U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

Technical Change
Issued December 12, 2022

TSA ACTION PLAN PROGRAM
EFFECTIVE AUGUST 26, 2019

I. PURPOSE

The Transportation Security Administration (TSA) believes that transportation security is well-served by creating incentives for eligible parties to identify security vulnerabilities, correct their own instances of regulatory noncompliance whether discovered by the eligible party or TSA, and invest resources and effort to improve transportation security. TSA's goal is to increase partnership with industry stakeholders, mitigate vulnerabilities, obtain compliance, and sustain the highest levels of security through shared outcomes.[1]

TSA's Action Plan Program provides an opportunity for eligible parties and TSA to discuss and reach an agreement on corrective actions to address the root cause of any security vulnerability or noncompliance with TSA's security requirements which qualifies for this program, and resolve that vulnerability or noncompliance with administrative action instead of a civil enforcement action.[2] The Action Plan Program provides eligible parties with the opportunity to offset potential civil penalties with investment and without a formal adjudication of regulatory violations, a clear benefit over the traditional civil enforcement process which results in a violation history. Participation in the Action Plan Program by an eligible party is completely voluntary.

This document informs eligible parties of which vulnerabilities or noncompliance will be eligible for an action plan and the process by which an action plan will be achieved. This Action Plan Program **document supersedes and** replaces **the Action Plan Program document issued on June 26, 2019**.[3]

II. APPLICABILITY

This Program applies to eligible parties when there is an identified security vulnerability or an instance of noncompliance, either disclosed voluntarily or discovered by TSA. This Program generally does not apply to egregious or intentional noncompliance with TSA's regulatory requirements or to those involving criminal activity or fraud, all of which present an unacceptable risk to security. The Action Plan Program is implemented by TSA's Security Operations and

---

[1] The Agency has a wide range of options available for addressing instances of noncompliance with TSA's security requirements such as oral or written counseling; administrative action, including remedial training; legal enforcement action; and referral for criminal prosecution. The Action Plan Program is an addition to TSA's progressive enforcement philosophy of resolved with counseling, Administrative Actions (Warning Notices and Letters of Correction), action plans, civil penalty actions, and withdrawal of TSA approval of a regulated entity's security program.

[2] This Program provides the policies and procedures under which eligible parties may avail themselves under the Action Plan Program. Additionally, TSA will circulate internal guidance that will govern TSA personnel under the Action Plan Program.

[3] **The Program document issued on June 26, 2019 replaced the Voluntary Disclosure Program Policy, the Resolution Corrective Action Policy for U.S. Locations, and the Vulnerability Mitigation Policy for U.S. Locations**

participation in the Action Plan Program is voluntary. Nothing in this Program prevents an eligible party from engaging with its assigned representative in TSA's Policy, Plans & Engagement.

1. **Voluntary Disclosures by Eligible Parties**: TSA encourages eligible parties to discover their own instances of noncompliance and take prompt and effective corrective action to ensure that the same or similar noncompliance does not reoccur.

2. **TSA Discovered Noncompliance**: TSA encourages eligible parties to take prompt and effective corrective action when TSA discovers an instance of noncompliance with a security requirement to ensure that the same or similar noncompliance does not reoccur.

3. **Security Vulnerabilities**: TSA encourages eligible parties to take prompt and effective action to address significant vulnerabilities identified by either an eligible party or TSA through audits, testing, and other data.[4] Vulnerabilities are not regulatory violations. In the event noncompliance with a TSA security requirement occurs during the execution of an action plan implemented to address a vulnerability, TSA will not initiate an administrative or civil enforcement action. Noncompliance which occurs during an action plan based on a vulnerability is fully discussed in Section X, Repeated Instances of Noncompliance.[5]

