Transportation Security Administration

ENFORCEMENT SANCTION GUIDANCE POLICY
(date updated: 14 November 2022)

INTRODUCTION: On November 19, 2001, Congress enacted the Aviation and Transportation Security Act (ATSA), which created TSA, and which transferred authority for enforcement of civil aviation security requirements from the Federal Aviation Administration to TSA. On July 21, 2009, TSA's Investigative and Enforcement Procedures, including the maximum civil monetary penalty amounts for violations of TSA's security regulations, were amended to conform to the Implementing Recommendations of the 9/11 Commission Act of 2007. On November 2, 2015, Congress enacted the Civil Penalties Inflation Adjustment Act Improvements Act of 2015, which required federal agencies to make annual inflation adjustments to civil penalties.

PURPOSE: This sanctions policy provides guidance for imposing civil monetary penalties up to $37,377 per violation for aircraft operators, up to $12,794 per violation for surface transportation modes and other non-aviation violations, and up to $14,950 per violation for all other persons, including but not limited to individuals, airport operators, indirect air carriers, and small business concerns. This sanction guidance provides agency enforcement personnel with guidance in selecting appropriate sanctions for civil penalty enforcement actions and to promote consistency in enforcement of TSA regulations; it does not restrict TSA from proposing higher penalties or penalties for violations not listed in the Sanction Guidance Table. The purpose of this guidance is to assist, not replace, the exercise of judgment in determining the appropriate civil penalty in a particular case. TSA has the authority to issue civil penalties up to the administrative maximums found in 49 C.F.R. § 1503.401, which may undergo annual inflation adjustment more frequently than this sanctions policy is updated.

GENERAL GUIDELINES: The Sanction Guidance Table ("Table") below represents the normal sanction range for a single violation of a particular regulation. Pursuant to a philosophy of progressive enforcement, the sanction generally increases with each repeated violation or based upon other aggravating factors. In selecting an appropriate sanction, TSA considers the totality of circumstances, including any aggravating and mitigating factors. A sanction amount at the higher end of a range is appropriate where there are aggravating factors surrounding the violation, while a sanction amount at the lower end of the range is appropriate for first time violations and where mitigating factors exist. Based on substantial aggravating or mitigating factors, TSA may seek a sanction amount that falls outside the Table's sanction ranges.

Transportation Security Administration

AGGRAVATING and MITIGATING FACTORS: As a general matter, TSA considers the following aggravating and mitigating factors:

1. Significance or degree of the security risk created by the violation;
2. Nature of the violation (whether the violation was inadvertent, deliberate, or the result of gross negligence);
3. Past violation history (compliance should be the norm, this factor is considered only to assess the need for an increased sanction);
4. Violator's level of experience;
5. Attitude of violator, including the nature of any corrective action taken by the alleged violator;
6. Economic impact of the civil penalty on the violator;
7. Criminal sanctions already paid for the same incident;
8. Disciplinary action by the violator's employer for the same incident;
9. Artful concealment; and
10. Fraud and intentional falsification.
11. For violations related to firearms, additional aggravating factors include:
    A. The violator is a member of the Known Crewmember® (KCM) Program using a KCM portal
    B. The violator is a crew member in uniform using a passenger checkpoint
    C. The violator is a member of TSA Pre√®
    D. A repeat firearm violation ("past violation history")
    E. The firearm was carried on the violator's person
    F. The firearm has a round that is chambered or the safety is off (loaded firearms carry a separate, higher penalty to unloaded firearms)

INDIVIDUALS: Section VI below addresses sanction amounts for individual violations. Penalty considerations for violations by individuals, who are not regulated entities or employed by a regulated entity, differ from the considerations for regulated entities such as an aircraft operator, airport, or indirect air carrier. Deterrence against an individual generally does not require a penalty range as high as that against a regulated entity. As a result, the Table contains ranges that list dollar amounts for violations by individuals. Egregious or intentional violations may support a civil penalty outside of the listed range. Reduced civil penalties allowed under the Notice of Violation (NOV) program are a program incentive and are not based on the typical mitigating factors.

