program under part 1546 of this chapter, as described in this part.
- (c) Each airport operator that receives a Security Directive or Information Circular and each person who receives information from a Security Directive or Information Circular issued by the Designated official for Civil Aviation Security.
- (d) Each airport operator that does not have a security program under this part that serves an aircraft operator operating under a security program under part 1544 of this chapter, or a foreign air carrier operating under a security program under part 1546 of this chapter. Such airport operators must comply with § 1542.5(e).

[67 FR 8355, Feb. 22, 2002, as amended at 71 FR 30509, May 26, 2006]

#### § 1542.3 Airport security coordinator.

- (a) Each airport operator must designate one or more Airport Security Coordinator(s) (ASC) in its security program.
- (b) The airport operator must ensure that one or more ASCs:
  - (1) Serve as the airport operator's primary and immediate contact for security-related activities and communications with TSA. Any individual designated as an ASC may perform other duties in addition to those described in this paragraph (b).
  - (2) Is available to TSA on a 24-hour basis.
  - (3) Review with sufficient frequency all security-related functions to ensure that all are effective and in compliance with this part, its security program, and applicable Security Directives.
  - (4) Immediately initiate corrective action for any instance of non-compliance with this part, its security program, and applicable Security Directives.
  - (5) Review and control the results of employment history, verification, and criminal history records checks required under § 1542.209.

- (6) Serve as the contact to receive notification from individuals applying for unescorted access of their intent to seek correction of their criminal history record with the FBI.
- (c) After July 17, 2003, no airport operator may use, nor may it designate any person as, an ASC unless that individual has completed subject matter training, as specified in its security program, to prepare the individual to assume the duties of the position. The airport operator must maintain ASC training documentation until at least 180 days after the withdrawal of an individual's designation as an ASC.
- (d) An individual's satisfactory completion of initial ASC training required under paragraph (c) of this section satisfies that requirement for all future ASC designations for that individual, except for site specific information, unless there has been a two or more year break in service as an active and designated ASC.

## § 1542.5

## § 1542.5 [Reserved]

### Subpart B—Airport Security Program

#### § 1542.101 General requirements.

- (a) No person may operate an airport subject to § 1542.103 unless it adopts and carries out a security program that—
  - (1) Provides for the safety and security of persons and property on an aircraft operating in air transportation or intrastate air transportation against an act of criminal violence, aircraft piracy, and the introduction of an unauthorized weapon, explosive, or incendiary onto an aircraft;
  - (2) Is in writing and is signed by the airport operator;
  - (3) Includes the applicable items listed in § 1542.103;
  - (4) Includes an index organized in the same subject area sequence as § 1542.103; and
  - (5) Has been approved by TSA.
- (b) Each airport operator subject to § 1542.103 must maintain one current and complete copy of its security program and provide a copy to TSA upon request.
- (c) Each airport operator subject to § 1542.103 must—
  - (1) Restrict the distribution, disclosure, and availability of sensitive security information (SSI), as defined in part 1520 of this chapter, to persons with a need to know; and
  - (2) Refer all requests for SSI by other persons to TSA.

[67 FR 8355, Feb. 22, 2002, as amended at 71 FR 30509, May 26, 2006]

#### § 1542.103 Content.

- (a) **Complete program.** Except as otherwise approved by TSA, each airport operator regularly serving operations of an aircraft operator or foreign air carrier described in § 1544.101(a)(1) or § 1546.101(a) of this chapter, must include in its security program the following:
  - (1) The name, means of contact, duties, and training requirements of the ASC required under § 1542.3.

- (2) [Reserved]
- (3) A description of the secured areas, including—
  - (i) A description and map detailing boundaries and pertinent features;
  - (ii) Each activity or entity on, or adjacent to, a secured area that affects security;
  - (iii) Measures used to perform the access control functions required under § 1542.201(b)(1);
  - (iv) Procedures to control movement within the secured area, including identification media required under § 1542.201(b)(3); and
  - (v) A description of the notification signs required under § 1542.201(b)(6).
- (4) A description of the AOA, including—
  - (i) A description and map detailing boundaries, and pertinent features;
  - (ii) Each activity or entity on, or adjacent to, an AOA that affects security;
  - (iii) Measures used to perform the access control functions required under § 1542.203(b)(1);
  - (iv) Measures to control movement within the AOA, including identification media as appropriate; and
  - (v) A description of the notification signs required under § 1542.203(b)(4).
- (5) A description of the SIDA's, including—
  - (i) A description and map detailing boundaries and pertinent features; and
  - (ii) Each activity or entity on, or adjacent to, a SIDA.
- (6) A description of the sterile areas, including—
  - (i) A diagram with dimensions detailing boundaries and pertinent features;
  - (ii) Access controls to be used when the passenger-screening checkpoint is non-operational and the entity responsible for that access control; and
  - (iii) Measures used to control access as specified in § 1542.207.
- (7) Procedures used to comply with § 1542.209 regarding fingerprint-based criminal history records checks.
- (8) A description of the personnel identification systems as described in § 1542.211.
- (9) Escort procedures in accordance with § 1542.211(e).
- (10) Challenge procedures in accordance with § 1542.211(d).
- (11) Training programs required under §§ 1542.213 and 1542.217(c)(2), if applicable.
- (12) A description of law enforcement support used to comply with § 1542.215(a).
- (13) A system for maintaining the records described in § 1542.221.

- (14) The procedures and a description of facilities and equipment used to support TSA inspection of individuals and property, and aircraft operator or foreign air carrier screening functions of parts 1544 and 1546 of this chapter.
- (15) A contingency plan required under § 1542.301.
- (16) Procedures for the distribution, storage, and disposal of security programs, Security Directives, Information Circulars, implementing instructions, and, as appropriate, classified information.
- (17) Procedures for posting of public advisories as specified in § 1542.305.
- (18) Incident management procedures used to comply with § 1542.307.
- (19) Alternate security procedures, if any, that the airport operator intends to use in the event of natural disasters, and other emergency or unusual conditions.
- (20) Each exclusive area agreement as specified in § 1542.111.
- (21) Each airport tenant security program as specified in § 1542.113.
- (b) **Supporting program.** Except as otherwise approved by TSA, each airport regularly serving operations of an aircraft operator or foreign air carrier described in § 1544.101(a)(2) or (f), or § 1546.101(b) or (c) of this chapter, must include in its security program a description of the following:
  - (1) Name, means of contact, duties, and training requirements of the ASC, as required under § 1542.3.
  - (2) A description of the law enforcement support used to comply with § 1542.215(a).
  - (3) Training program for law enforcement personnel required under § 1542.217(c)(2), if applicable.
  - (4) A system for maintaining the records described in § 1542.221.
  - (5) The contingency plan required under § 1542.301.
  - (6) Procedures for the distribution, storage, and disposal of security programs, Security Directives, Information Circulars, implementing instructions, and, as appropriate, classified information.
  - (7) Procedures for public advisories as specified in § 1542.305.
  - (8) Incident management procedures used to comply with § 1542.307.
- (c) **Partial program.** Except as otherwise approved by TSA, each airport regularly serving operations of an aircraft operator or foreign air carrier described in § 1544.101(b) or § 1546.101(d) of this chapter, must include in its security program a description of the following:
  - (1) Name, means of contact, duties, and training requirements of the ASC as required under § 1542.3.
  - (2) A description of the law enforcement support used to comply with § 1542.215(b).
  - (3) Training program for law enforcement personnel required under § 1542.217(c)(2), if applicable.
  - (4) A system for maintaining the records described in § 1542.221.
  - (5) Procedures for the distribution, storage, and disposal of security programs, Security Directives, Information Circulars, implementing instructions, and, as appropriate, classified information.
  - (6) Procedures for public advisories as specified in § 1542.305.
  - (7) Incident management procedures used to comply with § 1542.307.

- (d) **Use of appendices.** The airport operator may comply with paragraphs (a), (b), and (c) of this section by including in its security program, as an appendix, any document that contains the information required by paragraphs (a), (b), and (c) of this section. The appendix must be referenced in the corresponding section(s) of the security program.