III. APPLICABLE TSA REGULATIONS

This Program applies to the following Transportation Security Regulations (TSRs) and relevant security programs: 49 C.F.R. Part 1520, Protection of Sensitive Security Information; 49 C.F.R. Part 1540, Civil Aviation Security: General Rules (but not 49 C.F.R. § 1540.103); 49 C.F.R. Part 1542, Airport Security; 49 C.F.R. Part 1544, Aircraft Operator Security: Air Carriers and Commercial Operators; 49 C.F.R. Part 1546, Foreign Air Carrier Security; 49 C.F.R. Part 1548, Indirect Air Carrier Security; 49 C.F.R. Part 1549, Certified Cargo Screening Program; 49 C.F.R. Part 1550, Aircraft Security Under General Operating and Flight Rules; 49 C.F.R. Part 1552, Flight Schools; 49 C.F.R. Part 1554, Aircraft Repair Station Security; 49 C.F.R. Part 1560, Secure Flight Program; 49 C.F.R. Part 1562, Operations in the Washington, DC, Metropolitan Area; 49 C.F.R. Part 1570, General Rules (but not 49 C.F.R. §§ 1570.5, 1570.7,and 1570.13); 49 C.F.R. Part 1572, Credentialing and Security Threat Assessments; 49 C.F.R. Part 1580, **Freight** Rail Transportation Security**; 49 C.F.R. Part 1582, Public Transportation and Passenger Railroad Security; 49 C.F.R. Part 1584, Highway and Motor Carrier Security, and any other entity which is regulated by TSA**.

IV. DEFINITIONS

a) Action Plan Letter. This is a letter**, which may be** created by **either** the Designated TSA Official or the eligible party**, and is** based on information provided by the eligible party which contains specific details regarding how the eligible party will address the root cause of the

[4] TSA will provide compliance briefings to eligible parties upon request. A compliance briefing generally includes information from TSA concerning regulatory compliance and stakeholder security issues, including Action Plans, best practices/effective measures, security coordination, trend analysis, and any non-regulatory vulnerabilities.
[5] Not all vulnerabilities are appropriately addressed through an action plan. As with all action plans, both TSA and the Eligible Party must agree that an action plan is an appropriate response.

U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

violation(s) or vulnerability(ies) through corrective action(s). It must describe any corrective action(s) that has already been implemented by the eligible party, the proposed corrective action(s) to be taken, and an anticipated deadline for its completion. TSA and the eligible party must both agree to an Action Plan before it becomes final.

b) Analysis of root cause. A wide range of approaches, tools, and techniques which determine how noncompliance occurred or is likely to occur by examining the why, how, and when of the causal factors.

c) Compliance History. Compliance history contains facts concerning documented counseling, any Administrative Action, a Compromise Order, an action plan and pending civil penalty cases involving the same or similar alleged violation in an EIR during the past five (5) years for a regulated entity. The Compliance History does not include the Violation History, which includes only violations that have been formally adjudicated. Compliance History is neither an aggravating factor nor a mitigating factor when determining an appropriate monetary civil penalty. However, Compliance History may be used as notice to the eligible party that TSA considers the underlying conduct to be a violation of TSA security requirements. Compliance History may also be used by TSA to determine which step in the progressive enforcement philosophy is appropriate to address future instances of noncompliance. No Action letters are not part of Compliance History.

d) Designated TSA Official (DTO). The TSA official responsible for oversight and coordination of the resolution of the matter disclosed under this Program.

1. The DTO for matters involving airport operators, flight schools, aircraft repair stations, as well as those involving 49 C.F.R. parts 1562, 1570, 1572 and 1580, is the Federal Security Director (FSD) who has responsibility for the area where the noncompliance occurred. The FSD is also the DTO for matters involving aircraft operators, foreign air carriers, Indirect Air Carriers and Certified Cargo Screening Facilities if the matter occurs only in the FSD's area of responsibility.[6]

2. The DTO for matters at non-U.S. locations is the Regional Operations Center (ROC) Manager who has responsibility for the area where the noncompliance occurred.

3. The DTO for matters involving aircraft operators or other eligible parties where the noncompliance or vulnerability involves multiple FSDs or ROC Managers is the TSA Headquarters individual assigned to Security Operations who has responsibility for the entity.