SMALL BUSINESS ENTITIES: The maximum civil penalty that may be assessed against a violator that qualifies as a small business entity is $14,950 (freight and passenger rail is $12,794). TSA may consider the fact that the entity qualifies as a small business in determining the appropriate amount of the civil penalty. This information may not be readily available prior to the issuance of a proposed civil penalty and may be considered at any time after the initiation of enforcement action. Generally, it is the responsibility of the alleged violator to provide reliable evidence of its inability to pay a proposed civil penalty or of the impact the civil penalty it will have on its ability to continue in business.

MULTIPLE VIOLATIONS: Where multiple violations arise from the same incident, inspection, or investigation, a sanction amount generally should be calculated for each violation of the regulations. Similarly, a separate sanction amount generally should be assessed for each violation where there are continuing violations or related violations addressed in the same case.

CRIMINAL REFERRAL: Referral for criminal investigation and enforcement is appropriate where there appears to be a violation of criminal laws. Criminal penalties and fines are different and wholly separate from the civil penalties assessed by TSA. Withdrawal of criminal charges will not affect civil penalty charges, and vice versa.

Transportation Security Administration

TABLE RANGES: The Table describes civil monetary penalties as minimum, moderate, or maximum for a single violation of a particular regulation. These terms are defined as follows:

(1) Violations Committed by Aircraft Operators/Air Carriers
Maximum $26,900-$37,377
Moderate $13,400-$26,900
Minimum $4,500-$13,400

(2) Violations Committed by owners/operators of freight Rail Carriers, Rail-Sensitive Security Material (RSSM) Shippers, and Receivers; and Violations Committed by Public Transportation and Passenger Rail, and Over-the-road Bus companies. Other Non-Aviation Violations
Maximum $7,600-$12,794
Moderate $3,900-$7,600
Minimum $1,230-$3,900

(3) Violations Committed by All Other Entities Including, but Not Limited to Airport Operators, Indirect Air Carrier, CCSFs, Individuals, Contractors, Small Businesses, etc.
Maximum $11,290-$14,950
Moderate $5,900-$11,290
Minimum $1,450-$5,900

Transportation Security Administration

SANCTION GUIDANCE TABLE

I. AIRPORT OPERATOR*

1.	Failure to ensure that Airport Security Coordinator (ASC) fulfills required functions	Min.
2.	Failure to train ASC	Min.-Mod.
3.	Failure to allow TSA inspection	Max.
4.	Failure to provide evidence of regulatory compliance	Max.
5.	Failure to provide SIDA access ID to TSA personnel	Mod.
6.	Failure to carry out a requirement in the security program (general violation to be used when more specific violation is not listed)	Mod.-Max.
7.	Failure to restrict the distribution, disclosure of SSI	Min.-Max.
8.	Failure to notify TSA of changes to its security program	Min.
9.	Access control violations – Secured area, AOA, SIDA, and access control systems	Max.
10.	Failure to follow escort procedures	Mod.
11.	Failure to train or to maintain training records	Min.-Mod.
12.	Criminal history records check – Failure to perform, failure to suspend, failure to investigate charges	Max.
13.	Failure to maintain record of law enforcement response	Min.-Mod.
14.	Failure to implement a Security Directive	Max.
15.	False entry in record or report	Max. + Criminal Referral
16.	Failure to comply with requirements related to adequate law enforcement response/support	Max.
17.	Failure to follow accountability procedures for personnel identification systems	Max.

*Airport tenants operating under valid Exclusive Area Agreements assume responsibility for certain airport operator security responsibilities. For violations of security requirements assumed by such airport tenants, the airport operator section of the sanction guidance should be employed.

18. Cybersecurity Coordinator

Failure to designate a qualified Cybersecurity Coordinator and at least one alternate	Max.
Failure to provide Cybersecurity Coordinator contact information	Min.-Mod.