### § 1542.105 Approval and amendments.

- (a) **Initial approval of security program.** Unless otherwise authorized by the designated official, each airport operator required to have a security program under this part must submit its initial proposed security program to the designated official for approval at least 90 days before the date any aircraft operator or foreign air carrier required to have a security program under part 1544 or part 1546 of this chapter is expected to begin operations. Such requests will be processed as follows:
- (1) The designated official, within 30 days after receiving the proposed security program, will either approve the program or give the airport operator written notice to modify the program to comply with the applicable requirements of this part.
  - (2) The airport operator may either submit a modified security program to the designated official for approval, or petition the Administrator to reconsider the notice to modify within 30 days of receiving a notice to modify. A petition for reconsideration must be filed with the designated official.
  - (3) The designated official, upon receipt of a petition for reconsideration, either amends or withdraws the notice, or transmits the petition, together with any pertinent information, to the Administrator for reconsideration. The Administrator disposes of the petition within 30 days of receipt by either directing the designated official to withdraw or amend the notice to modify, or by affirming the notice to modify.
- (b) **Amendment requested by an airport operator.** Except as provided in § 1542.103(c), an airport operator may submit a request to the designated official to amend its security program, as follows:
- (1) The request for an amendment must be filed with the designated official at least 45 days before the date it proposes for the amendment to become effective, unless a shorter period is allowed by the designated official.
  - (2) Within 30 days after receiving a proposed amendment, the designated official, in writing, either approves or denies the request to amend.
  - (3) An amendment to a security program may be approved if the designated official determines that safety and the public interest will allow it, and the proposed amendment provides the level of security required under this part.
  - (4) Within 30 days after receiving a denial, the airport operator may petition the Administrator to reconsider the denial.
  - (5) Upon receipt of a petition for reconsideration, the designated official either approves the request to amend or transmits the petition within 30 days of receipt, together with any pertinent information, to the Administrator for reconsideration. The Administrator disposes of the petition within 30 days of receipt by either directing the designated official to approve the amendment or affirming the denial.
- (c) **Amendment by TSA.** If safety and the public interest require an amendment, the designated official may amend a security program as follows:

- (1) The designated official sends to the airport operator a notice, in writing, of the proposed amendment, fixing a period of not less than 30 days within which the airport operator may submit written information, views, and arguments on the amendment.
- (2) After considering all relevant material, the designated official notifies the airport operator of any amendment adopted or rescinds the notice. If the amendment is adopted, it becomes effective not less than 30 days after the airport operator receives the notice of amendment, unless the airport operator petitions the Administrator to reconsider no later than 15 days before the effective date of the amendment. The airport operator must send the petition for reconsideration to the designated official. A timely petition for reconsideration stays the effective date of the amendment.
- (3) Upon receipt of a petition for reconsideration, the designated official either amends or withdraws the notice, or transmits the petition, together with any pertinent information to the Administrator for reconsideration. The Administrator disposes of the petition within 30 days of receipt by either directing the designated official to withdraw or amend the amendment, or by affirming the amendment.
- (d) **Emergency amendments.** Notwithstanding paragraph (c) of this section, if the designated official finds that there is an emergency requiring immediate action with respect to safety and security in air transportation or in air commerce that makes procedures in this section contrary to the public interest, the designated official may issue an amendment, effective without stay on the date the airport operator receives the notice of it. In such a case, the designated official must incorporate in the notice a brief statement of the reasons and findings for the amendment to be adopted. The airport operator may file a petition for reconsideration under paragraph (c) of this section; however, this does not stay the effective date of the emergency amendment.

### § 1542.107 Changed conditions affecting security.

- (a) After approval of the security program, each airport operator must notify TSA when changes have occurred to the—
  - (1) Measures, training, area descriptions, or staffing, described in the security program;
  - (2) Operations of an aircraft operator or foreign air carrier that would require modifications to the security program as required under § 1542.103; or
  - (3) Layout or physical structure of any area under the control of the airport operator, airport tenant, aircraft operator, or foreign air carrier used to support the screening process, access, presence, or movement control functions required under part 1542, 1544, or 1546 of this chapter.
- (b) Each airport operator must notify TSA no more than 6 hours after the discovery of any changed condition described in paragraph (a) of this section, or within the time specified in its security program, of the discovery of any changed condition described in paragraph (a) of this section. The airport operator must inform TSA of each interim measure being taken to maintain adequate security until an appropriate amendment to the security program is approved. Each interim measure must be acceptable to TSA.
- (c) For changed conditions expected to be less than 60 days duration, each airport operator must forward the information required in paragraph (b) of this section in writing to TSA within 72 hours of the original notification of the change condition(s). TSA will notify the airport operator of the disposition of the notification in writing. If approved by TSA, this written notification becomes a part of the airport security program for the duration of the changed condition(s).

- (d) For changed conditions expected to be 60 days or more duration, each airport operator must forward the information required in paragraph (b) of this section in the form of a proposed amendment to the airport operator's security program, as required under § 1542.105. The request for an amendment must be made within 30 days of the discovery of the changed condition(s). TSA will respond to the request in accordance with § 1542.105.

### § 1542.109 Alternate means of compliance.

If in TSA's judgment, the overall safety and security of the airport, and aircraft operator or foreign air carrier operations are not diminished, TSA may approve a security program that provides for the use of alternate measures. Such a program may be considered only for an operator of an airport at which service by aircraft operators or foreign air carriers under part 1544 or 1546 of this chapter is determined by TSA to be seasonal or infrequent.

### § 1542.111 Exclusive area agreements.

- (a) TSA may approve an amendment to an airport security program under which an aircraft operator or foreign air carrier that has a security program under part 1544 or 1546 of this chapter assumes responsibility for specified security measures for all or portions of the secured area, AOA, or SIDA, including access points, as provided in § 1542.201, § 1542.203, or § 1542.205. The assumption of responsibility must be exclusive to one aircraft operator or foreign air carrier, and shared responsibility among aircraft operators or foreign air carriers is not permitted for an exclusive area.
- (b) An exclusive area agreement must be in writing, signed by the airport operator and aircraft operator or foreign air carrier, and maintained in the airport security program. This agreement must contain the following:
  - (1) A description, a map, and, where appropriate, a diagram of the boundaries and pertinent features of each area, including individual access points, over which the aircraft operator or foreign air carrier will exercise exclusive security responsibility.
  - (2) A description of the measures used by the aircraft operator or foreign air carrier to comply with § 1542.201, § 1542.203, or § 1542.205, as appropriate.
  - (3) Procedures by which the aircraft operator or foreign air carrier will immediately notify the airport operator and provide for alternative security measures when there are changed conditions as described in § 1542.103(a).
- (c) Any exclusive area agreements in effect on November 14, 2001, must meet the requirements of this section and § 1544.227 no later than November 14, 2002.

### § 1542.113 Airport tenant security programs.

- (a) TSA may approve an airport tenant security program as follows:
  - (1) The tenant must assume responsibility for specified security measures of the secured area, AOA, or SIDA as provided in §§ 1542.201, 1542.203, and 1542.205.
  - (2) The tenant may not assume responsibility for law enforcement support under § 1542.215.
  - (3) The tenant must assume the responsibility within the tenant's leased areas or areas designated for the tenant's exclusive use. A tenant may not assume responsibility under a tenant security program for the airport passenger terminal.

- (4) Responsibility must be exclusive to one tenant, and shared responsibility among tenants is not permitted.
- (5) TSA must find that the tenant is able and willing to carry out the airport tenant security program.
- (b) An airport tenant security program must be in writing, signed by the airport operator and the airport tenant, and maintained in the airport security program. The airport tenant security program must include the following:
  - (1) A description and a map of the boundaries and pertinent features of each area over which the airport tenant will exercise security responsibilities.
  - (2) A description of the measures the airport tenant has assumed.
  - (3) Measures by which the airport operator will monitor and audit the tenant's compliance with the security program.
  - (4) Monetary and other penalties to which the tenant may be subject if it fails to carry out the airport tenant security program.
  - (5) Circumstances under which the airport operator will terminate the airport tenant security program for cause.
  - (6) A provision acknowledging that the tenant is subject to inspection by TSA in accordance with § 1542.5.
  - (7) A provision acknowledging that individuals who carry out the tenant security program are contracted to or acting for the airport operator and are required to protect sensitive information in accordance with part 1520 of this chapter, and may be subject to civil penalties for failing to protect sensitive security information.
  - (8) Procedures by which the tenant will immediately notify the airport operator of and provide for alternative security measures for changed conditions as described in § 1542.103(a).
- (c) If TSA has approved an airport tenant security program, the airport operator may not be found to be in violation of a requirement of this part in any case in which the airport operator demonstrates that:
  - (1) The tenant or an employee, permittee, or invitee of the tenant, is responsible for such violation; and
  - (2) The airport operator has complied with all measures in its security program to ensure the tenant has complied with the airport tenant security program.
- (d) TSA may amend or terminate an airport tenant security program in accordance with § 1542.105.

## Subpart C—Operations

### § 1542.201 Security of the secured area.

- (a) Each airport operator required to have a security program under § 1542.103(a) must establish at least one secured area.
- (b) Each airport operator required to establish a secured area must prevent and detect the unauthorized entry, presence, and movement of individuals and ground vehicles into and within the secured area by doing the following:



- (1) Establish and carry out measures for controlling entry to secured areas of the airport in accordance with § 1542.207.
- (2) Provide for detection of, and response to, each unauthorized presence or movement in, or attempted entry to, the secured area by an individual whose access is not authorized in accordance with its security program.
- (3) Establish and carry out a personnel identification system described under § 1542.211.
- (4) Subject each individual to employment history verification as described in § 1542.209 before authorizing unescorted access to a secured area.
- (5) Train each individual before granting unescorted access to the secured area, as required in § 1542.213(b).
- (6) Post signs at secured area access points and on the perimeter that provide warning of the prohibition against unauthorized entry. Signs must be posted by each airport operator in accordance with its security program not later than November 14, 2003.