4. **The DTO for matters involving pipelines operators is the Regional Security Director (RSD) who has responsibility for the area where the noncompliance occurred.**

[6] The FSD may delegate this responsibility to the applicable Assistant Federal Security Director – Inspections (AFSD-I).

5. **The DTO for matters involving freight and passengers rail operators under 49 C.F.R. 1580 and 49 C.F.R. 1582, respectively, as well as over-the-road bus (OTRB) operators under 49 C.F.R. 1584, is the RSD.**

e) Eligible party. Aircraft operators, foreign air carriers, indirect air carriers, certified cargo screening facilities (including Third-Party Canine-Cargo Program – 3PK9-C Program), airport operators, flight training providers, all freight and passenger railroad carriers, certain facilities that ship or receive specified hazardous materials by rail, rail transit systems**, OTRB operators, and owners and operators of hazardous liquid and natural gas pipelines or liquefied natural gas facilities notified by TSA that their pipeline system or facility is critical.**

f) Joint test. A test conducted by TSA and one or more eligible parties to determine collaboratively the parties' compliance with TSA requirements and/or security effectiveness.

g) Letter of Correction (LOC). In matters involving noncompliance, this letter is issued by a DTO when all corrective actions in an action plan have been validated by TSA. This includes, where applicable, coordination with other offices within TSA. A LOC is not part of an eligible party's violation history. This letter, which is not appealable, will state that it does not constitute a formal adjudication of the matter and that it is part of only the Compliance History of the eligible party. A LOC will not be issued in action plans involving exclusively security vulnerabilities.

h) Letter of Rejection. This letter is issued by a DTO when an action plan is not feasible or is agreed to but not implemented in whole or part, including but not limited to, if: (1) the eligible party does not respond in a timely manner to the DTO's requests for information or answers, does not provide the supporting materials at the action plan meeting, or does not provide the projected **tangible and intangible** cost of implementation of the action plan, if applicable; (2) the eligible party fails to participate in the action plan meeting with TSA; (3) the action plan details cannot be agreed upon by the parties; (4) the eligible party fails to acknowledge and confirm the action plan in writing; (5) the action plan is not implemented and/or the DTO is unable to validate the corrective actions; or (6) there is an inability to resolve any issue under Section VIII, Dispute Resolution of this Program. After issuance of this letter, TSA will proceed with an investigation into any noncompliance, if applicable. An issued Letter of Rejection cannot be considered as an aggravating factor for any related or subsequent civil enforcement matter.

i) Supporting Materials. Supporting materials include, but are not limited to, all written documentation, audio and video recordings, electronic data, and photographs that support an eligible party's noncompliance or vulnerability. Supporting materials may include an analysis of the corrective actions' impact to transportation security.

j) Violation History. Violation history contains facts concerning all prior adjudicated findings of violations involving the same or similar alleged violation during the past five (5) years for a regulated entity. Only those prior violations in which formal adjudications were made (e.g.,

an Order Assessing Civil Penalty (OACP) or a Consent Order issued by a TSA attorney, an Initial Decision/Order from an administrative law judge (ALJ), a Final Decision from the TSA Decision Maker, or a Decision by an Appellate Court) should be included in the Violation History. An entity's Violation History is an aggravating factor when determining an appropriate civil penalty.

k) Voluntary Disclosure Report (VDR). This report must be provided to the DTO by an official for the eligible party making a voluntary disclosure within seven (7) business days after the initial voluntary disclosure notification. It must include a description and summary of the noncompliance, a description of the immediate action(s) taken to address the noncompliance, and a summary and analysis of supporting materials, including the impact to transportation security. The VDR is fully discussed in Section VI.d.

l) Vulnerability. A vulnerability is a physical feature or operational attribute that renders an entity open to exploitation or makes it susceptible to a given hazard. For purposes of this document, a vulnerability refers to any circumstances or conditions which are a threat to transportation security prior to the occurrence of any noncompliance related to that vulnerability. **A vulnerability may also include occasions when an eligible party is required to implement a new security requirement and notifies TSA ahead of the implementation deadline that it will be unable to meet the deadline due to circumstances beyond its control.**