19. Reporting Cybersecurity Incidents

Failure to report a cybersecurity incident to CISA within the specified time frame	Min.-Mod.
Failure to include required information in report to CISA	Min.

20. Cybersecurity Implementation Plan

Operating without a TSA-approved Cybersecurity Implementation Plan	Max.
Failure to identify a Critical Cyber System	Max.
Failure to comply with a network segmentation policy or control as described in TSA-approved Cybersecurity Implementation Plan	Mod.-Max.
Failure to comply with an access control measure as described in TSA-approved Cybersecurity Implementation Plan	Mod.-Max.
Failure to comply with a continuous monitoring and detection policy or procedure as described in TSA-approved Cybersecurity Implementation Plan	Mod.-Max.
Failure to comply with a mitigation measure or manual control, as described in TSA-approved Cybersecurity Implementation Plan, implemented to ensure that industrial control systems can be isolated when a cybersecurity incident in the Information Technology system creates a risk to the safety and reliability of the Operational Technology system	Max.
Failure to apply a security patch or update consistent with the risk-based methodology described in TSA-approved Cybersecurity Implementation Plan	Max.
Failure to submit a request to amend TSA-approved Cybersecurity Implementation Plan in the event of a change in ownership or control of operations or a change in conditions affecting security	Min.-Mod.

21. Cybersecurity Incident Response Plan

Failure to have a Cybersecurity Incident Response Plan	Max.
Failure to include a required piece of information in a Cybersecurity Incident Response Plan	Mod.-Max.

22. Cybersecurity Assessment Program

Failure to submit the annual plan for the Cybersecurity Assessment Program	Mod.-Max.
Failure to include a required piece of information in the annual plan for the Cybersecurity Assessment Program	Mod.-Max.

23. Cybersecurity Self-Assessment

Failure to conduct a cybersecurity assessment and develop remediation measures	Mod.-Max.
Failure to submit a completed vulnerability assessment form and remediation measures to TSA within the specified timeframe	Mod.-Max.

II. AIRCRAFT OPERATOR AND AIR CARRIER

1. Failure to carry out security program (covers all violations of security program requirements; general violation to be used if more specific violation is not listed in the Table)	Mod.-Max.
2. Failure to allow TSA inspection	Max.
3. Failure to provide evidence of regulatory compliance	Max.
4. Failure to provide SIDA access ID to TSA personnel	Mod.
5. Failure to restrict distribution and disclosure of security program	Mod.-Max.
6. Failure to comply with a security requirement pertaining to the acceptance, control, or screening of checked baggage	Max. per piece
7. Failure to comply with a security requirement pertaining to the acceptance, control, or screening of cargo	Max.
7b. Failure to screen cargo: unscreened cargo flew on passenger aircraft	Max. per piece
7c. Failure to screen cargo: unscreened cargo did not fly on passenger aircraft because of inspector intervention	Min. per piece
8. Failure to comply with requirements for carriage of an accessible weapon by an armed LEO	Mod.
9. Failure to prevent unauthorized access to secured area or to aircraft	Max.
10. Failure to conduct a security inspection of aircraft	Mod.-Max.
11. Failure to comply with criminal history records check requirements	Max.

12. Failure to comply with requirements for aircraft operator-issued identification and access media	Mod.
13. Failure to train or to maintain training records	Min.-Mod.
14. Failure to comply with Security Directives or Emergency Amendment	Max.
15. Failure to comply with security requirements related to screening of passengers and/or property (excluding cargo)	Mod.-Max.
16. False entry in record or report	Max. + Criminal Referral
17. Failure to transport Federal Air Marshals	Max.
18. Failure to pay security fees	Mod.
19. No-Fly List and Selectee List violations	Max.
20. Failure to provide adequate rest areas for CCSP-K9 teams screening cargo	Max.
21. Cybersecurity Coordinator	
Failure to designate a qualified Cybersecurity Coordinator and at least one alternate	Max.
Failure to provide Cybersecurity Coordinator contact information	Min.-Mod.
22. Reporting Cybersecurity Incidents	
Failure to report a cybersecurity incident to CISA within the specified timeframe	Min.-Mod.
Failure to include required information in report to CISA	Min.
23. Cybersecurity Implementation Plan	
Operating without a TSA-approved Cybersecurity Implementation Plan	Max.
Failure to identify a Critical Cyber System	Max.
Failure to comply with a network segmentation policy or control as described in TSA-approved Cybersecurity Implementation Plan	Mod.-Max.
Failure to comply with an access control measure as described in TSA-approved Cybersecurity Implementation Plan	Mod.-Max.
Failure to comply with a continuous monitoring and detection policy or procedure as described in TSA-approved Cybersecurity Implementation Plan	Mod.-Max.