### **§ 1542.203 Security of the air operations area (AOA).**

- (a) Each airport operator required to have a security program under § 1542.103(a) must establish an AOA, unless the entire area is designated as a secured area.
- (b) Each airport operator required to establish an AOA must prevent and detect the unauthorized entry, presence, and movement of individuals and ground vehicles into or within the AOA by doing the following:
  - (1) Establish and carry out measures for controlling entry to the AOA of the airport in accordance with § 1542.207.
  - (2) Provide for detection of, and response to, each unauthorized presence or movement in, or attempted entry to, the AOA by an individual whose access is not authorized in accordance with its security program.
  - (3) Provide security information as described in § 1542.213(c) to each individual with unescorted access to the AOA.
  - (4) Post signs on AOA access points and perimeters that provide warning of the prohibition against unauthorized entry to the AOA. Signs must be posted by each airport operator in accordance with its security program not later than November 14, 2003.
  - (5) If approved by TSA, the airport operator may designate all or portions of its AOA as a SIDA, or may use another personnel identification system, as part of its means of meeting the requirements of this section. If it uses another personnel identification system, the media must be clearly distinguishable from those used in the secured area and SIDA.

### **§ 1542.205 Security of the security identification display area (SIDA).**

- (a) Each airport operator required to have a complete program under § 1542.103(a) must establish at least one SIDA, as follows:
  - (1) Each secured area must be a SIDA.

- (2) Each part of the air operations area that is regularly used to load cargo on, or unload cargo from, an aircraft that is operated under a full program or a full all-cargo program as provided in § 1544.101(a) or (h) of this chapter, or a foreign air carrier under a security program as provided in § 1546.101(a), (b), or (e), must be a SIDA.
  - (3) Each area on an airport where cargo is present after an aircraft operator operating under a full program or a full all-cargo program under § 1544.101(a) or (h) of this chapter, or a foreign air carrier operating under a security program under § 1546.101(a), (b), or (e) of this chapter, or an indirect air carrier, accepts it must be a SIDA. This includes areas such as: Cargo facilities; loading and unloading vehicle docks; and areas where an aircraft operator, foreign air carrier, or indirect air carrier sorts, stores, stages, consolidates, processes, screens, or transfers cargo.
  - (4) Other areas of the airport may be SIDAs.
- (b) Each airport operator required to establish a SIDA must establish and carry out measures to prevent the unauthorized presence and movement of individuals in the SIDA and must do the following:
- (1) Establish and carry out a personnel identification system described under § 1542.211.
  - (2) Subject each individual to a criminal history records check as described in § 1542.209 before authorizing unescorted access to the SIDA.
  - (3) Train each individual before granting unescorted access to the SIDA, as required in § 1542.213(b).
- (c) An airport operator that is not required to have a complete program under § 1542.103(a) is not required to establish a SIDA under this section.

[67 FR 8355, Feb. 22, 2002, as amended at 71 FR 30509, May 26, 2006]

### § 1542.207 Access control systems.

- (a) **Secured area.** Except as provided in paragraph (b) of this section, the measures for controlling entry to the secured area required under § 1542.201(b)(1) must—
- (1) Ensure that only those individuals authorized to have unescorted access to the secured area are able to gain entry;
  - (2) Ensure that an individual is immediately denied entry to a secured area when that person's access authority for that area is withdrawn; and
  - (3) Provide a means to differentiate between individuals authorized to have access to an entire secured area and individuals authorized access to only a particular portion of a secured area.
- (b) **Alternative systems.** TSA may approve an amendment to a security program that provides alternative measures that provide an overall level of security equal to that which would be provided by the measures described in paragraph (a) of this section.
- (c) **Air operations area.** The measures for controlling entry to the AOA required under § 1542.203(b)(1) must incorporate accountability procedures to maintain their integrity.
- (d) **Secondary access media.** An airport operator may issue a second access medium to an individual who has unescorted access to secured areas or the AOA, but is temporarily not in possession of the original access medium, if the airport operator follows measures and procedures in the security program that—
- (1) Verifies the authorization of the individual to have unescorted access to secured areas or AOA;

- (2) Restricts the time period of entry with the second access medium;
- (3) Retrieves the second access medium when expired;
- (4) Deactivates or invalidates the original access medium until the individual returns the second access medium; and
- (5) Provides that any second access media that is also used as identification media meet the criteria of § 1542.211(b).

### § 1542.209 Fingerprint-based criminal history records checks (CHRC).

(a) **Scope.** The following persons are within the scope of this section—

- (1) Each airport operator and airport user.
- (2) Each individual currently having unescorted access to a SIDA, and each individual with authority to authorize others to have unescorted access to a SIDA (referred to as unescorted access authority).
- (3) Each individual seeking unescorted access authority.
- (4) Each airport user and aircraft operator making a certification to an airport operator pursuant to paragraph (n) of this section, or 14 CFR 108.31(n) in effect prior to November 14, 2001 (see 14 CFR Parts 60 to 139 revised as of January 1, 2001). An airport user, for the purposes of this section only, is any person other than an aircraft operator subject to § 1544.229 of this chapter making a certification under this section.

(b) **Individuals seeking unescorted access authority.** Except as provided in paragraph (m) of this section, each airport operator must ensure that no individual is granted unescorted access authority unless the individual has undergone a fingerprint-based CHRC that does not disclose that he or she has a disqualifying criminal offense, as described in paragraph (d) of this section.

(c) **Individuals who have not had a CHRC.**

- (1) Except as provided in paragraph (m) of this section, each airport operator must ensure that after December 6, 2002, no individual retains unescorted access authority, unless the airport operator has obtained and submitted a fingerprint under this part.
- (2) When a CHRC discloses a disqualifying criminal offense for which the conviction or finding of not guilty by reason of insanity was on or after December 6, 1991, the airport operator must immediately suspend that individual's authority.

(d) **Disqualifying criminal offenses.** An individual has a disqualifying criminal offense if the individual has been convicted, or found not guilty of by reason of insanity, of any of the disqualifying crimes listed in this paragraph (d) in any jurisdiction during the 10 years before the date of the individual's application for unescorted access authority, or while the individual has unescorted access authority. The disqualifying criminal offenses are as follows—

- (1) Forgery of certificates, false marking of aircraft, and other aircraft registration violation; 49 U.S.C. 46306.
- (2) Interference with air navigation; 49 U.S.C. 46308.
- (3) Improper transportation of a hazardous material; 49 U.S.C. 46312.
- (4) Aircraft piracy; 49 U.S.C. 46502.

- (5) Interference with flight crew members or flight attendants; 49 U.S.C. 46504.
- (6) Commission of certain crimes aboard aircraft in flight; 49 U.S.C. 46506.
- (7) Carrying a weapon or explosive aboard aircraft; 49 U.S.C. 46505.
- (8) Conveying false information and threats; 49 U.S.C. 46507.
- (9) Aircraft piracy outside the special aircraft jurisdiction of the United States; 49 U.S.C. 46502(b).
- (10) Lighting violations involving transporting controlled substances; 49 U.S.C. 46315.
- (11) Unlawful entry into an aircraft or airport area that serves air carriers or foreign air carriers contrary to established security requirements; 49 U.S.C. 46314.
- (12) Destruction of an aircraft or aircraft facility; 18 U.S.C. 32.
- (13) Murder.
- (14) Assault with intent to murder.
- (15) Espionage.
- (16) Sedition.
- (17) Kidnapping or hostage taking.
- (18) Treason.
- (19) Rape or aggravated sexual abuse.
- (20) Unlawful possession, use, sale, distribution, or manufacture of an explosive or weapon.
- (21) Extortion.
- (22) Armed or felony unarmed robbery.
- (23) Distribution of, or intent to distribute, a controlled substance.
- (24) Felony arson.
- (25) Felony involving a threat.
- (26) Felony involving—
  - (i) Willful destruction of property;
  - (ii) Importation or manufacture of a controlled substance;
  - (iii) Burglary;
  - (iv) Theft;
  - (v) Dishonesty, fraud, or misrepresentation;
  - (vi) Possession or distribution of stolen property;
  - (vii) Aggravated assault;
  - (viii) Bribery; or

(ix) Illegal possession of a controlled substance punishable by a maximum term of imprisonment of more than 1 year.

(27) Violence at international airports; 18 U.S.C. 37.

(28) Conspiracy or attempt to commit any of the criminal acts listed in this paragraph (d).

(e) ***Fingerprint application and processing.***

(1) At the time of fingerprinting, the airport operator must provide the individual to be fingerprinted a fingerprint application that includes only the following—

(i) The disqualifying criminal offenses described in paragraph (d) of this section.

(ii) A statement that the individual signing the application does not have a disqualifying criminal offense.