V. ACTION PLAN CONDITIONS

In evaluating whether noncompliance or vulnerabilities are covered by this Program, the following conditions must be met:

1. The noncompliance or vulnerability cannot include egregious, flagrant, continuous, wanton, bad-faith, extraordinary, or conspicuously bad or glaring deviations from TSA's regulatory requirements. Also, the noncompliance or vulnerability cannot include deliberate or intentional deviations from TSA's regulatory requirements, deviations from TSA's regulatory requirements founded upon reckless disregard for the facts committed by the eligible party's mid or upper level management, nor those involving criminal activity or fraud.[7]
2. Immediate action or action as soon as practicable was taken upon discovery of the noncompliance to terminate the conduct that resulted in the noncompliance, if applicable.

[7] This list is not intended to cover all possible conduct or behavior that could lead to non-availability of an action plan. In some cases, noncompliance which is considered intentional or egregious may be resolved through corrective actions undertaken as part of a settlement agreement during or after an investigation has been completed. In those circumstances, TSA reserves the ability to notify affected regulated entities and refer the matter to Chief Counsel's office for settlement negotiation.

U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

VI. VOLUNTARY DISCLOSURE PROCEDURES

This Section only applies to eligible parties making a voluntary disclosure of noncompliance with a TSA security requirement:

a) Initial Notification to TSA. The voluntary disclosure is made to the DTO immediately or as soon as possible after the eligible party discovers the noncompliance. The initial notification must be made electronically by emailing the DTO and copying TSAVDP@tsa.dhs.gov and must include, to the extent possible, the following information:

1. A brief description of the instance(s) of noncompliance, where it occurred, an estimate of the time that it remained undetected, as well as how and when it was discovered.

2. Verification that, upon discovery, immediate action was taken to terminate the relevant conduct.

3. The name, title, and contact information for the individual making the initial notification.

b) Upon receipt of the Initial Notification, TSA will email the notifying individual acknowledging that the initial notification has been received by TSA and, if different, also notify the individual who would have received the Letter of Investigation (LOI) under the civil enforcement process. The eligible party must preserve all supporting materials regarding the underlying violations.

c) The eligible party will provide a written VDR to the DTO within seven (7) business days of the date of the TSA email response acknowledging receipt of the initial notification. If the eligible party cannot provide a written VDR to the DTO within this timeframe, the eligible party may request a reasonable extension of time. It is within the discretion of the DTO to grant an extension or determine if an action plan continues to remain feasible in light of the request for extension of time.

d) The following information must be provided to the DTO by the eligible party in the VDR:

1. Description of noncompliance. This should include a citation of the relevant TSA regulation(s), Security Program(s), Security Directives (SD) and/or Emergency Amendments (EA), the date, time, and location of the noncompliance, and the date, time, and recipient of the initial notification.

2. Summary of noncompliance. This should include a brief statement describing each instance of noncompliance, the number of times it occurred, and identifying the associated equipment, facilities, procedures, checkpoint, gate, cargo, and/or individuals.

3. Immediate action. This should include the date, time, and description of when immediate action was taken to address the noncompliance, and the company official responsible for taking the immediate action including name, position and telephone number.

4. Summary and analysis of supporting material. This should include a description of the scope of the noncompliance, an explanation of how it was detected, and why it occurred. It should also include the supporting materials associated with each instance of noncompliance. It may also include an analysis of impact of any proposed corrective actions.

e) Upon receipt of the VDR, TSA will review the information and decide whether the information is sufficient enough to determine if an action plan is appropriate.

1. If the VDR is accepted, the DTO will follow the procedures outlined in Section VII, Action Plan Process.

2. If the VDR is not acceptable, the DTO will work with the eligible party to resolve any issues. If a revised VDR is insufficient, the DTO will issue a Letter of Rejection advising that TSA will proceed with an investigation.