Failure to comply with a mitigation measure or manual control, as described in TSA-approved Cybersecurity Implementation Plan, implemented to ensure that industrial control systems can be isolated when a cybersecurity incident in the Information Technology system creates a risk to the safety and reliability of the Operational Technology system	Max.
Failure to apply a security patch or update consistent with the risk-based methodology described in TSA-approved Cybersecurity Implementation Plan	Max.
Failure to submit a request to amend TSA-approved Cybersecurity Implementation Plan in the event of a change in ownership or control of operations or a change in conditions affecting security	Min.-Mod.

24. Cybersecurity Incident Response Plan

Failure to have a Cybersecurity Incident Response Plan	Max.
Failure to include a required piece of information in a Cybersecurity Incident Response Plan	Mod.-Max.

25. Cybersecurity Assessment Program

Failure to submit the annual plan for the Cybersecurity Assessment Program	Mod.-Max.
Failure to include a required piece of information in the annual plan for the Cybersecurity Assessment Program	Mod.-Max.

26. Cybersecurity Self-Assessment

Failure to conduct a cybersecurity assessment and develop remediation measures	Mod.-Max.
Failure to submit a completed vulnerability assessment form and remediation measures to TSA within the specified timeframe	Mod.-Max.

III. OTHER AVIATION SECURITY REQUIREMENTS

Part 1550:

Failure to comply with a security requirement set forth in, or pursuant to, 49 C.F.R. part 1550	Max.

Transportation Security Administration

Part 1552 (Flight Training Providers):

Failure to comply with any requirement issued pursuant to 49 U.S.C. § 44939 and set forth in 49 C.F.R. part 1552	Mod.-Max.

Flight training providers that are also aircraft operators are subject to a civil penalty maximum of up to $37,377 per violation. Flight training providers that are not aircraft operators are subject to a civil penalty maximum of up to $14,950 per violation.

Failure to provide flight training without TSA approval	Max.
Failure to determine/record citizenship status	Mod.-Max.
Failure to obtain candidate photograph	Mod.
Failure to provide security awareness training	Mod.

Part 1562 (Subpart A):

(ASC) Failure to carry out its security procedures (General violation to be used when more specific violation is not listed)	Mod.-Max.
(ASC) Failure to allow TSA inspection	Mod.-Max.
(ASC) Failure to monitor the security of aircraft at the airport during operational and non-operational hours	Mod.-Max.
(ASC) Failure to report unsecured aircraft	Min.-Mod.
(Pilot) Failure to protect from unauthorized disclosure any identification information issued by TSA (i.e., TSA-Issued Personal Identification Number (PIN))	Mod.-Max.
(Pilot) Failure to secure the aircraft after returning to a MD3 airport	Mod.-Max.
(Pilot) Failure to comply with air traffic instructions as required by the FAA	Mod.-Max.
(ASC and Pilot) Failure to report to TSA within 24 hours a conviction or found not guilty by reason of insanity any crime specified in 49 CFR § 1542.209 or 49 C.F.R § 1572.103	Mod.-Max.
(Pilot) Failure to report to TSA within 24 hours any violation described in 49 CFR § 1562.3(e)(5)	Mod.

Part 1562 (Subpart B):

(Aircraft Operator) Failure to carry out its security program (General violation to be used when more specific violation is not listed)	Mod.-Max.
(Aircraft Operator) Failure to ensure each crewmember meets the requirements to operate into/out of DCA	Mod.-Max.