(iii) A statement informing the individual that Federal regulations under 49 CFR 1542.209 (l) impose a continuing obligation to disclose to the airport operator within 24 hours if he or she is convicted of any disqualifying criminal offense that occurs while he or she has unescorted access authority. After February 17, 2002, the airport operator may use statements that have already been printed referring to 14 CFR 107.209 until stocks of such statements are used up.

(iv) A statement reading, "The information I have provided on this application is true, complete, and correct to the best of my knowledge and belief and is provided in good faith. I understand that a knowing and willful false statement on this application can be punished by fine or imprisonment or both. (See section 1001 of Title 18 United States Code.)"

(v) A line for the printed name of the individual.

(vi) A line for the individual's signature and date of signature.

(2) Each individual must complete and sign the application prior to submitting his or her fingerprints.

(3) The airport operator must verify the identity of the individual through two forms of identification prior to fingerprinting, and ensure that the printed name on the fingerprint application is legible. At least one of the two forms of identification must have been issued by a government authority, and at least one must include a photo.

(4) The airport operator must advise the individual that:

(i) A copy of the criminal record received from the FBI will be provided to the individual, if requested by the individual in writing; and

(ii) The ASC is the individual's point of contact if he or she has questions about the results of the CHRC.

(5) The airport operator must collect, control, and process one set of legible and classifiable fingerprints under direct observation of the airport operator or a law enforcement officer.

(6) Fingerprints may be obtained and processed electronically, or recorded on fingerprint cards approved by the FBI and distributed by TSA for that purpose.

(7) The fingerprint submission must be forwarded to TSA in the manner specified by TSA.

- (f) **Fingerprinting fees.** Airport operators must pay for all fingerprints in a form and manner approved by TSA. The payment must be made at the designated rate (available from the local TSA security office) for each set of fingerprints submitted. Information about payment options is available through the designated TSA headquarters point of contact. Individual personal checks are not acceptable.
- (g) **Determination of arrest status.**
- (1) When a CHRC on an individual seeking unescorted access authority discloses an arrest for any disqualifying criminal offense listed in paragraph (d) of this section without indicating a disposition, the airport operator must determine, after investigation, that the arrest did not result in a disqualifying offense before granting that authority. If there is no disposition, or if the disposition did not result in a conviction or in a finding of not guilty by reason of insanity of one of the offenses listed in paragraph (d) of this section, the individual is not disqualified under this section.
  - (2) When a CHRC on an individual with unescorted access authority discloses an arrest for any disqualifying criminal offense without indicating a disposition, the airport operator must suspend the individual's unescorted access authority not later than 45 days after obtaining the CHRC unless the airport operator determines, after investigation, that the arrest did not result in a disqualifying criminal offense. If there is no disposition, or if the disposition did not result in a conviction or in a finding of not guilty by reason of insanity of one of the offenses listed in paragraph (d) of this section, the individual is not disqualified under this section.
  - (3) The airport operator may only make the determinations required in paragraphs (g)(1) and (g)(2) of this section for individuals for whom it is issuing, or has issued, unescorted access authority, and who are not covered by a certification from an aircraft operator under paragraph (n) of this section. The airport operator may not make determinations for individuals described in § 1544.229 of this chapter.
- (h) **Correction of FBI records and notification of disqualification.**
- (1) Before making a final decision to deny unescorted access authority to an individual described in paragraph (b) of this section, the airport operator must advise him or her that the FBI criminal record discloses information that would disqualify him or her from receiving or retaining unescorted access authority and provide the individual with a copy of the FBI record if he or she requests it.
  - (2) The airport operator must notify an individual that a final decision has been made to grant or deny unescorted access authority.
  - (3) Immediately following the suspension of unescorted access authority of an individual, the airport operator must advise him or her that the FBI criminal record discloses information that disqualifies him or her from retaining unescorted access authority and provide the individual with a copy of the FBI record if he or she requests it.
- (i) **Corrective action by the individual.** The individual may contact the local jurisdiction responsible for the information and the FBI to complete or correct the information contained in his or her record, subject to the following conditions—
- (1) For an individual seeking unescorted access authority on or after December 6, 2001, the following applies:
    - (i) Within 30 days after being advised that the criminal record received from the FBI discloses a disqualifying criminal offense, the individual must notify the airport operator in writing of his or her intent to correct any information he or she believes to be inaccurate. The airport operator

must obtain a copy, or accept a copy from the individual, of the revised FBI record, or a certified true copy of the information from the appropriate court, prior to granting unescorted access authority.

- (ii) If no notification, as described in paragraph (h)(1) of this section, is received within 30 days, the airport operator may make a final determination to deny unescorted access authority.
- (2) For an individual with unescorted access authority before December 6, 2001, the following applies: Within 30 days after being advised of suspension because the criminal record received from the FBI discloses a disqualifying criminal offense, the individual must notify the airport operator in writing of his or her intent to correct any information he or she believes to be inaccurate. The airport operator must obtain a copy, or accept a copy from the individual, of the revised FBI record, or a certified true copy of the information from the appropriate court, prior to reinstating unescorted access authority.
- (j) **Limits on dissemination of results.** Criminal record information provided by the FBI may be used only to carry out this section and § 1544.229 of this chapter. No person may disseminate the results of a CHRC to anyone other than:
  - (1) The individual to whom the record pertains, or that individual's authorized representative.
  - (2) Officials of other airport operators who are determining whether to grant unescorted access to the individual under this part.
  - (3) Aircraft operators who are determining whether to grant unescorted access to the individual or authorize the individual to perform screening functions under part 1544 of this chapter.
  - (4) Others designated by TSA.
- (k) **Recordkeeping.** The airport operator must maintain the following information:
  - (1) **Investigations conducted before December 6, 2001.** The airport operator must maintain and control the access or employment history investigation files, including the criminal history records results portion, or the appropriate certifications, for investigations conducted before December 6, 2001.
  - (2) **Fingerprint application process on or after December 6, 2001.** Except when the airport operator has received a certification under paragraph (n) of this section, the airport operator must physically maintain, control, and, as appropriate, destroy the fingerprint application and the criminal record. Only direct airport operator employees may carry out the responsibility for maintaining, controlling, and destroying criminal records.
  - (3) **Certification on or after December 6, 2001.** The airport operator must maintain the certifications provided under paragraph (n) of this section.
  - (4) **Protection of records—all investigations.** The records required by this section must be maintained in a manner that is acceptable to TSA and in a manner that protects the confidentiality of the individual.
  - (5) **Duration—all investigations.** The records identified in this section with regard to an individual must be maintained until 180 days after the termination of the individual's unescorted access authority. When files are no longer maintained, the criminal record must be destroyed.
- (l) **Continuing responsibilities.**

- (1) Each individual with unescorted access authority on December 6, 2001, who had a disqualifying criminal offense in paragraph (d) of this section on or after December 6, 1991, must, by January 7, 2002, report the conviction to the airport operator and surrender the SIDA access medium to the issuer.
  - (2) Each individual with unescorted access authority who has a disqualifying criminal offense must report the offense to the airport operator and surrender the SIDA access medium to the issuer within 24 hours of the conviction or the finding of not guilty by reason of insanity.
  - (3) If information becomes available to the airport operator or the airport user indicating that an individual with unescorted access authority has a disqualifying criminal offense, the airport operator must determine the status of the conviction. If a disqualifying offense is confirmed the airport operator must immediately revoke any unescorted access authority.
- (m) **Exceptions.** Notwithstanding the requirements of this section, an airport operator must authorize the following individuals to have unescorted access authority:
- (1) An employee of the Federal, state, or local government (including a law enforcement officer) who, as a condition of employment, has been subjected to an employment investigation that includes a criminal records check.
  - (2) Notwithstanding the requirements of this section, an airport operator may authorize the following individuals to have unescorted access authority:
    - (i) An individual who has been continuously employed in a position requiring unescorted access authority by another airport operator, airport user, or aircraft operator, or contractor to such an entity, provided the grant for his or her unescorted access authority was based upon a fingerprint-based CHRC through TSA or FAA.
    - (ii) An individual who has been continuously employed by an aircraft operator or aircraft operator contractor, in a position with authority to perform screening functions, provided the grant for his or her authority to perform screening functions was based upon a fingerprint-based CHRC through TSA or FAA.
- (n) **Certifications by aircraft operators.** An airport operator is in compliance with its obligation under paragraph (b) or (c) of this section when the airport operator accepts, for each individual seeking unescorted access authority, certification from an aircraft operator subject to part 1544 of this chapter indicating it has complied with § 1544.229 of this chapter for the aircraft operator's employees and contractors seeking unescorted access authority. If the airport operator accepts a certification from the aircraft operator, the airport operator may not require the aircraft operator to provide a copy of the CHRC.
- (o) **Airport operator responsibility.** The airport operator must—
- (1) Designate the ASC, in the security program, or a direct employee if the ASC is not a direct employee, to be responsible for maintaining, controlling, and destroying the criminal record files when their maintenance is no longer required by paragraph (k) of this section.
  - (2) Designate the ASC, in the security program, to serve as the contact to receive notification from individuals applying for unescorted access authority of their intent to seek correction of their FBI criminal record.