3. If the eligible party fails to meet any deadline or revised deadline date, the DTO may issue a Letter of Rejection advising that TSA will proceed with an investigation.

VII. ACTION PLAN PROCESS

After the DTO evaluates the matter and makes a determination that the noncompliance or vulnerability is eligible for an action plan based on the parameters outlined in Section V, Action Plan Conditions, the following steps will occur:

a) The DTO will contact the eligible party's representative who would have received the Letter of Investigation (LOI) under the civil enforcement process and notify them that the noncompliance or vulnerability is being considered for an action plan.

b) Upon notification of any TSA-discovered noncompliance or vulnerability, the DTO will provide up to fourteen (14) business days for the eligible party to review the circumstances and conduct their own investigation into the noncompliance or vulnerability.

c) After the review period, the eligible party will contact the DTO, indicate whether the eligible party wishes to proceed with the action plan process, and set up a time to discuss the root cause of the noncompliance or vulnerability and potential corrective actions. This meeting may be either in person, over video conference, or over teleconference and should occur within seven (7) business days of the eligible party's response.

d) Participation in an action plan is voluntary. The eligible party may request to withdraw completely from the action plan process at any time. If the action plan is based on a vulnerability, there are no consequences for an entity's withdrawal from the process. If the action plan is based on noncompliance, TSA will initiate an investigation into that noncompliance. However, if an eligible party does not wish to proceed with an action plan or

chooses to withdraw from an action plan, it will not be an aggravating factor in any related civil enforcement matter.

e) The meeting between the DTO and the eligible party will be a discussion and negotiation to agree upon appropriate corrective actions which address the root cause of the issue.

f) In order to properly ascertain whether an action plan is appropriate and whether the proposed corrective actions are commensurate with the noncompliance or vulnerability, the eligible party must be prepared to discuss during the meeting with the DTO:

1. An analysis of root cause, including any supporting materials that confirm the analysis of the root cause;

2. A detailed description of the corrective action(s) proposed or already taken to address the noncompliance and the root cause(s), and the specific equipment, facilities, procedures, checkpoint, gate, cargo and/or individuals associated with each instance of noncompliance or vulnerability;

3. Whether procedural or organizational changes, such as the hiring of a manager dedicated to TSA security requirements, are part of the actions that resolve the noncompliance or vulnerability;

4. The projected cost of implementing the corrective action(s), if applicable, including but not limited to the acquisition, replacement, or upgrade of any screening equipment, salaries of any new hires directly related to correcting the noncompliance or vulnerability, upgrades to security training, the installation of a video monitoring system, the implementation of audit procedures, and/or the implementation of a covert testing program of security procedures;

5. **The projected intangible cost(s), if applicable, (for example, hours dedicated to retraining employees);** and

6. The anticipated completion date of each corrective action**, including identifying substantive milestones and when they are anticipated to be reached**.

g) If the eligible party wishes to participate in the action plan process but cannot provide the above information within the seven (7) day timeframe, it is within the discretion of the DTO to grant an extension and/or determine if an action plan remains feasible.

h) During the meeting, the eligible party will bring all requested supporting materials available at the time,[8] which may include an analysis of the impact of the corrective actions on

[8] Action plans are mutually agreed upon and are designed to address root causes of noncompliance with TSA security regulations or security vulnerabilities. It is important that both TSA and the eligible entity have a full understanding of the facts and circumstances in order to determine root causes. Accordingly, it is important that the eligible party make available in a timely fashion documents and other information requested by the DTO.

transportation security, and the DTO and eligible party will collaborate and agree upon the corrective action(s) to be included in the action plan. The failure to provide requested supporting materials or the projected **tangible and/or intangible** cost of the corrective action will conclude the action plan process and a Letter of Rejection will be issued.

i) The failure to provide an analysis of root cause will not preclude a DTO's acceptance of an action plan. While it is strongly recommended that the eligible party provide an analysis of root cause whenever possible, failure to provide an analysis of root cause should not necessarily result in a delay of the action plan's implementation.