(Aircraft Operator) Failure to comply with additional security procedures required by TSA through order, Security Directive, or other means	Max.
(Flight Crew Member) Possession of a violation record on file with the FAA of airspace identified in 49 CFR §§ 1562.23(c)(2)(i) through 1562.23(c)(2)(vii)	Max.
(Aircraft Operator) Failure to notify the National Capital Region Coordination Center (NCRCC) prior to departure of the aircraft DCA or a gateway airport	Max.
(Aircraft Operator) Failure to allow TSA inspection	Max.
(FBO) Failure to carry out the FBO Standard Security Program	Mod.-Max.
(FBO) Failure to allow TSA inspection	Mod.-Max.

49 USC 46301(a)(6):

Failure to collect airport security badges (by employees other than government or airport operators)	Max.

IV. CARGO SECURITY

This part applies to all persons who offer, accept, or transport cargo pursuant to a TSA-approved security program and/or subject to the requirements of the Transportation Security Regulations. Such persons include, but are not limited to, Certified Cargo Screening Facilities (CCSF) and indirect air carriers (IACs).

1.	Acting as an IAC without an approved program	Max.
2.	Failure to provide evidence of regulatory compliance	Max.
3.	Failure to retain or produce training records	Min.-Mod.
4.	Failure to provide required training	Mod.
5.	Failure to inform agent in writing of responsibilities under the program	Mod.-Max.
6.	Failure to comply with the TSA-approved security program (general violation to be used if a more specific violation is not given)	Mod.-Max
7.	Failure to maintain IACMS up to date	Min.-Mod.
8.	Failure to produce copy of the program, relevant portions, or implementing instructions at a station where cargo is accepted or processed	Min.
9.	Failure to restrict distribution of security program or implementing instructions to persons with a need to know	Mod.-Max.

10. Failure to maintain or to be able to produce a current listing of authorized agents/contractors (chronic or intentional failures)	Mod.-Max.
11. Failure to supply certification to the aircraft operator	Min.
12. Failure to comply with any requirement necessary to establish a known shipper (repeated failure would justify a maximum penalty)	Mod.
13. False certification or falsification of any document/statement required under the security program	Max. + Criminal Referral
14. Failure to control access to cargo by unauthorized persons	Mod.-Max.
15. Failure to transport cargo in locked or closely-monitored vehicle (includes CCSF chain-of-custody violations)	Mod.-Max.
16. Failure to comply with cargo acceptance requirements	Mod.-Max.
17. Failure to allow access for inspections (sanction should be imposed for every day that access is denied)	Mod.-Max. per day
18. Failure to comply with any requirement related to the screening or inspection of cargo, including failure to screen cargo	Max.
18b. Failure to screen cargo: unscreened cargo flew on passenger aircraft	Max. per piece
18c. Failure to screen cargo: unscreened cargo did not fly on passenger aircraft because of inspector intervention	Min. per piece
19. Failure to obtain required transfer certification	Min.-Mod.
20. Failure to comply with the requirement to submit complete STAs according to 49 C.F.R. §§ 1548.15, 1548.16, 1540.23	Mod.-Max.
21. Failure maintain the health of a canine who screens cargo under the CCSP-K9 program (such as veterinary visits and shots, or using a canine who a vet has determined is not fit to screen cargo)	Max.
22. Failure to adequately rest a canine (such as not resting for the required period of time or resting the canine under inadequate conditions)	Max.
23. Cybersecurity Coordinator	
Failure to designate a qualified Cybersecurity Coordinator and at least one alternate	Max.
Failure to provide Cybersecurity Coordinator contact information	Min.-Mod.

24. Reporting Cybersecurity Incidents

Failure to report a cybersecurity incident to CISA within the specified timeframe	Min.-Mod.
Failure to include required information in report to CISA	Min.