(3) Audit the employment history investigations performed by the airport operator in accordance with this section and 14 CFR 107.31 in effect prior to November 14, 2001 (see 14 CFR Parts 60 through 139 revised as of January 1, 2001), and those investigations conducted by the airport users who provided certification to the airport operator. The audit program must be set forth in the airport security program.

(p) ***Airport user responsibility.***

(1) The airport user must report to the airport operator information, as it becomes available, that indicates an individual with unescorted access authority may have a disqualifying criminal offense.

(2) The airport user must maintain and control, in compliance with paragraph (k) of this section, the employment history investigation files for investigations conducted before December 6, 2001, unless the airport operator decides to maintain and control the employment history investigation file.

(3) The airport user must provide the airport operator with either the name or title of the individual acting as custodian of the files described in this paragraph (p), the address of the location where the files are maintained, and the phone number of that location. The airport user must provide the airport operator and TSA with access to these files.

### § 1542.211 Identification systems.

(a) ***Personnel identification system.*** The personnel identification system under §§ 1542.201(b)(3) and 1542.205(b)(1) must include the following:

(1) Personnel identification media that—

(i) Convey a full-face image, full name, employer, and identification number of the individual to whom the identification medium is issued;

(ii) Indicate clearly the scope of the individual's access and movement privileges;

(iii) Indicate clearly an expiration date; and

(iv) Are of sufficient size and appearance as to be readily observable for challenge purposes.

(2) Procedures to ensure that each individual in the secured area or SIDA continuously displays the identification medium issued to that individual on the outermost garment above waist level, or is under escort.

(3) Procedures to ensure accountability through the following:

(i) Retrieving expired identification media and media of persons who no longer have unescorted access authority.

(ii) Reporting lost or stolen identification media.

(iii) Securing unissued identification media stock and supplies.

(iv) Auditing the system at a minimum of once a year or sooner, as necessary, to ensure the integrity and accountability of all identification media.

(v) As specified in the security program, revalidate the identification system or reissue identification media if a portion of all issued, unexpired identification media are lost, stolen, or otherwise unaccounted for, including identification media that are combined with access media.

- (vi) Ensure that only one identification medium is issued to an individual at a time, except for personnel who are employed with more than one company and require additional identification media to carry out employment duties. A replacement identification medium may only be issued if an individual declares in writing that the medium has been lost, stolen, or destroyed.
- (b) **Temporary identification media.** Each airport operator may issue personnel identification media in accordance with its security program to persons whose duties are expected to be temporary. The temporary identification media system must include procedures and methods to—
  - (1) Retrieve temporary identification media;
  - (2) Authorize the use of a temporary media for a limited time only;
  - (3) Ensure that temporary media are distinct from other identification media and clearly display an expiration date; and
  - (4) Ensure that any identification media also being used as an access media meet the criteria of § 1542.207(d).
- (c) **Airport-approved identification media.** TSA may approve an amendment to the airport security program that provides for the use of identification media meeting the criteria of this section that are issued by entities other than the airport operator, as described in the security program.
- (d) **Challenge program.** Each airport operator must establish and carry out a challenge program that requires each individual who has authorized unescorted access to secured areas and SIDA's to ascertain the authority of any individual who is not displaying an identification medium authorizing the individual to be present in the area. The challenge program must include procedures to challenge individuals not displaying airport approved identification media. The procedure must—
  - (1) Apply uniformly in secured areas, SIDAs, and exclusive areas;
  - (2) Describe how to challenge an individual directly or report any individual not visibly displaying an authorized identification medium, including procedures to notify the appropriate authority; and
  - (3) Describe support of challenge procedures, including law enforcement and any other responses to reports of individuals not displaying authorized identification media.
- (e) **Escorting.** Each airport operator must establish and implement procedures for escorting individuals who do not have unescorted access authority to a secured area or SIDA that—
  - (1) Ensure that only individuals with unescorted access authority are permitted to escort;
  - (2) Ensure that the escorted individuals are continuously accompanied or monitored while within the secured area or SIDA in a manner sufficient to identify whether the escorted individual is engaged in activities other than those for which escorted access was granted, and to take action in accordance with the airport security program;
  - (3) Identify what action is to be taken by the escort, or other authorized individual, should individuals under escort engage in activities other than those for which access was granted;
  - (4) Prescribe law enforcement support for escort procedures; and
  - (5) Ensure that individuals escorted into a sterile area without being screened under § 1544.201 of this chapter remain under escort until they exit the sterile area, or submit to screening pursuant to § 1544.201 or § 1546.201 of this chapter.

- (f) **Effective date.** The identification systems described in this section must be implemented by each airport operator not later than November 14, 2003.

### § 1542.213 Training.

- (a) Each airport operator must ensure that individuals performing security-related functions for the airport operator are briefed on the provisions of this part, Security Directives, and Information Circulars, and the security program, to the extent that such individuals need to know in order to perform their duties.
- (b) An airport operator may not authorize any individual unescorted access to the secured area or SIDA, except as provided in § 1542.5, unless that individual has successfully completed training in accordance with TSA-approved curriculum specified in the security program. This curriculum must detail the methods of instruction, provide attendees with an opportunity to ask questions, and include at least the following topics—
- (1) The unescorted access authority of the individual to enter and be present in various areas of the airport;
  - (2) Control, use, and display of airport-approved access and identification media;
  - (3) Escort and challenge procedures and the law enforcement support for these procedures;
  - (4) Security responsibilities as specified in § 1540.105;
  - (5) Restrictions on divulging sensitive security information as described in part 1520 of this chapter; and
  - (6) Any other topics specified in the security program.
- (c) An airport operator may not authorize any individual unescorted access to the AOA, except as provided in § 1542.5, unless that individual has been provided information in accordance with the security program, including—
- (1) The unescorted access authority of the individual to enter and be present in various areas of the airport;
  - (2) Control, use, and display of airport-approved access and identification media, if appropriate;
  - (3) Escort and challenge procedures and the law enforcement support for these procedures, where applicable;
  - (4) Security responsibilities as specified in § 1540.105;
  - (5) Restrictions on divulging sensitive security information as described in part 1520 of this chapter; and
  - (6) Any other topics specified in the security program.
- (d) Each airport operator must maintain a record of all training and information given to each individual under paragraphs (b) and (c) of this section for 180 days after the termination of that person's unescorted access authority.
- (e) As to persons with unescorted access to the SIDA on November 14, 2001, training on responsibility under § 1540.105 can be provided by making relevant security information available.
- (f) Training described in paragraph (c) of this section must be implemented by each airport operator not later than November 14, 2002.

### § 1542.215 Law enforcement support.

- (a) In accordance with § 1542.217, each airport operator required to have a security program under § 1542.103(a) or (b) must provide:
  - (1) Law enforcement personnel in the number and manner adequate to support its security program.
  - (2) Uniformed law enforcement personnel in the number and manner adequate to support each system for screening persons and accessible property required under part 1544 or 1546 of this chapter, except to the extent that TSA provides Federal law enforcement support for the system.
- (b) Each airport required to have a security program under § 1542.103(c) must ensure that:
  - (1) Law enforcement personnel are available and committed to respond to an incident in support of a civil aviation security program when requested by an aircraft operator or foreign air carrier that has a security program under part 1544 or 1546 of this chapter.
  - (2) The procedures by which to request law enforcement support are provided to each aircraft operator or foreign air carrier that has a security program under part 1544 or 1546 of this chapter.

### § 1542.217 Law enforcement personnel.

- (a) Each airport operator must ensure that law enforcement personnel used to meet the requirements of § 1542.215, meet the following qualifications while on duty at the airport—
  - (1) Have arrest authority described in paragraph (b) of this section;
  - (2) Are identifiable by appropriate indicia of authority;
  - (3) Are armed with a firearm and authorized to use it; and
  - (4) Have completed a training program that meets the requirements of paragraphs (c) and (d) of this section.
- (b) Each airport operator must ensure that each individual used to meet the requirements of § 1542.215 have the authority to arrest, with or without a warrant, while on duty at the airport for the following violations of the criminal laws of the State and local jurisdictions in which the airport is located—
  - (1) A crime committed in the presence of the individual; and
  - (2) A felony, when the individual has reason to believe that the suspect has committed it.
- (c) The training program required by paragraph (a)(4) of this section must—
  - (1) Meet the training standard for law enforcement officers prescribed by either the State or local jurisdiction in which the airport is located for law enforcement officers performing comparable functions.
  - (2) Specify and require training standards for private law enforcement personnel acceptable to TSA, if the State and local jurisdictions in which the airport is located do not prescribe training standards for private law enforcement personnel that meets the standards in paragraph (a) of this section.
  - (3) Include training in—
    - (i) The use of firearms;

- (ii) The courteous and efficient treatment of persons subject to inspection, detention, search, arrest, and other aviation security activities;
  - (iii) The responsibilities of law enforcement personnel under the security program; and
  - (iv) Any other subject TSA determines is necessary.
- (d) Each airport operator must document the training program required by paragraph (a)(4) of this section and maintain documentation of training at a location specified in the security program until 180 days after the departure or removal of each person providing law enforcement support at the airport.