j) For cases involving a voluntary disclosure, the voluntary disclosure must be considered a mitigating factor during the discussion and negotiation of an action plan.

k) In order to promote consistency, if an eligible party has successfully implemented a corrective action plan at a different location, if that other action plan addresses the same root cause(s), TSA will consider the implemented corrective actions during the action plan meeting.

l) At the conclusion of the meeting, TSA and the eligible party will have agreed upon the root cause and the corrective measure(s) to be implemented in the action plan.[9] In the event the corrective measure(s) are not agreed upon during the meeting, TSA and the eligible party will continue to meet and/or discuss the proposed measure(s) until both parties are in agreement. It is within the discretion of the DTO to assess whether continued negotiations will conclude with an agreed upon action plan. If the eligible party does not agree with the corrective measure(s) proposed by the DTO and the parties are unable to resolve the issues, the eligible party may elect to refer the matter pursuant to the provisions of Section VIII of this Program, Dispute Resolution.

m) After agreeing upon the root cause and corrective actions, the DTO will create and send the action plan letter to the eligible party, which details the corrective action(s) agreed upon by the parties during the meeting. If the parties agree, the action plan letter may be drafted by the eligible party.

n) Each corrective action(s) documented within the action plan letter must identify either a completion date or the period of time that the corrective action(s) will remain in place.

o) Upon receipt of an action plan letter, within seven (7) business days, the eligible party must send a written acknowledgment to the DTO indicating the action plan is accurate and agreeing to the corrective actions contained in the action plan letter. If the action plan letter is created

[9] In rare circumstances, the DTO may include as an agreed upon measure a request for an amendment to modify the eligible party's TSA Approved Security Program to include some, or all, of the corrective measure(s) identified in the action plan letter as a condition of resolving the regulatory violations by action plan versus civil penalty. Circumstances where the inclusion of the action plan in the entity's security program is justified must be based on the nature of the noncompliance, for example, noncompliance which approaches egregiousness but where TSA has agreed to resolve the issue under the Action Plan Program. In these rare instances, this inclusion will be an agreed upon term of the action plan and TSA will follow the amendment procedures outlined in 49 C.F.R. §§ 1542.105, 1544.105, 1546.105, 1548.7, and 1549.7.

by the eligible party, TSA will send the written acknowledgment of receipt indicating the action plan is accurate and agreeing to the corrective actions contained in the letter.

p) If changes need to be made to any action plan, the eligible party may request the DTO amend the corrective actions. The request for an amendment must include the reasons for the proposed changes. If the amendment is approved, the DTO will provide written notification to the eligible party. If the amendment is not acceptable, TSA will work with the eligible party to resolve any issues. If the issue cannot be resolved, the matter will be handled pursuant to the provisions in Section VIII, Dispute Resolution, in this Program.

q) The eligible party will notify TSA immediately upon successful completion of any corrective action contained in any action plan and verify the successful implementation of the corrective action(s).

r) A failure of a joint test is not considered an instance of noncompliance and TSA will work with the eligible party to resolve any issues. For other instances of noncompliance, see Section X, Repeated Instances of Noncompliance.

s) For only instances involving noncompliance, once the DTO has verified the corrective action(s) detailed in the action plan, TSA will send the eligible party a LOC advising that the corrective action(s) is approved. A LOC will not be issued in matters involving only security vulnerabilities. The LOC is part of the compliance history of an eligible party but is not a part of the violation history.

t) For only instances involving vulnerabilities, once the DTO has verified the corrective action(s) detailed in the action plan, TSA will send the eligible party a written acknowledgment that the action plan has been completed. This letter will not be a part of the entity's compliance history or violation history.