V. FREIGHT RAIL CARRIERS, RSSM SHIPPERS AND RECEIVERS, PUBLIC TRANSPORTATION AND PASSENGER RAIL, AND OVER-THE-ROAD BUS OWNERS/OPERATORS

Inspection

1.	Denial of access to property or failure to cooperate with TSA Inspector	Max.

Responsibility Determinations

2.	Failure to self-identify applicability of Security Training rule (new or modified operations)	Min.- Mod.
3.	Failure to self-identify (pattern of non-compliance)	Mod.-Max.

Recordkeeping and Availability

4.	No records or failure to maintain records	Max.
5.	No records or failure to maintain records (pattern of non-compliance)	Mod.-Max.

Security Coordinator

6.	No Security Coordinator or failure to report to TSA	Max.

Reporting Significant Security Concerns

7.	No system in place to report security concerns/incidents	Max.
8.	Failure to report significant security concern (single event)	Min.
9.	Failure to report significant security concern (pattern of non-compliance)	Mod.-Max

Security Program

10.	No TSA-approved security program	Max.
11.	Failure to follow TSA-Approve Security Program	Mod.-Max.
12.	Failure to amend Security Program	Mod.-Max.
13.	Pattern of noncompliance	Max.

Security Training Plan

14.	No Point of Contact (POC) responsible for security training program	Max.
15.	Failure to identify by number security-sensitive employees, specific job function category, trained or to be trained	Mod.
16.	Failure to maintain and track implementation schedule for employees	Mod.
17.	Failure to follow TSA-approved Curriculum or lesson plan, including learning objectives and method of delivery	Min.-Mod.
18.	Failure to follow TSA-approved plan for ensuring supervision of untrained security-sensitive employees	Min.-Mod.
19.	Failure to follow TSA-approved plan for notifying employees of changes to security measures	Min.-Mod.
20.	Failure to adhere to TSA-Approved method(s) for evaluating the effectiveness of the security training program	Mod.-Max.
21.	Pattern of noncompliance	Max.

Security Training and Knowledge for SSEs

22.	Failure to ensure use of non-trained employees performing SJF's does not exceed sixty (60) calendar days	Mod.-Max.
23.	Failure to ensure use of non-trained employees performing SJF's does not exceed sixty (60) calendar days (pattern of noncompliance)	Max.

Chain of Custody (RSSM)

24.	No system for documenting Chain of Custody	Max.
25.	Leaving RSSM rail car(s) unattended during physical transfer of custody	Mod.
26.	Failure to document transfer of custody-single event	Min.
27.	Failure to maintain transfer of custody documents (Unable to produce records at time of inspection)	Mod.
28.	Failure to keep loaded RSSM cars in a rail secure area	Mod.
29.	Pattern of non-compliance	Max.
30.	Failure to perform security inspection per 49 CFR § 174.9	Min.

Location and Shipping Information

31.	Failure to have process in place to provide RSSM car location	Mod.
32.	Failure to provide information for a single car within five minutes of request (Class 1 Railroad only)	Min.
33.	Failure to provide requested information within thirty (30) minutes	Min.
34.	Failure to provide telephone number to TSA for requesting car location	Mod.
35.	Pattern of noncompliance	Mod.-Max.

Security Directives

36.	Failure to carry out a requirement in a Security Directive (general violation to be used when more specific violation is not listed)	Mod.-Max.

Cybersecurity Coordinator

37.	Failure to designate a qualified Cybersecurity Coordinator and at least one alternate	Max.
38.	Failure to provide Cybersecurity Coordinator contact information	Min.-Mod.

Reporting Cybersecurity Incidents

39.	Failure to report a cybersecurity incident to CISA within the specified timeframe	Min.-Mod.
40.	Failure to include required information in report to CISA	Min.

Cybersecurity Implementation Plan

41.	Operating without a TSA-approved Cybersecurity Implementation Plan	Max.
42.	Failure to identify a Critical Cyber System	Max.
43.	Failure to comply with a network segmentation policy or control as described in TSA-approved Cybersecurity Implementation Plan	Mod.-Max.
44.	Failure to comply with an access control measure as described in TSA-approved Cybersecurity Implementation Plan	Mod.-Max.
45.	Failure to comply with a continuous monitoring and detection policy or procedure as described in TSA-approved Cybersecurity Implementation Plan	Mod.-Max.