### **§ 1542.219 Supplementing law enforcement personnel.**

- (a) When TSA decides, after being notified by an airport operator as prescribed in this section, that not enough qualified State, local, and private law enforcement personnel are available to carry out the requirements of § 1542.215, TSA may authorize the airport operator to use, on a reimbursable basis, personnel employed by TSA, or by another department, agency, or instrumentality of the Government with the consent of the head of the department, agency, or instrumentality to supplement State, local, and private law enforcement personnel.
- (b) Each request for the use of Federal personnel must be submitted to TSA and include the following information:
- (1) The number of passengers enplaned at the airport during the preceding calendar year and the current calendar year as of the date of the request.
  - (2) The anticipated risk of criminal violence, sabotage, aircraft piracy, and other unlawful interference to civil aviation operations.
  - (3) A copy of that portion of the security program which describes the law enforcement support necessary to comply with § 1542.215.
  - (4) The availability of law enforcement personnel who meet the requirements of § 1542.217, including a description of the airport operator's efforts to obtain law enforcement support from State, local, and private agencies and the responses of those agencies.
  - (5) The airport operator's estimate of the number of Federal personnel needed to supplement available law enforcement personnel and the period of time for which they are needed.
  - (6) A statement acknowledging responsibility for providing reimbursement for the cost of providing Federal personnel.
  - (7) Any other information TSA considers necessary.
- (c) In response to a request submitted in accordance with this section, TSA may authorize, on a reimbursable basis, the use of personnel employed by a Federal agency, with the consent of the head of that agency.

### **§ 1542.221 Records of law enforcement response.**

- (a) Each airport operator must ensure that—
- (1) A record is made of each law enforcement action taken in furtherance of this part; and
  - (2) The record is maintained for a minimum of 180 days.

- (b) Data developed in response to paragraph (a) of this section must include at least the following, except as authorized by TSA:
  - (1) The number and type of weapons, explosives, or incendiaries discovered during any passenger-screening process, and the method of detection of each.
  - (2) The number of acts and attempted acts of aircraft piracy.
  - (3) The number of bomb threats received, real and simulated bombs found, and actual detonations on the airport.
  - (4) The number of arrests, including—
    - (i) Name, address, and the immediate disposition of each individual arrested;
    - (ii) Type of weapon, explosive, or incendiary confiscated, as appropriate; and
    - (iii) Identification of the aircraft operators or foreign air carriers on which the individual arrested was, or was scheduled to be, a passenger or which screened that individual, as appropriate.

## Subpart D—Contingency Measures

### § 1542.301 Contingency plan.

- (a) Each airport operator required to have a security program under § 1542.103(a) and (b) must adopt a contingency plan and must:
  - (1) Implement its contingency plan when directed by TSA.
  - (2) Conduct reviews and exercises of its contingency plan as specified in the security program with all persons having responsibilities under the plan.
  - (3) Ensure that all parties involved know their responsibilities and that all information contained in the plan is current.
- (b) TSA may approve alternative implementation measures, reviews, and exercises to the contingency plan which will provide an overall level of security equal to the contingency plan under paragraph (a) of this section.

### § 1542.303 Security Directives and Information Circulars.

- (a) TSA may issue an Information Circular to notify airport operators of security concerns. When TSA determines that additional security measures are necessary to respond to a threat assessment or to a specific threat against civil aviation, TSA issues a Security Directive setting forth mandatory measures.
- (b) Each airport operator must comply with each Security Directive issued to the airport operator within the time prescribed in the Security Directive.
- (c) Each airport operator that receives a Security Directive must—
  - (1) Within the time prescribed in the Security Directive, verbally acknowledge receipt of the Security Directive to TSA.
  - (2) Within the time prescribed in the Security Directive, specify the method by which the measures in the Security Directive have been implemented (or will be implemented, if the Security Directive is not yet effective).

- (d) In the event that the airport operator is unable to implement the measures in the Security Directive, the airport operator must submit proposed alternative measures and the basis for submitting the alternative measures to TSA for approval. The airport operator must submit the proposed alternative measures within the time prescribed in the Security Directive. The airport operator must implement any alternative measures approved by TSA.
- (e) Each airport operator that receives a Security Directive may comment on the Security Directive by submitting data, views, or arguments in writing to TSA. TSA may amend the Security Directive based on comments received. Submission of a comment does not delay the effective date of the Security Directive.
- (f) Each airport operator that receives a Security Directive or an Information Circular and each person who receives information from a Security Directive or an Information Circular must:
  - (1) Restrict the availability of the Security Directive or Information Circular, and information contained in either document, to those persons with an operational need-to-know.
  - (2) Refuse to release the Security Directive or Information Circular, and information contained in either document, to persons other than those who have an operational need to know without the prior written consent of TSA.

### § 1542.305 Public advisories.

When advised by TSA, each airport operator must prominently display and maintain in public areas information concerning foreign airports that, in the judgment of the Secretary of Transportation, do not maintain and administer effective security measures. This information must be posted in the manner specified in the security program and for such a period of time determined by the Secretary of Transportation.

### § 1542.307 Incident management.

- (a) Each airport operator must establish procedures to evaluate bomb threats, threats of sabotage, aircraft piracy, and other unlawful interference to civil aviation operations.
- (b) Immediately upon direct or referred receipt of a threat of any of the incidents described in paragraph (a) of this section, each airport operator must—
  - (1) Evaluate the threat in accordance with its security program;
  - (2) Initiate appropriate action as specified in the Airport Emergency Plan under 14 CFR 139.325; and
  - (3) Immediately notify TSA of acts, or suspected acts, of unlawful interference to civil aviation operations, including specific bomb threats to aircraft and airport facilities.
- (c) Airport operators required to have a security program under § 1542.103(c) but not subject to 14 CFR part 139, must develop emergency response procedures to incidents of threats identified in paragraph (a) of this section.
- (d) To ensure that all parties know their responsibilities and that all procedures are current, at least once every 12 calendar months each airport operator must review the procedures required in paragraphs (a) and (b) of this section with all persons having responsibilities for such procedures.

**Assembly Bill No. 1522**

## CHAPTER 317

An act to amend Section 2810.5 of, and to add Article 1.5 (commencing with Section 245) to Chapter 1 of Part 1 of Division 2 of, the Labor Code, relating to employment.

[Approved by Governor September 10, 2014. Filed with Secretary of State September 10, 2014.]

## LEGISLATIVE COUNSEL'S DIGEST

AB 1522, Gonzalez. Employment: paid sick days.

Existing law authorizes employers to provide their employees paid sick leave.

This bill would enact the Healthy Workplaces, Healthy Families Act of 2014 to provide that an employee who, on or after July 1, 2015, works in California for 30 or more days within a year from the commencement of employment is entitled to paid sick days for prescribed purposes, to be accrued at a rate of no less than one hour for every 30 hours worked. An employee would be entitled to use accrued sick days beginning on the 90th day of employment. The bill would authorize an employer to limit an employee's use of paid sick days to 24 hours or 3 days in each year of employment. The bill would prohibit an employer from discriminating or retaliating against an employee who requests paid sick days. The bill would require employers to satisfy specified posting and notice and recordkeeping requirements. The bill would define terms for those purposes.

The bill would require the Labor Commissioner to enforce these requirements, including the investigation, mitigation, and relief of violations of these requirements. The bill would authorize the Labor Commissioner to impose specified administrative fines for violations and would authorize the commissioner or the Attorney General to recover specified civil penalties against an offender who violated these provisions on behalf of the aggrieved, as well as attorney's fees, costs, and interest.

The bill would not apply to certain categories of employees that meet specified requirements.

*The people of the State of California do enact as follows:*

## SECTION 1.

The Legislature finds and declares the following:

(a) Nearly every worker in the State of California will at some time during the year need some time off from work to take care of his or her own health or the health of family members.

(b) Many workers in California do not have any paid sick days, or have an inadequate number of paid sick days, to care for their own health or the health of family members.

(c) Low-income workers are significantly less likely to have paid sick time than other workers.

(d) Providing workers time off to attend to their own health care and the health care of family members will ensure a healthier and more productive workforce in California.

(e) Paid sick days will have an enormously positive impact on the public health of Californians by allowing sick workers paid time off to care for themselves when ill, thus lessening their recovery time and reducing the likelihood of spreading illness to other members of the workforce.

(f) Paid sick days will allow parents to provide personal care for their sick children. Parental care ensures children's speedy recovery, prevents more serious illnesses, and improves children's overall mental and physical health.

(g) Providing paid sick days is affordable for employers and good for business.

(h) Employers who provide paid sick days enjoy greater employee retention and reduce the likelihood of employees coming to work sick. Studies have shown that costs



of decreased productivity caused by sick workers exceed the costs of employee absenteeism. Attachment D

(i) Many adults have significant elder care responsibilities requiring them to take time off from work or to work reduced hours.