VIII. DISPUTE RESOLUTION

Any dispute pertaining to the details of an action plan or the above described process may be referred to TSA Security Operations, **Assistant Administrator** of Compliance for resolution. At the time of the referral, the eligible party may submit a letter or email explaining the issue along with any supporting documentation. Should there be an inability to resolve the issue or if the eligible party does not agree with the decision, a Letter of Rejection will be issued to the eligible party and, only in matters involving noncompliance, TSA will proceed with an investigation. If the action plan is based entirely on a vulnerability without noncompliance, the DTO will issue a Letter of Rejection and any noncompliance based on that vulnerability will be resolved under Section X, Repeated Instances of Noncompliance.

In the event there is an issue regarding an agreed upon or proposed term in an action plan in relation to an interpretation of a TSA regulation, security program, SD or EA, the eligible party may request the issue be taken under consideration by requesting in writing and provide supporting documentation

to TSA Security Operations, **Assistant Administrator** of Compliance for resolution.[10] The issue will be coordinated with the appropriate parties within TSA and a decision will be made regarding the issue. If the eligible party disagrees with the decision and does not wish to participate in an action plan, in matters involving noncompliance, a Letter of Investigation will be issued and TSA will proceed with an investigation. If the action plan is based entirely on a vulnerability without noncompliance, the DTO will issue a Letter of Rejection and any noncompliance based on that vulnerability will be resolved under Section X, Repeated Instances of Noncompliance.

IX. DISCLOSURE OF RECORDS PROVIDED TO TSA

Supporting materials submitted to TSA for review will be protected to the full extent allowed by law.[11]

X. REPEATED INSTANCES OF NONCOMPLIANCE

During the action plan process but prior to the issuance of the LOC, if any repeated similar instance(s) of noncompliance is disclosed by the eligible party or discovered by TSA, unless the noncompliance involves egregious deviations or intentional deviations by mid or upper level management from TSA's regulatory requirements, criminal activity or fraud, TSA will not initiate an administrative or civil enforcement action on the repeated similar noncompliance at that time.

In matters where the action plan is based on a vulnerability, if noncompliance is discovered or disclosed based on that identified vulnerability, unless the noncompliance involves egregious deviations or intentional deviations by mid or upper level management from TSA's regulatory requirements, criminal activity or fraud, TSA will not initiate an administrative or civil enforcement action on the noncompliance at that time.

Instead, under both circumstances, TSA and the eligible party will work together to amend the action plan, as described in Section VII, paragraph o, to address the instance(s) of noncompliance. If the subsequent noncompliance is disclosed by the eligible party, the DTO is required to consider that disclosure as a mitigating factor during any amendment negotiations. If the parties cannot agree on an amendment and are unable to resolve any dispute under Section VIII, Dispute Resolution, TSA will issue a Letter of Rejection to the eligible party advising the action plan is being terminated, and TSA will proceed with an investigation into the subsequent noncompliance and, if applicable, the initial noncompliance.

However, if the repeated instance of noncompliance involves egregious deviations or intentional deviations by mid or upper level management, criminal activity or fraud, all of which present an unacceptable risk to security, TSA will immediately proceed with an investigation.

---

[10] All policy interpretation issues unrelated to a specific corrective action of an action plan must be referred to the TSA Policy, Plans & Engagement for resolution.

[11] In the event an eligible party has entered into an Information Sharing Agreement (ISA) with TSA, any commercial or proprietary information will be deemed and marked Confidential and will be protected under the parameters of the ISA. Additionally, information disclosed to TSA may be Sensitive Security Information (SSI) and receive the protections specified under 49 C.F.R. Part 1520.

U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

After the LOC or Letter of Rejection is issued, if any repeated similar instance(s) of noncompliance is disclosed by the eligible party or discovered by TSA, TSA will follow its progressive enforcement philosophy and offer an action plan again whenever possible.

In matters where the action plan is based on a vulnerability, if noncompliance is discovered after the completion of an action plan on that identified vulnerability, TSA will follow its progressive enforcement philosophy and offer an action plan again whenever possible.

XI. EFFECTIVE DATE OF THE TSA ACTION PLAN PROGRAM

The effective date of this Action Plan Program is August 26, 2019. This Program remains effective unless otherwise terminated or amended by TSA.