46. Failure to comply with a mitigation measure or manual control, as described in TSA-approved Cybersecurity Implementation Plan, implemented to ensure that industrial control systems can be isolated when a cybersecurity incident in the Information Technology system creates a risk to the safety and reliability of the Operational Technology system	Max.
47. Failure to apply a security patch or update consistent with the risk-based methodology described in TSA-approved Cybersecurity Implementation Plan	Max.
48. Failure to submit a request to amend TSA-approved Cybersecurity Implementation Plan in the event of a change in ownership or control of operations or a change in conditions affecting security	Min.-Mod.
<u>Cybersecurity Incident Response Plan</u>	
49. Failure to have an up-to-date Cybersecurity Incident Response Plan	Max.
50. Failure to include a required piece of information in a Cybersecurity Incident Response Plan	Mod.-Max.
<u>Cybersecurity Assessment Program</u>	
51. Failure to submit the annual plan for the Cybersecurity Assessment Program	Mod.-Max.
52. Failure to include a required piece of information in the annual plan for the Cybersecurity Assessment Program	Mod.-Max.
<u>Cybersecurity Vulnerability Assessment</u>	
53. Failure to submit a completed vulnerability assessment form and remediation plan to TSA within the specified timeframe	Mod.-Max.
<u>Inspections and Documentation</u>	
54. Failure to make a record available or failure to provide a record necessary to establish compliance with a Security Directive	Max.
55. Failure to allow a TSA inspection	Max.

Transportation Security Administration

VI. INDIVIDUALS

1. Security Violations by Individuals for Prohibited Items Discovered at Checkpoint/Sterile Area/Onboard Aircraft

A. Firearms (including 3D-printed), Realistic Firearm Replicas, and Shocking Devices

i. Loaded firearms (or unloaded firearms with accessible ammunition)	$3,000-$10,700 + Criminal Referral or $10,700-$14,950 + Criminal Referral (repeat offense)
ii. Unloaded firearms	$1,500-$5,370 + Criminal Referral
iii. BB, pellet, and compressed-air guns; flare and starter pistols; realistic replicas of firearms (including gun lighters or training devices/aids); permanently inert firearms; spear guns; stun guns, cattle prods, or other shocking devices	$390-$2,250
iv. Silencers, mufflers, frames and/or receivers	$740-$1,490 + Criminal Referral

B. Sharp Objects

i. Axes and hatchets; bows and/or arrows; ice axes and ice picks; knives with blades that open automatically (such as switchblades) at any length; knives with blades that open via gravity (such as butterfly knives) at any length; double-edge knives or daggers; meat cleavers; sabers; swords; fencing foils; and machetes; throwing stars and throwing knives (including 3D-printed throwing stars and knives)	$390-$2,250

C. Incendiaries

i. Any flammable liquid or gel fuels, including but not limited to gasoline, lighter fluids, cooking fuels; turpentine and paint thinners	$390-$2,250
ii. Smoke grenades/flash bangs	$740-$3,720 + Criminal Referral

D. Disabling Chemicals

i.	Self-defense spray; tear gas	$390-$2,250

E. Explosives

i.	Blasting caps; initiators; dynamite; gunpowder more than 10 oz.); hand grenades; plastic explosives; all other high explosives	$8,960-$14,950 + Criminal Referral
ii.	Realistic replicas of explosives; inert hand grenades; intact vehicle air bags	$740-$3,720 + Criminal Referral
iii.	Novelty hand grenades (such as perfume bottles, stress balls, costume jewelry, and grenade lighters); consumer fireworks, novelty fireworks, professional display fireworks; flares; gunpowder (10 oz. or less); ammunition; inert initiator or primer	$390-$2,250 + Criminal Referral