(j) Employees frequently lose their jobs or are disciplined for taking sick days to care for sick family members or to recover from their own illnesses.

(k) Workers whose jobs involve significant contact with the public, such as service workers and restaurant workers, are very unlikely to have paid sick days. Often, these workers have no choice but to come to work when they are ill, thereby spreading illness to coworkers and customers.

(l) Domestic violence and sexual assault affect many persons without regard to age, race, national origin, sexual orientation, or socioeconomic status.

(m) Domestic violence is a crime that has a devastating effect on families, communities, and the workplace. It impacts productivity, effectiveness, absenteeism, and employee turnover in the workplace. The National Crime Survey estimates that 175,000 days of work each year are missed due to domestic violence.

(n) Survivors of domestic violence and sexual assault may be vulnerable at work when trying to end an abusive relationship because the workplace may be the only place where the perpetrator knows to contact the victim. Studies show that up to one-half of domestic violence victims experience job loss. Forty percent reported on-the-job harassment. Nearly 50 percent of sexual assault survivors lose their jobs or are forced to quit in the aftermath of the assaults.

(o) Affording survivors of domestic violence and sexual assault paid sick days is vital to their independence and recovery.

#### SEC. 2.

In enacting this act, it is the intent of the Legislature to do the following:

(a) Ensure that workers in California can address their own health needs and the health needs of their families by requiring employers to provide a minimum level of paid sick days including time for family care.

(b) Decrease public and private health care costs in California by enabling workers to seek early and routine medical care for themselves and their family members and to address domestic violence or sexual assault.

(c) Protect employees in California from losing their jobs while they use sick days to care for themselves or their families.

(d) Provide economic security to employees in California who take time off from work for reasons related to domestic violence or sexual assault.

(e) Safeguard the welfare, health, safety, and prosperity of the people of and visitors to California.

#### SEC. 3.

Article 1.5 (commencing with Section 245) is added to Chapter 1 of Part 1 of Division 2 of the Labor Code, to read:

### Article 1.5. Paid Sick Days

#### 245.

(a) This article shall be known and may be cited as the Healthy Workplaces, Healthy Families Act of 2014.

(b) The provisions of this article are in addition to and independent of any other rights, remedies, or procedures available under any other law and do not diminish, alter, or negate any other legal rights, remedies, or procedures available to an aggrieved person.

#### 245.5.

As used in this article:

(a) "Employee" does not include the following:

(1) An employee covered by a valid collective bargaining agreement if the agreement expressly provides for the wages, hours of work, and working conditions of employees, and expressly provides for paid sick days or a paid leave or paid time off policy that permits the use of sick days for those employees, final and binding arbitration of

disputes concerning the application of its paid sick days provisions, premium wage rates for all overtime hours worked, and regular hourly rate of pay of not less than 30 percent more than the state minimum wage rate.

(2) An employee in the construction industry covered by a valid collective bargaining agreement if the agreement expressly provides for the wages, hours of work, and working conditions of employees, premium wage rates for all overtime hours worked, and regular hourly pay of not less than 30 percent more than the state minimum wage rate, and the agreement either (A) was entered into before January 1, 2015, or (B) expressly waives the requirements of this article in clear and unambiguous terms. For purposes of this subparagraph, "employee in the construction industry" means an employee performing onsite work associated with construction, including work involving alteration, demolition, building, excavation, renovation, remodeling, maintenance, improvement, repair work, and any other work as described by Chapter 9 (commencing with Section 7000) of Division 3 of the Business and Professions Code, and other similar or related occupations or trades.

(3) A provider of in-home supportive services under Section 14132.95, 14132.952, or 14132.956 of, or Article 7 (commencing with Section 12300) of Chapter 3 of Part 3 of Division 9 of, the Welfare and Institutions Code.

(4) An individual employed by an air carrier as a flight deck or cabin crew member that is subject to the provisions of Title II of the federal Railway Labor Act (45 U.S.C. 181 et seq.), provided that the individual is provided with compensated time off equal to or exceeding the amount established in paragraph (1) of subdivision (b) of Section 246.

(b) "Employer" means any person employing another under any appointment or contract of hire and includes the state, political subdivisions of the state, and municipalities.

(c) "Family member" means any of the following:

(1) A child, which for purposes of this article means a biological, adopted, or foster child, stepchild, legal ward, or a child to whom the employee stands in loco parentis. This definition of a child is applicable regardless of age or dependency status.

(2) A biological, adoptive, or foster parent, stepparent, or legal guardian of an employee or the employee's spouse or registered domestic partner, or a person who stood in loco parentis when the employee was a minor child.

(3) A spouse.

(4) A registered domestic partner.

(5) A grandparent.

(6) A grandchild.

(7) A sibling.

(d) "Health care provider" has the same meaning as defined in paragraph (6) of subdivision (c) of Section 12945.2 of the Government Code.

(e) "Paid sick days" means time that is compensated at the same wage as the employee normally earns during regular work hours and is provided by an employer to an employee for the purposes described in Section 246.5.

246.

(a) An employee who, on or after July 1, 2015, works in California for 30 or more days within a year from the commencement of employment is entitled to paid sick days as specified in this section.

(b) (1) An employee shall accrue paid sick days at the rate of not less than one hour per every 30 hours worked, beginning at the commencement of employment or the operative date of this article, whichever is later.

(2) An employee who is exempt from overtime requirements as an administrative, executive, or professional employee under a wage order of the Industrial Welfare Commission is deemed to work 40 hours per workweek for the purposes of this section, unless the employee's normal workweek is less than 40 hours, in which case the employee shall accrue paid sick days based upon that normal workweek.

(c) An employee shall be entitled to use accrued paid sick days beginning on the 90th day of employment, after which day the employee may use paid sick days as they are accrued.

(d) Accrued paid sick days shall carry over to the following year of employment. However, an employer may limit an employee's use of paid sick days to 24 hours or three days in each year of employment. This section shall be satisfied and no accrual or carry over is required if the full amount of leave is received at the beginning of each year, in accordance with subdivision (e).

(e) An employer is not required to provide additional paid sick days pursuant to this section if the employer has a paid leave policy or paid time off policy, the employer makes available an amount of leave that may be used for the same purposes and under the same conditions as specified in this section, and the policy does either of the following:

(1) Satisfies the accrual, carry over, and use requirements of this section.

(2) Provides no less than 24 hours or three days of paid sick leave, or equivalent paid leave or paid time off, for employee use for each year of employment or calendar year or 12-month basis.

(f) (1) Except as specified in paragraph (2), an employer is not required to provide compensation to an employee for accrued, unused paid sick days upon termination, resignation, retirement, or other separation from employment.

(2) If an employee separates from an employer and is rehired by the employer within one year from the date of separation, previously accrued and unused paid sick days shall be reinstated. The employee shall be entitled to use those previously accrued and unused paid sick days and to accrue additional paid sick days upon rehiring.

(g) An employer may lend paid sick days to an employee in advance of accrual, at the employer's discretion and with proper documentation.

(h) An employer shall provide an employee with written notice that sets forth the amount of paid sick leave available, or paid time off leave an employer provides in lieu of sick leave, for use on either the employee's itemized wage statement described in Section 226 or in a separate writing provided on the designated pay date with the employee's payment of wages. The penalties described in this article for a violation of this subdivision shall be in lieu of the penalties for a violation of Section 226.

(i) An employer has no obligation under this section to allow an employee's total accrual of paid sick leave to exceed 48 hours or 6 days, provided that an employee's rights to accrue and use paid sick leave under this section are not otherwise limited.

(j) An employee may determine how much paid sick leave he or she needs to use, provided that an employer may set a reasonable minimum increment, not to exceed two hours, for the use of paid sick leave.

(k) The rate of pay shall be the employee's hourly wage. If the employee in the 90 days of employment before taking accrued sick leave had different hourly pay rates, was paid by commission or piece rate, or was a nonexempt salaried employee, then the rate of pay shall be calculated by dividing the employee's total wages, not including overtime premium pay, by the employee's total hours worked in the full pay periods of the prior 90 days of employment.

(l) If the need for paid sick leave is foreseeable, the employee shall provide reasonable advance notification. If the need for paid sick leave is unforeseeable, the employee shall provide notice of the need for the leave as soon as practicable.

(m) An employer shall provide payment for sick leave taken by an employee no later than the payday for the next regular payroll period after the sick leave was taken.

246.5.

(a) Upon the oral or written request of an employee, an employer shall provide paid sick days for the following purposes:

(1) Diagnosis, care, or treatment of an existing health condition of, or preventive care for, an employee or an employee's family member.

(2) For an employee who is a victim of domestic violence, sexual assault, or stalking, the purposes described in subdivision (c) of Section 230 and subdivision (a) of Section 230.1.

(b) An employer shall not require as a condition of using paid sick days that the employee search for or find a replacement worker to cover the days during which the employee uses paid sick days.

(c) (1) An employer shall not deny an employee the right to use accrued sick days, discharge, threaten to discharge, demote, suspend, or in any manner discriminate against an employee for using accrued sick days, attempting to exercise the right to use accrued sick days, filing a complaint with the department or alleging a violation of this article, cooperating in an investigation or prosecution of an alleged violation of this article, or opposing any policy or practice or act that is prohibited by this article.

(2) There shall be a rebuttable presumption of unlawful retaliation if an employer denies an employee the right to use accrued sick days, discharges, threatens to discharge, demotes, suspends, or in any manner discriminates against an employee within 30 days of any of the following:

(A) The filing of a complaint by the employee with the Labor Commissioner or alleging a violation of this article.

(B) The cooperation of an employee with an investigation or prosecution of an alleged violation of this article.

(C) Opposition by the employee to a policy, practice, or act that is prohibited by this article.

247.

(a) In each workplace of the employer, the employer shall display a poster in a conspicuous place containing all the information specified in subdivision (b). The Labor Commissioner shall create a poster containing this information and make it available to employers.

(b) The poster shall state all of the following:

(1) An employee is entitled to accrue, request, and use paid sick days.

(2) The amount of sick days provided for by this article.

(3) The terms of use of paid sick days.

(4) That retaliation or discrimination against an employee who requests paid sick days or uses paid sick days, or both, is prohibited and that an employee has the right under this article to file a complaint with the Labor Commissioner against an employer who retaliates or discriminates against the employee.

(c) An employer who willfully violates the posting requirements of this section is subject to a civil penalty of not more than one hundred dollars (\$100) per each offense.

247.5.

An employer shall keep for at least three years records documenting the hours worked and paid sick days accrued and used by an employee, and shall allow the Labor Commissioner to access these records pursuant to the requirements set forth in Section 1174. An employer shall make these records available to an employee in the same manner as described in Section 226. If an employer does not maintain adequate records pursuant to this section, it shall be presumed that the employee is entitled to the maximum number of hours accruable under this article, unless the employer can show otherwise by clear and convincing evidence.

248.5.

(a) The Labor Commissioner shall enforce this article, including investigating an alleged violation, and ordering appropriate temporary relief to mitigate the violation or to maintain the status quo pending the completion of a full investigation or hearing.

(b) (1) If the Labor Commissioner, after a hearing that contains adequate safeguards to ensure that the parties are afforded due process, determines that a violation of this article has occurred, he or she may order any appropriate relief, including reinstatement, backpay, the payment of sick days unlawfully withheld, and the payment of an additional sum in the form of an administrative penalty to an employee or other person whose rights under this article were violated.

(2) If paid sick days were unlawfully withheld, the dollar amount of paid sick days withheld from the employee multiplied by three, or two hundred fifty dollars (\$250), whichever amount is greater, but not to exceed an aggregate penalty of four thousand dollars (\$4,000), shall be included in the administrative penalty.

(3) If a violation of this article results in other harm to the employee or person, such as discharge from employment, or otherwise results in a violation of the rights of the employee or person, the administrative penalty shall include a sum of fifty dollars (\$50)

for each day or portion thereof that the violation occurred or continued, not to exceed an aggregate penalty of four thousand dollars (\$4,000).

(c) Where prompt compliance by an employer is not forthcoming, the Labor Commissioner may take any appropriate enforcement action to secure compliance, including the filing of a civil action. In compensation to the state for the costs of investigating and remedying the violation, the commissioner may order the violating employer to pay to the state a sum of not more than fifty dollars (\$50) for each day or portion of a day a violation occurs or continues for each employee or other person whose rights under this article were violated.

(d) An employee or other person may report to the Labor Commissioner a suspected violation of this article. The commissioner shall encourage reporting pursuant to this subdivision by keeping confidential, to the maximum extent permitted by applicable law, the name and other identifying information of the employee or person reporting the violation. However, the commissioner may disclose that person's name and identifying information as necessary to enforce this article or for other appropriate purposes, upon the authorization of that person.

(e) The Labor Commissioner or the Attorney General may bring a civil action in a court of competent jurisdiction against the employer or other person violating this article and, upon prevailing, shall be entitled to collect legal or equitable relief on behalf of the aggrieved as may be appropriate to remedy the violation, including reinstatement, backpay, the payment of sick days unlawfully withheld, the payment of an additional sum, not to exceed an aggregate penalty of four thousand dollars (\$4,000), as liquidated damages in the amount of fifty dollars (\$50) to each employee or person whose rights under this article were violated for each day or portion thereof that the violation occurred or continued, plus, if the employer has unlawfully withheld paid sick days to an employee, the dollar amount of paid sick days withheld from the employee multiplied by three; or two hundred fifty dollars (\$250), whichever amount is greater; and reinstatement in employment or injunctive relief; and further shall be awarded reasonable attorney's fees and costs, provided, however, that any person or entity enforcing this article on behalf of the public as provided for under applicable state law shall, upon prevailing, be entitled only to equitable, injunctive, or restitutionary relief, and reasonable attorney's fees and costs.

(f) In an administrative or civil action brought under this article, the Labor Commissioner or court, as the case may be, shall award interest on all amounts due and unpaid at the rate of interest specified in subdivision (b) of Section 3289 of the Civil Code.

(g) The remedies, penalties, and procedures provided under this article are cumulative.

(h) An employer shall not be assessed any penalty or liquidated damages under this article due to an isolated and unintentional payroll error or written notice error that is a clerical or an inadvertent mistake regarding the accrual or available use of paid sick leave. In reviewing for compliance with this section, the factfinder may consider as a relevant factor whether the employer, prior to an alleged violation, has adopted and is in compliance with a set of policies, procedures, and practices that fully comply with this section.

249.

(a) This article does not limit or affect any laws guaranteeing the privacy of health information, or information related to domestic violence or sexual assault, regarding an employee or employee's family member. That information shall be treated as confidential and shall not be disclosed to any person except to the affected employee, or as required by law.

(b) This article shall not be construed to discourage or prohibit an employer from the adoption or retention of a paid sick days policy more generous than the one required herein.

(c) This article does not lessen the obligation of an employer to comply with a contract, collective bargaining agreement, employment benefit plan, or other agreement providing more generous sick days to an employee than required herein.

(d) This article establishes minimum requirements pertaining to paid sick days and does not preempt, limit, or otherwise affect the applicability of any other law, regulation, requirement, policy, or standard that provides for greater accrual or use by employees of sick days, whether paid or unpaid, or that extends other protections to an employee.

SEC. 4.

Section 2810.5 of the Labor Code is amended to read:

2810.5.

(a) (1) At the time of hiring, an employer shall provide to each employee a written notice, in the language the employer normally uses to communicate employment-related information to the employee, containing the following information:

(A) The rate or rates of pay and basis thereof, whether paid by the hour, shift, day, week, salary, piece, commission, or otherwise, including any rates for overtime, as applicable.

(B) Allowances, if any, claimed as part of the minimum wage, including meal or lodging allowances.

(C) The regular payday designated by the employer in accordance with the requirements of this code.

(D) The name of the employer, including any "doing business as" names used by the employer.

(E) The physical address of the employer's main office or principal place of business, and a mailing address, if different.

(F) The telephone number of the employer.

(G) The name, address, and telephone number of the employer's workers' compensation insurance carrier.

(H) That an employee: may accrue and use sick leave; has a right to request and use accrued paid sick leave; may not be terminated or retaliated against for using or requesting the use of accrued paid sick leave; and has the right to file a complaint against an employer who retaliates.

(I) Any other information the Labor Commissioner deems material and necessary.

(2) The Labor Commissioner shall prepare a template that complies with the requirements of paragraph (1). The template shall be made available to employers in such manner as determined by the Labor Commissioner.

(3) If the employer is a temporary services employer, as defined in Section 201.3, the notice described in paragraph (1) must also include the name, the physical address of the main office, the mailing address if different from the physical address of the main office, and the telephone number of the legal entity for whom the employee will perform work, and any other information the Labor Commissioner deems material and necessary. The requirements of this paragraph do not apply to a security services company that is licensed by the Department of Consumer Affairs and that solely provides security services.

(b) An employer shall notify his or her employees in writing of any changes to the information set forth in the notice within seven calendar days after the time of the changes, unless one of the following applies:

(1) All changes are reflected on a timely wage statement furnished in accordance with Section 226.

(2) Notice of all changes is provided in another writing required by law within seven days of the changes.

(c) For purposes of this section, "employee" does not include any of the following:

(1) An employee directly employed by the state or any political subdivision thereof, including any city, county, city and county, or special district.

(2) An employee who is exempt from the payment of overtime wages by statute or the wage orders of the Industrial Welfare Commission.

(3) An employee who is covered by a valid collective bargaining agreement if the agreement expressly provides for the wages, hours of work, and working conditions of the employee, and if the agreement provides premium wage rates for all overtime hours worked and a regular hourly rate of pay for those employees of not less than 30 percent more than the state minimum wage.

O