2. Security Violations for Prohibited Items Discovered in Checked Baggage

A. Firearms

i.	Loaded firearms	$1,490-$2,990 + Criminal Referral
ii.	Undeclared and/or improperly packaged silencers; mufflers; frames and/or receivers	$390-$2,250
iii.	Undeclared and/or improperly packaged firearms; modified starter pistols	$740-$1,490

B. Incendiaries

i.	Any flammable liquid or gel fuels, including but not limited to gasoline, lighter fluids, cooking fuels; turpentine and paint thinners	$390-$2,250
ii.	Smoke grenades/flash bangs	$740-$3,720 + Criminal Referral

C. Explosives

i.	Blasting caps; initiators; dynamite; gunpowder more than 10 oz.); hand grenades; plastic explosives; all other high explosives	$8,960-$14,950 + Criminal Referral
ii.	Realistic replicas of explosives; inert hand grenades; intact vehicle air bags	$740-$3,720 + Criminal Referral

iii. Novelty hand grenades (such as perfume bottles, stress balls, costume jewelry, and grenade lighters); consumer fireworks, novelty fireworks, professional display fireworks; flares; gunpowder (10 oz. or less); ammunition; inert initiator or primer	$390-$2,250 + Criminal Referral

3. Other Security Violations by Individuals or Persons*

A. Attempt to circumvent a security system, measure, or procedure by the artful concealment of a non-explosive liquid, aerosol, or gel (other than those permitted)	$140-$300
B. Ordinary artful concealment	
i. Shocking devices; cellphone and/or flashlight stun guns; tasers	$390-$2,250
ii. Sharp objects; cane swords; lipstick/pen/belt buckle knives	$530-$2,250
iii. Guns/firearms; pen/cell phone guns	$4,950-$10,700
C. Extraordinary artful concealment	
i. Gun wrapped in aluminum foil; book that has been hollowed out to uniquely fit a prohibited item	$5,320-$10,700
D. Interference with screening	
i. Assault with injury	$11,300-$14,950
ii. Assault without injury	$5,830-$11,300
iii. Non-physical interference	$2,250-$5,830
E. Entering sterile area without submitting to screening	$740-$4,480
F. Tampering or interfering with, compromising, modifying, attempting to circumvent, or causing a person to tamper or interfere with, compromise, modify or attempt to circumvent any security system, measure, or procedure	Sanction amount based on underlying security requirement
G. Entering or being present within a secured area, AOA, SIDA, or sterile area without complying with the systems, measures, or procedures being applied to control access to, or presence or movement in, such areas	$740-$4,480
H. Improper use of airport access medium	$740-$4,480
I. Fraud and intentional falsification	$3,720-$8,960 + Criminal Referral

J.	Failure to allow inspection of airman certificate, authorization, FAA license	$1,490-$4,480
K.	Failure to comply with any other requirements for operating to or from the airport specified by TSA or FAA per 49 CFR § 1562.3(f)(3)	$3,720 - $8,960
L.	False information - knowing the information to be false, gives, or causes to be given, under circumstances in which the information reasonably may be believed, false information	$1,490-$4,480
M.	Failure to protect Sensitive Security Information (SSI) per 49 CFR Part 1520	Up to $12,794
N.	Failure of TSA employees to return TSA patches, badges, and other insignia	$1,450-$5,900

*Violations not listed above are subject to the regulatory civil penalty maximum of $14,950.

VII. SECURITY VIOLATIONS RELATED TO THE TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC)

1.	Misuse of a TWIC	$630-$3,830
2.	Fraudulent manufacture or alteration of a TWIC	$1,190-$3,830 + Criminal Referral
3.	Circumvention or compromise of TWIC access control procedures	$1,280-$3,830
4.	Failure of individual to allow inspection of a TWIC	$630-$1,280
5.	Failure to allow inspection of a TWIC	$630-$1,280
6.	False application for a TWIC	$1,280-$3,830 + Criminal Referral
7.	Failure to surrender a TWIC	$630-$3,830
8.	Fraud, intentional falsification	$1,280-$3,830